IDENTITY MANAGEMENT IN DER ÖFFENTLICHEN VERWALTUNG

Seit in der Bankenkrise Millionenbeträge durch unautorisierte Transaktionen vernichtet wurden, ist Identity und Access Management (IAM) in der Finanzbranche Chefsache. Unter dem Druck der Wirtschaftsprüfer sind in den vergangenen Jahren leistungsfähige Regelwerke und Lösungen entstanden. Die öffentliche Verwaltung kann davon nun profitieren.

| von ANDREAS RAQUET

IM KLEINEN EINFACH ...

Benutzer- und Berechtigungssysteme sind integraler Bestandteil betrieblicher Informationssysteme. Den meisten liegt ein Rollenmodell zugrunde (RBAC – Role Based Access Control). Die Theorie dahinter ist gut verstanden und entsprechende Systeme sind leicht zu administrieren – zumindest, solange man nur ein einzelnes System betrachtet. Tritt man einen Schritt zurück und betrachtet die gesamte IT eines Unternehmens oder einer Behörde, sieht das ganz anders aus. Hier gilt es, mehrere Hundert Fachverfahren mit Tausenden von Benutzern zu verwalten. Die Anzahl einzelner Berechtigungen und Berechtigungsvergaben geht leicht in die Millionen. Die daraus entstehende Komplexität ist nicht mehr ohne Weiteres zu beherrschen.

Die Konsequenz: Bei der Administration passieren Fehler, die über Jahre unerkannt bleiben können. Einen Gesamtüberblick über die Rechte eines Benutzers zu bekommen, ist aufwendig und in vielen Fällen nahezu unmöglich.

... IM GROSSEN SCHWER

Dass dies nicht nur ein theoretisches Problem ist, hat sich spätestens in der Bankenkrise gezeigt. In den Jahren 2008 bis 2010 wurden etliche Fälle bekannt, in denen Mitarbeiter renommierter Großbanken Beträge in Milliardenhöhe durch riskante Geschäfte vernichtet haben. Beispielsweise wird der Junior-Trader Jérôme Kerviel alleine für einen Verlust von 4,9 Mrd. Euro verantwortlich gemacht.[1] Ungeachtet der in der Öffentlichkeit diskutierten moralischen Fragestellungen ist klar: Die betroffenen Mitarbeiter hätten niemals die Rechte haben dürfen, solche Geschäfte überhaupt zu tätigen.

Die Sicherheitsexperten haben das Problem erkannt und reagiert: Bereits seit Jahren unternimmt die Finanzbranche erhebliche Anstrengungen, die Kontrolle über die Berechtigungsvergabe in der IT zurückzuerlangen. Mittlerweile sind für diese Aufgabe leistungsfähige Systeme, sogenannte Identity-and-Access-Management-Systeme (IAM), und sich darauf abstützende

1 http://www.nytimes.com/2008/01/25/business/worldbusiness/25bank.html

Kontrollprozesse (Access Governance) entstanden. Diese Systeme sind inzwischen mehrfach implementiert, haben die Kinderkrankheiten überstanden und sind somit reif für den Einsatz in der Breite – auch in der öffentlichen Verwaltung.

KONTROLLE DURCH ZENTRALISIERUNG

Die Kernidee der Systeme und Prozesse ist dabei immer dieselbe: Die gesamte Berechtigungsstruktur der IT wird in einem zentralen Modell konsolidiert. Dieses wird um fachliche Regeln ergänzt – mit dem Ziel, Risiken durch die strukturierte Vergabe von Rechten zu minimieren. Die Regeln entstammen letztlich dem Information-Security-Management-System (ISMS[2]) des Unternehmens, im Behördenumfeld also in der Regel dem IT-Grundschutz. Sind alle Berechtigungen in dieses Modell überführt, können beispielsweise die Rechte eines Benutzers über die gesamte IT einfach aus diesem abgerufen werden. Neu zu vergebende Rechte können zuvor gegen die Regeln des Modells geprüft werden.

Das IAM ist dabei mehr als nur eine zentrale Berechtigungsdatenbank. Vielmehr geht es darum, alle Prozesse des Identitäts- und Access-Managements so weit wie möglich zu standardisieren und zu automatisieren.

