IAM

Identity Access Management

Wer darf was und wann?

Strukturierte und schnelle Rechtevergabe in IT-Strukturen

KEYIDENTITY

WE SECURE IDENTITIES

Identity Access Management

Wer darf was und wann? Strukturierte Rechtevergabe in IT-Systemen

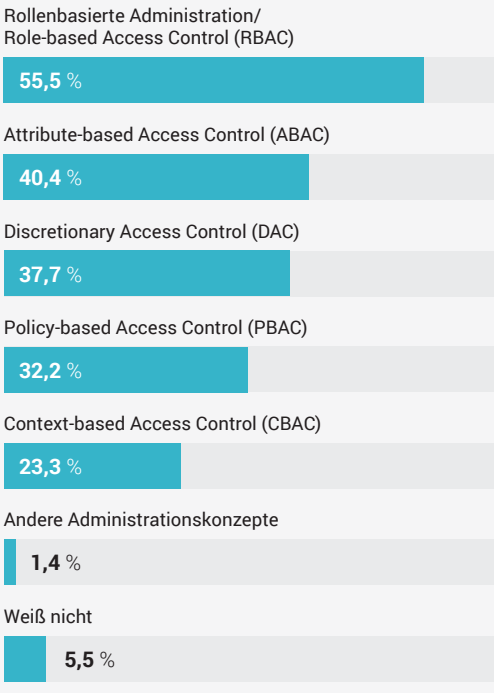
Unternehmen müssen eine große Anzahl von Identitäten und Zugriffsrechten verwalten. Das Thema Sicherheit ist ein beherrschendes Thema: Es gibt viele Anwendungen und Software-Systeme, regelmäßige Audits, Gesetzen und Richtlinien im Bereich von HIPAA, SOX, BIG, ISO 2700x oder KonTraG, Mitarbeiter, die kommen und gehen – und eine Heerschar von Mitarbeitern, die für die nötige Sicherheit sorgen muss. Das erzeugt enorme Kosten und verhindert letztlich, dass sich das Unternehmen dynamisch weiterentwickeln kann. Mit einem neuen IAM-Sicherheitssystem lassen sich der Aufwand und die Kosten aber drastisch senken.

Große Datenbanken, viele Anwendungen, sehr viele Systeme, die intern und extern angebunden sind: Oft sind hunderte verschiedener Server-Systeme und Softwareprodukte im Einsatz. Das fordert die IT ungemein heraus, denn Sicherheit und die Einhaltung von Compliance-Vorgaben stehen meist ganz oben auf der Prioritätenliste.

Das Thema Zugriffsrechte für interne und externe Mitarbeiter, das Identity Access Management (IAM), beschäftigt bei großen Unternehmen mit mehr als 10.000 Mitarbeitern gerne einmal 150 Personen – diese Gruppe kümmert sich im Prinzip um nichts anderes als die Veränderungen von Rechten. Wenn bei internationalen Unternehmen mehr als 1.000 verschiedene Systeme im Einsatz sind, führt die Veränderung eines Mitarbeiters (On-Boarding, Off-Boarding, Positionsänderung) sofort zu unzähligen Aktionen. Entsprechend haben sich verschiedene Administrationskonzepte herausgebildet, um den Anforderungen Herr zu werden. Die aktuelle **IDG-Studie zum Thema Identity- & Access-Management von 2017** [1] zeigt, dass sich noch kein Konzept durchgesetzt hat, die meisten Unternehmen aber rollen- oder attributbasierte Systeme einsetzen. Dies setzt aber voraus, dass die Rollen- und Attributdefinitionen stets aktuell sind und zu den Zugriffsherausforderungen passen. Ob ein Kunde heute eine Hotline anruft, morgen das Online-Service-Angebot nutzt oder

Welche Administrationskonzepte nutzen Sie in Ihrem IAM?

Mehrfachnennungen möglich. Angaben in Prozent. Basis: n = 146 (Filter: Nur Unternehmen mit softwaregestütztem Identity- & Access-Management) **Quelle: IDG-Studie zum Thema Identity- & Access-Management von 2017** [1]



1 https://timetoact-group.de/wp-content/uploads/IAM-Studie_2017_TIMETOACT_IDG.pdf

nächste Woche in eine Filiale geht: Alle Mitarbeiter, die ihn betreuen, brauchen die gleichen Rechte, aber eben auch nur solche, die wirklich notwendig sind – unabhängig von der Art des Kontakts („Touchpoint“) mit dem Kunden.

