Auf der sicheren Seite

Wirkungsvoller Zugriffsschutz (Teil I)

von Martin Mertens

Im Januar 2008 erlitt die zweitgrößte französische Bank, die Société Générale, einen Verlust von knapp 4,9 Mrd. Euro. Das Ereignis erregte großes internationales Aufsehen, denn der Verlust war die Folge spekulativer Aktionen eines einzigen Händlers.

Nachträgliche Untersuchungen haben ergeben, dass unter anderem

- unterlassene regelmäßige Prüfungen der eingeräumten IT-Zugriffsrechte sowie
- die mangelnde Implementierung der sogenannten Funktionstrennung (Segregation of Duties – SoD)

in der Bank diese Spekulationsgeschäfte ermöglicht hatten.

Die periodische Prüfung der Zugriffsrechte gegen die fachlichen Aufgaben (Rezertifizierung) und die Implementierung der SoD sind unverzichtbare Bestandteile eines wirkungsvollen Zugriffsschutzes (Identity & Access Management – IAM). Kein Wunder, dass BaFin und Bundesbank das IAM unter den IT-Prüfungsthemen an prominenter Stelle führen. In diesem Artikel werden die Grundlagen des IAM beleuchtet. In den nächsten Ausgaben der msgGillardon NEWS folgen Artikel zu zentralen weiterführenden Themen.

IAM: Modellierung der Zugriffsrealität

Das IAM einer Organisation hat die Aufgabe, berechtigten Zugriff auf die zu schützenden IT-Systeme und damit auf die dort gespeicherten Daten der Organisation zu gewährleisten und unberechtigten Zugriff darauf zu verhindern.

Zu diesem Zweck wird ein Modell der realen Welt verwendet: In der realen Welt greifen Nutzer (zum Beispiel Marianne Mustermann) auf IT-Systeme (zum Beispiel ein ERP-System) zu, indem sie sich dort mit einer Kennung (zum Beispiel muster) anmelden. Die Kennung ist mit einem oder mehreren (Zugriffs-)Recht(en) ausgestattet – sie gehört beispielsweise zu einer Active Directory-Gruppe, deren Mitglieder bestimmte Transaktionen durchführen dürfen.

Jeder Nutzer wird im IAM-Modell durch eine sogenannte digitale Identität abgebildet. Diese besteht im Wesentlichen aus Stammdaten des Nutzers, die eine eindeutige Identifizierung ermöglichen und die für die Verwaltung der Berechtigungen nötig sind.

Die Verwaltung digitaler Identitäten ist Gegenstand des Identity Managements. Hier ist das IAM-Modell deskriptiv, indem es die Realität nachbildet.

Eine Kennung auf einem IT-System wird im IAM-Modell durch ein Konto abgebildet, die Rechte auf dem IT-System durch Berechtigungen. Ein Konto ist also eine Struktur zur Aufnahme von Berechtigungen. Einem Konto können auch mehrere Kennungen zugeordnet sein.

Die Verwaltung von Konten und Berechtigungen ist Gegenstand des Access Managements. Hier ist das IAM-Modell präskriptiv: Erst werden Konten eingerichtet und Berechtigungen darauf gesammelt („gebucht“), dann werden die zugehörigen Kennungen auf den Ziel-IT-Systemen eingerichtet und mit Rechten ausge-

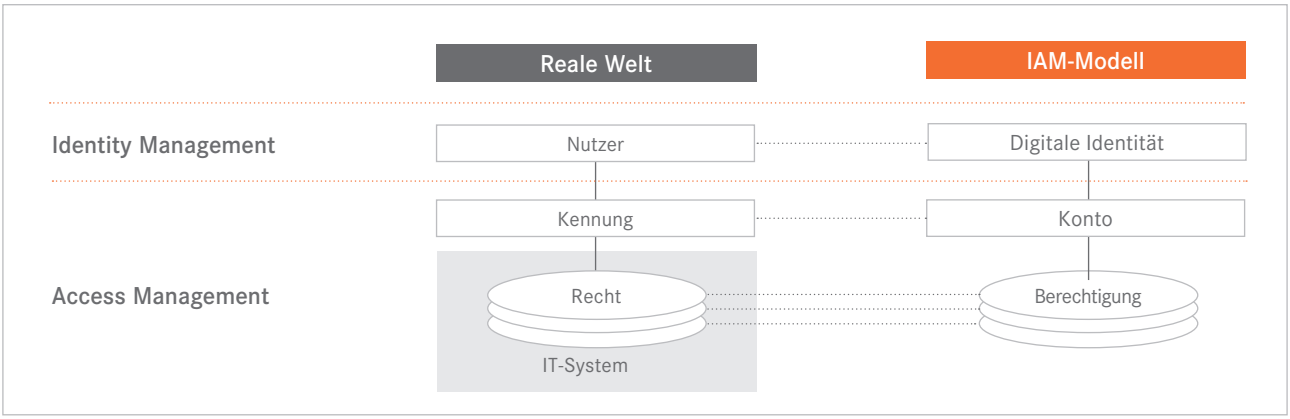

Abbildung 1: Das IAM-Modell der Zugriffsrealität (vereinfacht)

stattet; andernfalls kann das IAM seine Funktion nicht erfüllen. Ausnahmen sind Systeme beziehungsweise Umgebungen, die nicht unter IAM-Kontrolle stehen müssen (zum Beispiel abgeschottete Schulungsumgebungen mit fiktiven Daten) und Systemkennungen, die nach der Installation eines IT-Systems bereits vorhanden sind.

IAM: Plattform

Unsere Erfahrung zeigt, dass bereits in kleineren Finanzinstituten die Durchführung des IAM mit Bordmitteln (Spreadsheets und selbst gebaute Applikationen) problematisch ist. Daher empfehlen unter anderem auch die BSI-Grundschutzkataloge die Verwendung dedizierter Werkzeuge (M 2.586). Ein solches Werkzeug heißt IAM-System oder Provisionierungssystem.

IAM: Zentrale Prozesse

Die wichtigsten Prozesse im IAM sind:

Übermittlung von Stammdaten und Zuweisung von Standardrechten:
Über eine Schnittstelle zum HR-System der Organisation werden die nötigen Stammdaten ins IAM-System übertragen; der Eintritt einer Mitarbeiterin oder eines Mitarbeiters in eine Organisationseinheit löst die Zuweisung von Standardrechten aus.

Beantragung und Genehmigung von Berechtigungen:
Jede über die Standardrechte hinausgehende Berechtigung wird über einen Workflow des IAM-Systems beantragt und sowohl dem Vorgesetzten des Empfängers als auch dem für die Berechtigung fachlich Verantwortlichen zur Genehmigung vorgelegt.

Deaktivierung von Konten und Entzug von Berechtigungen:
Scheidet ein Nutzer aus einer Organisationseinheit oder der Organisation aus, so werden seine zugehörigen Konten deaktiviert und die entsprechenden Berechtigungen entzogen.

Provisionierung (Enforcement) von Konten und Berechtigungen:
Für die Konten im IAM-System werden die zugehörigen Kennungen in den Zielsystemen eingerichtet und mit denjenigen Rechten ausgestattet, die den Berechtigungen entsprechen. Analog auch der Rechteentzug bei Berechtigungsentzug.

Rezertifizierung:
Es wird periodisch geprüft, ob die gewährten Zugriffsrechte dem Aufgabenbereich der Person angemessen sind (Minimalitätsprinzip).

Ansprechpartner

Martin Mertens
Principal IT Consultant
> martin.mertens@msg-gillardon.de