Das beginnt bereits bei der automatischen Anlage von Benutzerkonten mit einem Basissatz an Berechtigungen, sobald ein neuer Beschäftigter im Personalsystem erfasst wird. Neue Berechtigungen werden über ein zentrales Antragsverfahren gesteuert und über ein Provisionierungssystem direkt in den Zielsystemen umgesetzt. Über flexible Berichtsfunktionen – am besten risikobasiert – werden Analysen ermöglicht, die zu einer Verbesserung der Gesamtsicherheitslage in der Behörde im Rahmen eines KVP (kontinuierlicher Verbesserungsprozess) beitragen können. Schließlich können auch regelmäßige Rezertifizierungen[3] der fachlichen Rechtevergabe über das System gesteuert werden.

KOMPLEXITÄT DURCH ABSTRAKTION BEHERRSCHEN

Dreh- und Angelpunkt für die genannten Funktionalitäten ist das zentrale Rollen- und Prozessmodell. Aber ist es überhaupt möglich, Hunderttausende von unterschiedlichen Berechtigungen in einem gemeinsamen Modell praxisnah und zur Laufzeit auswertbar abzubilden? Die Antwort lautet mittlerweile „ja“. Möglich wird das durch eine mehrstufige Abstraktion.

Die meisten IAM-Systeme setzen im Kern ein hierarchisches Rollenmodell um (HRBAC – Hierarchical Role Based Access Control). Die Berechtigungssysteme der anzusteuernden IT-Systeme werden dabei durch Rollen niedriger Abstraktion abgebildet (oft technische Rollen oder alternativ auch Systemrollen genannt) und dann über mehrere Hierarchieebenen zu Rollen höherer Abstraktion (auch fachliche Rollen genannt) gebündelt. Die Verwal-

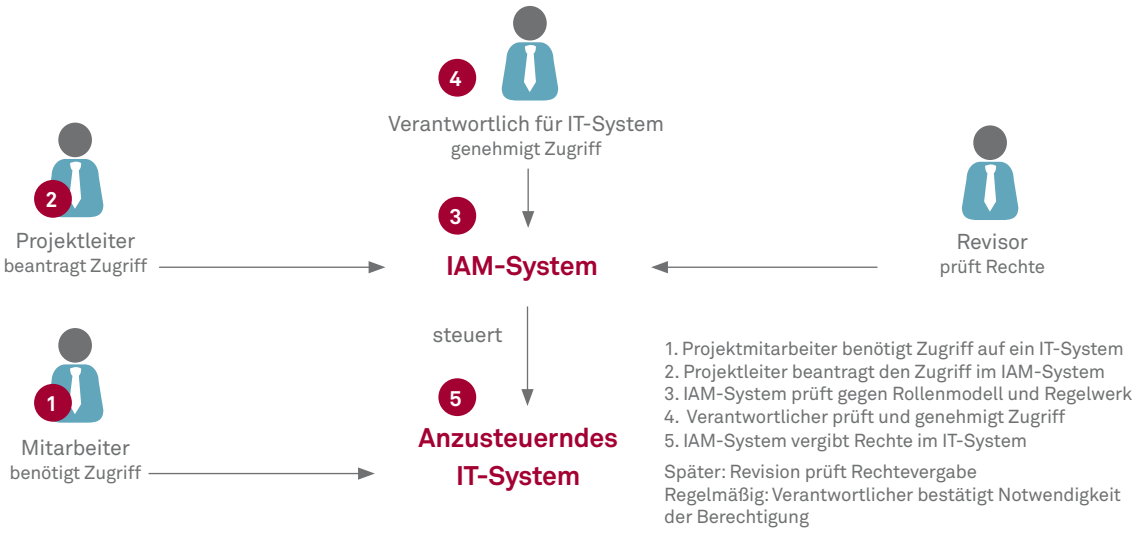

Abbildung 1: Berechtigungsvergabe über ein IAM System

2 Siehe ISO/IEC 27001
3 Regelmäßige Überprüfung der Berechtigungen eines Benutzerkreises

tung der Rollen erfolgt bevorzugt auf der Ebene der fachlichen Rollen, die Umsetzung auf der Ebene der technischen Rollen. Einige IAM-Systeme bieten auch parametrisierbare Rollen oder ergänzen das Rollenmodell durch attributbasierte Berechtigungen (ABAC – Attribute Based Access Control). Bei geeigneter Abstraktion lässt sich mittels eines überschaubaren Satzes an fachlichen Rollen ein Großteil der Berechtigungsvergabe abbilden. Der Rest kann durch Rollen niedrigerer Abstraktionsebene realisiert werden. In der Praxis hat sich eine Beschränkung der Rollenhierarchie auf drei Abstraktionsebenen bewährt.