Das Mitarbeiter-Risiko ist hoch

Von den Administratoren werden Mitarbeitern gerne zu viele Rechte zugestanden, weil es das Identity- und Access-Management vereinfacht. So werden gerne die Rechte einer Person (mit allen Sonderrechten) für einen neuen Kollegen kopiert. Später weiß niemand mehr, warum eine Person eigentlich genau diese Rechte besitzt, sie werden nur noch “additiv” (mit den Sonderrechten) vergeben. Das schönste Beispiel ist deshalb der Azubi, der bei seinem Gang durch die unterschiedlichen Stationen des Unternehmens immer mehr Rechte ansammelt und nach seiner Ausbildung mehr Rechte als alle anderen hat. Das kann sich schnell rächen und zu Katastrophen wie bei der Société Général 2008 [2] ausweiten, die ein ähnliches Vorgehen letztlich 5 Mrd. Euro gekostet hat.

Aber auch schon regelmäßige Kontrollen, wie im Bankensektor die Kontrollen der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) [3] können im schlimmsten Fall zum Verlust der Banklizenz führen. Angesicht der Vielfalt der Systeme und Menge an Mitarbeitern ein zwar nicht wahrscheinliches, aber auch nicht völlig aus der Luft gegriffenes Szenario. Und letztlich ist der CEO der Bank auch strafrechtlich verantwortlich für die Sicherheit. Neben diesen Aspekten hinden komplexe Rechte-Management-Prozesse Unternehmen auch daran, die digitale Transformation zügig voranzutreiben. Wenn es bis zu einem Jahr dauern kann, bis ein Mitarbeiter alle notwendigen Rechte erhält, kann er nicht effizient arbeiten und seine Arbeitskraft nicht voll einbringen. Das be- und verstärkt oft die Schatten-IT.

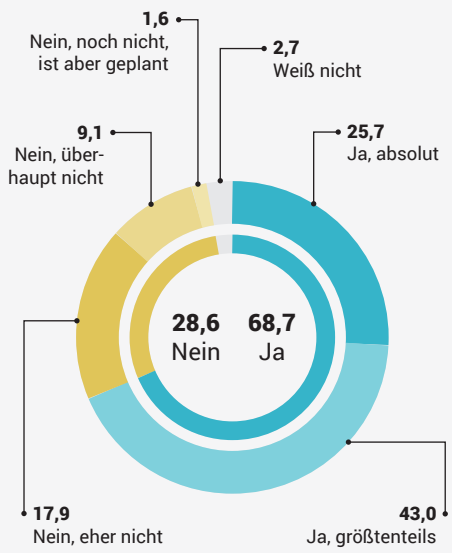
Bisherige Lösungsansätze

Die meisten IAM-Systeme haben einen rollenbasierten Ansatz. Jedem Mitarbeiter werden dabei eine oder mehrere Zugriffsrechte-Sets (die „Rollen“) zugewiesen, die ihren Aufgaben und Tätigkeiten entsprechen. Für jede Rolle ist genau festgelegt, welche Rechte ein Mitarbeiter bekommt und welche ihm verwehrt werden. Da Mitarbeiter oft mehrere Aufgaben haben und verschiedene Rollen einnehmen, muss man ihnen oft auch mehrere Rollen zuweisen. Hierbei können Rechteüberschneidungen entstehen, die sich manchmal nicht auflösen lassen oder zu Zugriffen führen, die ein großes Risiko erzeugen (toxische Kombinationen).

Es führt jedoch auch dazu, dass Mitarbeiter zusätzlich Einzelrechte (gern „Sonder-

Ist in Ihrem Unternehmen die Rolle eines jeden Mitarbeiters so genau definiert, dass sich daraus alle Zugänge oder Zugriffsberechtigungen eindeutig ableiten lassen?

Basis: n = 374 (Quelle: DG-Studie zum Thema Identity- & Access-Management von 2017 [1])



2 http://www.faz.net/aktuell/wirtschaft/unternehmen/societe-generale-kleiner-haendler-grosser-betrug-1293718.html
3 https://www.bafin.de/DE/Startseite/startseite_node.html

locken“ genannt) erteilt bekommen. Nicht selten werden dabei in einer einzelnen Rolle bis zu 50 IT-Rechte kombiniert (die oft total unerheblich sind). Warum ein Mitarbeiter ein Recht hat, lässt sich später kaum noch nachvollziehen. Ändert man dann die zugrundeliegende Technologie (etwa von Microsoft Sharepoint auf Atlasian Confluence) müssen sämtliche Rollen angepasst werden – was einen erheblichen Aufwand erzeugt.

Hinzu kommt, dass die Rollendefinitionen stets überprüft und aktuellen Anforderungen angepasst werden müssen. Die IT-Mitarbeiter müssen aufpassen, dass sie dabei keine Fehler machen und Mitarbeitern nicht zu viele Freiheiten erlauben. Vielfach ist es schon schwierig, die passenden Rollen für Mitarbeiter zu finden und zu entscheiden, welche Rollen zugewiesen werden sollen. Dies muss dann noch von Berechtigten und Vorgesetzten freigegeben werden. All das erzeugt eine hohe Komplexität, die zwangsläufig auch zu Fehlern führt.

Die genannte IDG-Studie zeigt hierbei, dass es bisher nur einem Viertel aller befragten Unternehmen (25,7 %) gelungen ist, alle Rollen exakt zu definieren. Gerade das letzte Quäntchen Genauigkeit ist aber bei Banken besonders wichtig, um 100 % Sicherheit zu gewährleisten. Bisherige rollenbasierte Administrationskonzepte stoßen daher zwangsläufig an Grenzen, wenn die Komplexität zu groß wird.

Mit MIRA reduzieren Sie den administrativen Aufwand auf ein Minimum und sparen bis zu 20 % der Kosten in Ihrem IAM-Team.

Dr. Amir Alsbih,
CEO von KeyIdentity

Die Probleme rollenbasierter IAM-Lösungen sind schon länger bekannt und haben daher zur Entwicklung alternativer Ansätzen geführt, wie die Attribut Based Access Control (ABAC). Statt statischer Tabellen, wie sie bei Rollen-Rechte-Vergabetechniken typisch sind, kommen dynamische Attribute zum Einsatz, mit deren Hilfe im jeweiligen Fall entschieden wird, ob ein Zugriff erlaubt ist. Wenn beispielsweise ein Login zuerst aus Deutschland und eine Minute später aus den USA erfolgt, kann etwas nicht stimmen. Solche Methoden werden oft mit Rollensystemen kombiniert, um eine feinere Steuerung zu erlauben, ohne das Rollensystem ausufern zu lassen.

Doch auch diese Systeme lösen das Kernproblem nicht: die Komplexität zu begrenzen und das IAM deutlich zu vereinfachen, um damit die Kosten und den Aufwand zu senken und das Unternehmen fit für schnelle Änderungen der digitalen Transformation zu machen.

Ein neuer radikaler und effizienter Ansatz

KeyIdentity hat sich als Partner von Banken, Versicherungen sowie von Institutionen aus dem Gesundheitssektor und der Industrie das Ziel gesetzt, die vielen komplexen Probleme bei IAM mit einem radikalen Ansatz völlig neu anzugehen und zu lösen. Die neue User-Access-Governance-Lösung wurde auf der itsa 2018 in Nürnberg vorgestellt: MIRA.

Ziel der Entwicklung war ein einfaches und verständliches Modell, das beschreibt, weshalb ein Benutzer bestimmte Zugriffsrechte hat und somit Transparenz für Geschäftsführer und IT-Experten schafft.

Man muss kein Genie sein, um zu erkennen, dass bei über 2.700 IAM-Rollen und weniger als 100 unterschiedliche Stellenbezeichnungen etwas fundamental im Argen liegen muss. CEOs haben damit das Gefühl, auf einem nicht beherrschbaren Pulverfass zu sitzen. Die KeyIdentity-Lösung basiert deshalb nicht auf einem Rollen-Rechte-System und gibt Entscheidungsträgern und Technikern wieder die Möglichkeit, sich vollständig auf ihre regulären Aufgaben zu fokussieren.

Die Vorteile der neuen User-Access-Governance-Lösung sind:

» **Transparenz:** Die Begründung für den Zugriff ist in den Zugriff selbst eingebettet, was durch den neuartigen Ansatz (Modell) möglich wird.

» **Skalierbarkeit:** Das Hinzufügen weiterer Assets, Benutzern oder Rollen wirkt sich nicht auf die Komplexität aus. Das macht die Nutzung wesentlich effizienter.