KONSISTENZ DURCH EIN ZENTRALES REGELWERK

Auf Basis des Rollenmodells gilt es, die für die Rechtevergabe relevanten Vorgaben des ISMS in Form von Regeln umzusetzen. Im öffentlichen Sektor entspricht der Aufbau dem BSI-Grundschutz und dem damit verbundenen Grundschutzkatalog. Die Regeln basieren auf zwei Prinzipien:

Das **Prinzip der minimalen Rechte** (least privilege) nach dem Need-to-know-Grundsatz soll sicherstellen, dass Benutzer nur genau die Rechte besitzen, die sie für die Erfüllung ihrer beruflichen Aufgaben (Arbeitsplatz und Tätigkeitsbeschreibung) benötigen. Das heißt, es soll verhindert werden, dass Benutzer mehr Rechte besitzen, als sie für ihre Arbeit benötigen. Letzteres ist ein fachlicher Aspekt, den das Regelwerk des IAM-Systems nicht bewerten kann. Es kann jedoch die Kritikalität der Berechtigungen eines Benutzers auswerten und so transparent machen, ob ein Benutzer über besonders viele oder besonders kritische Rechte verfügt. Dazu wird jeder Rolle ein Risikowert zugeordnet und aus allen an einen Benutzer vergebenen Rollen ein kumulierter Risikowert berechnet.

Das **Prinzip der Funktionstrennung** (segregation of duties) soll verhindern, dass Benutzer besonders kritische Kombinationen von Berechtigungen erhalten. Gängig ist zum Beispiel das Verbot von gleichzeitig verfügbaren administrativen und fachlichen Berechtigungen in derselben Anwendung. Das Regelwerk kann solche gegenseitigen Ausschlüsse von zwei oder mehr Rollen direkt abbilden oder sie mit einem Risikowert belegen und analog zu den Rollenzuweisungen in den Gesamtrisikowert eines Benutzers miteinbeziehen.

Einmal etabliert, kann das Regelwerk verwendet werden, um bestehende Regelverstöße oder hohe Risiken präventiv zu erkennen und entsprechend gegenzusteuern, zum Beispiel, indem die Vergabe beantragter Rechte abgelehnt wird oder Ausnahmegenehmigungen eingeholt und regelmäßig erneuert werden.

KONTROLLE DURCHSETZEN

Mit dem Rollenmodell und dem darauf basierenden Regelwerk ist der fachliche Grundstein gelegt. Nun gilt es, dieses Regelwerk auch durchzusetzen.

Dazu werden zunächst die Berechtigungen auf den anzusteuernden Zielsystemen eingelesen und auf die Rollen des zentralen IAM-Modells abgebildet. Über das Berichtswesen (Reporting) können nun Regelverstöße oder auffällige Risikostrukturen erkannt und aufgelöst werden. Das kann durch Anpassung der Berechtigungen, aber auch durch das Einholen von Ausnahmegenehmigungen für bestimmte Regelverstöße erfolgen.

Ist dieser Schritt abgeschlossen, ist das Rollenmodell im IAM-System mit den Berechtigungsstrukturen in den anzusteuernden IT-Systemen konsistent und konform zum Regelsystem. Änderungen an den Berechtigungen werden von da an ausschließlich auf dem zentralen Rollenmodell durchgeführt. Erst danach werden die daraus resultierenden Rechte in den anzusteuernden IT-Systemen umgesetzt. Das IAM-System wird damit zum führenden System der Rechtevergabe für alle anzusteuernden IT-Systeme.

Der gesamte Prozess wird dabei so weit wie möglich automatisiert. Im einfachsten Fall kann die Vergabe einer Berechtigung vollautomatisch erfolgen. In der Regel sind zusätzlich manuelle Schritte erforderlich, sei es bei der Abwicklung des Antragsverfahrens oder bei der Umsetzung der Berechtigungen auf den anzusteuernden IT-Systemen. In dem Fall steuert das IAM-System den Workflow und hält die Bearbeitungshistorie nach.

Bei der Anbindung von Systemen an ein neu aufzusetzendes IAM empfiehlt es sich, schrittweise vorzugehen:

- Im ersten Schritt werden die besonders wichtigen IT-Systeme in der Behörde und im Personalsystem angebunden. So kann den größten Risiken bei einer noch überschaubaren Anzahl anzusteuernder Systeme entgegengewirkt werden.

- In weiteren Schritten werden sukzessive weniger wichtige Systeme angebunden und weitere Funktionalitäten (siehe Kasten „Weitere Funktionen eines IAM-Systems“) ergänzt.

FLEXIBILITÄT DURCH MODULARE ARCHITEKTUR

Als umfassendes System zur Steuerung von Benutzerkonten und Berechtigungen beinhaltet ein IAM-System eine Reihe von

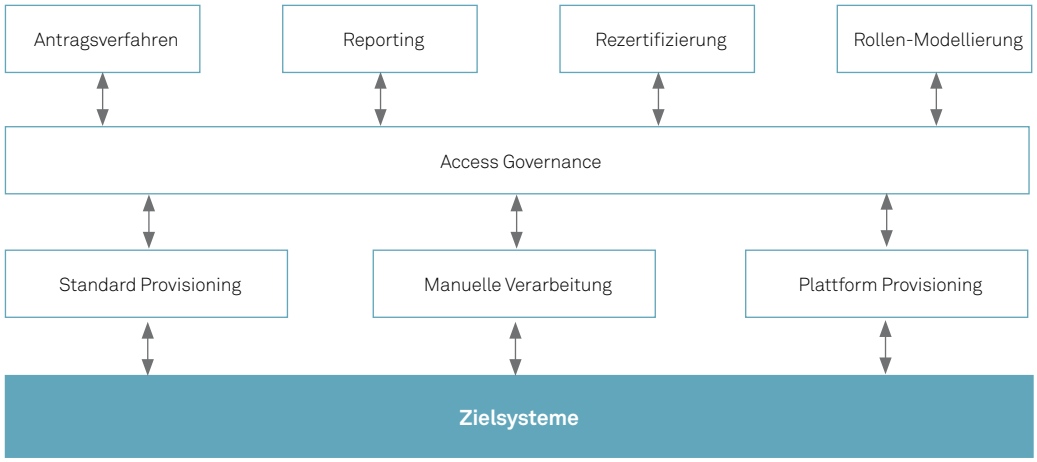

Abbildung 2: Typische Architektur eines IAM-Systems

Funktionalitäten, die zuvor durch dedizierte Systeme abgebildet wurden:

- Das Antragsverfahren (Ticketsystem) steuert die Antragsworkflows, die letztlich die Vergabe von Berechtigungen legitimieren.
- Das Provisionierungssystem steuert die Vergabe von Berechtigungen in einem oder mehreren Zielsystemen.
- Verzeichnisdienste verwalten die Berechtigungsdaten jeweils für eine technische Plattform.

Die meisten der am Markt verfügbaren IAM-Systeme einschlägiger Hersteller, wie z. B. Oracle, NetIQ oder Sailpoint, bringen diese Funktionen bereits mit. Häufig sind diese unterschiedlich gut ausgebaut. In der Regel sind IAM-Systeme aus einem der oben aufgeführten dedizierten Systeme hervorgegangen und in ihrer angestammten Domäne besonders stark. Andere Funktionalitäten sind oft zugekauft oder nur rudimentär umgesetzt.

Daher sollte bei der Einführung eines neuen IAM-Systems geprüft werden, welche bestehenden Funktionen bewährt sind und erhalten bleiben sollen. Diese können dann mit dem ausgewählten IAM-System integriert werden.