» **Flexibilität**: In Unternehmen arbeiten Personen in verschiedenen formalen und virtuellen Teams. Das KeyIdentity-Modell unterstützt das und ermöglicht somit eine echte Agilität.

» **Automatisierung:** Ein einziges Modell, das geschäftliche Vorgänge von der Technologie-Implementierung trennt, kann durch einen einzigen Prozess verwaltet werden. Das ermöglicht einen wesentlich höheren Automatisierungsgrad in allen IAM-Bereichen.

» **Kosteneffizienz:** Ein nachhaltig geringer Aufwand bei Implementierung und Betrieb für alle Benutzergruppen (IT-Admins, Support, Endnutzer, Externe).

» **Minimalisierung:** Ein sicheres Konzept der minimalen Berechtigungen, der Trennung von Aufgaben und Prozesse innerhalb des Unternehmens.

» **Einfachheit:** Extrem anwenderfreundliche Berechtigungszertifizierungen, die keine lange Einarbeitung erfordern.

Die Vorteile von MIRA zeigen sich an vielen Stellen: Es erfordert keine ausgefeilte und ausdefinierte Rollen-Rechte-Struktur und erleichtert damit, Veränderungen in der Unternehmensstruktur schnell und effizient umzusetzen. Damit unterstützt es die digitale Transformation, auch wenn in der Bank aktuell viele Anwendungssysteme im Einsatz sind.

Neue Mitarbeiter haben sehr schnell (meist in wenigen Tagen) kompletten Zugriff auf alle Systeme, die sie für ihre Aufgaben benötigen. Außerdem kann die Anzahl der Mitarbeiter, die in der IT nur mit dem Identity Access Management beschäftigt sind, radikal gesenkt werden. Diese stehen damit für andere, dringend anstehende Projekte zur Verfügung, um das Unternehmen fit für die Zukunft zu machen.

Die neue User-Access-Governance-Lösung unterstützt bis zu 80 % aller IT-Systeme, die große Unternehmen typischerweise im Einsatz haben, und senkt die Kosten im Bereich IAM um bis zu 20 %.

Fazit

Bei hoher Komplexität bei der Rechtevergabe für verschiedene Anwendungen können Rollen-Rechte-Konzepte und -Techniken den aktuellen Ansprüchen nicht mehr genügen. Sie erhöhen das Risiko von Fehlern und ermöglichen den Missbrauch, was gerade bei Banken nicht tolerierbar ist – gerade auch unter strafrechtlichen Gesichtspunkten.

Moderne User-Access-Governance-Lösungen wie MIRA sorgen dagegen nicht nur für die notwendige Sicherheit, sondern begeistern auch durch ihre Einfachheit und Effizienz. Sie erlauben es, das Unternehmen fit für die digitale Transformation zu machen und reduzieren darüber hinaus sowohl die Zeiten für die Rechtevergabe als auch die Personalkosten in der IT drastisch.

KeyIdentity GmbH

Das 2002 als LSE gegründete Unternehmen mit Sitz im hessischen Weiterstadt firmiert seit 2016 als KeyIdentity GmbH und ist eine 100%ige Tochter der MAX21 AG. CEO Dr. Amir Alsbih entwickelt zusammen mit seinem Team effiziente Lösungen, um digitale Identitäten und Transaktionen auf allen Ebenen mittels Multi-Faktor-Authentifizierung zu schützen. Mit einem semantisch neuen, nichttechnokratischen Ansatz im IAM-Segment revolutioniert KeyIdentity die Vergabe und Verwaltung von Zugriffsrechten in großen Unternehmen. KeyIdentity ist im „Gartner Market Guide for User Authentication" gelistet und gewann den Outstanding Security Performance Award. Für seine IAM-Lösung bekam das Team auf den IT-Awards 2018 den Security-Insider Readers' Choice Award.

Die IAM-Lösungen von KeyIdentity werden ausschließlich in Deutschland entwickelt und bereitgestellt und erfüllen höchste Sicherheitsstandards nach deutschem Recht. KeyIdentity gehört seit 2002 zur Initiative **„Security made in Germany"**.

KEYIDENTITY

WE SECURE IDENTITIES

Sie wollen mehr erfahren?
Dann nehmen Sie Kontakt mit uns auf:

https://www.keyidentity.com

Telefon: +49 6151 86086277

E-Mail: info@keyidentity.com