Den Kern in der typischen Architektur eines IAM-Systems bildet das zentrale Modell (vgl. Abbildung 2). Die Komponenten zur

Prozesse eines IAM-Systems

IAM-Systeme unterstützen die folgenden fachlichen Prozesse:

- **Operative Prozesse:**
  - Zuteilung von Berechtigungen
  - Abbildung der Genehmigungsworkflows bei der Berechtigungsvergabe auf Basis des Regelwerks
  - Umsetzung der zugeteilten Rollen auf den Zielsystemen
  - Eventuell Entzug der Berechtigungen
- **Analytische Prozesse:**
  - Analyse und Bewertung der Berechtigungsstrukturen
  - Kennzahlen zum Gesamtzustand der Berechtigungsvergabe
  - Risikoanalyse
- **Modellierungsprozesse:**
  - Definition von Rollen und Regeln
- **(Re-)Zertifizierungsprozesse:**
  - Überprüfung fachlicher Berechtigungen

Alle diese Prozesse arbeiten auf einem gemeinsamen Rollenmodell und einem gemeinsamen Prozess und Regelwerk.

Weitere Funktionen eines IAM-Systems

Viele der IAM-Systeme und IAM-Suiten am Markt bieten weitergehende Funktionalitäten. Dazu zählen:

- **Zentrale Passwortverwaltung** und Abbildung der Password Security Policy
- **Single Sign-On und Webaccess** – zentrale Anmeldung und Zugriffssteuerung auf Webanwendungen, vorwiegend auf SAML-Basis[1]
- **Privileged Account und Access Management** – Beschränkung der Zugriffsrechte privilegierter Benutzer (z. B. root) und Protokollierung administrativer Tätigkeiten
- **Cloud Security & Federation** – Erweiterung des Identitätsmanagements um extern verwaltete Identitäten/Rechte, z. B. Facebook-Log-on
- **Support von BYOD** (Bring Your Own Device) – die Benutzung und Verwendung von eigenen, in das Unternehmen eingebrachten mobilen Gerätschaften mit gleichzeitiger Verwendung von privaten Daten und Firmendaten beim Zugriff auf die Unternehmensinfrastruktur (Mobile Access)

Pflege des Modells (Modellierung) und zu dessen Auswertung (Reporting) sind eng mit dem Kern gekoppelt. Alle anderen Komponenten benötigen nur eine lose Kopplung und können ausgetauscht werden – sofern das IAM-System seine Schnittstellen offenlegt und die zu integrierenden Systeme entsprechende Möglichkeiten bieten. In modernen IAM-Systemen, wie zum Beispiel Sailpoint IdentityIQ, ist das in der Regel der Fall.

Im Bereich der Provisionierung sind in komplexen Unternehmensstrukturen häufig mehrere Systemlandschaften mit verschiedenen Anforderungen anzutreffen. Zum einen werden für bestimmte Plattformen eigene Provisionierungssysteme benötigt (zum Beispiel SAP Netweaver IDM), zum anderen gibt es Systeme, die nicht automatisiert anzusteuern sind. Das trifft insbesondere auf moderne Cloud-Dienste zu. In diesen Fällen kann beispielsweise ein übergreifendes Workflowsystem an die Stelle des Provisionierungssystems treten.

FAZIT

Die zentrale Steuerung von Berechtigungen ist in großen IT-Organisationen nicht mehr ohne Unterstützung einer übergreifenden Softwarelösung möglich. In den letzten Jahren wurden leistungsfähige Systeme entwickelt, die nahezu alle Funktionalitäten eines modernen Identity Managements abbilden. Im Kern der Systeme steht ein zentrales Rollen- und Prozessmodell. Die zu steuernden Berechtigungen der Zielsysteme müssen auf dieses Modell abbildbar sein. Daher ist die Mächtigkeit und Flexibilität des Modells von entscheidender Bedeutung.

Darauf basierend werden die im Kasten „Prozesse eines IAM-Systems“ zusammengefassten Funktionalitäten von modernen IAM-Systemen mitgeliefert. Alternativ können bestehende Komponenten integriert werden, die häufig leistungsfähiger sind. Ob sich der Aufwand gegenüber der Nutzung der bereits integrierten Funktionalität lohnt, muss im Einzelfall evaluiert und entschieden werden. ●

ANSPRECHPARTNER – ANDREAS RAQUET
Lead IT-Consultant
Public Sector
- +49 711 94958-693
- andreas.raquet@msg-systems.com