Martin Mertens

Auf der sicheren Seite: Wirkungsvoller Zugriffsschutz (Teil II)

Im Fokus dieses Artikels stehen zwei wesentliche Disziplinen innerhalb des IAM: die Funktionstrennung (Segregation of Duties – SoD) und ein fachliches Rollenmodell als Grundlage des Zugriffsschutzes (Role Based Access Control – RBAC).

Nachdem im ersten Teil (vgl. NEWS 03/2017) unserer Serie über wirkungsvollen Zugriffsschutz (Identity & Access Management – IAM) das IAM als ein Modell der Zugriffsrealität vorgestellt, das nötige zentrale Provisionierungssystem gestreift und die zentralen IAM-Prozesse beleuchtet wurden, werden im zweiten Teil zunächst die SoD, dann das RBAC und schließlich die enge Verbindung der beiden im IAM analysiert.

SOD: VERMEIDUNG TOXISCHER BERECHTIGUNGS-KOMBINATIONEN

In den MaRisk heißt es im Abschnitt AT 4.3.1 (Aufbau- und Ablauforganisation): „Bei der Ausgestaltung der Aufbau- und Ablauforganisation ist sicherzustellen, dass miteinander unvereinbare Tätigkeiten durch unterschiedliche Mitarbeiter durchgeführt und auch bei Arbeitsplatzwechseln Interessenkonflikte vermieden werden“. Außerdem erwähnt dieser Abschnitt das Verbot der Selbstprüfung und -überprüfung. Abschnitt BTO 1.1 (Funktionstrennung und Votierung) detailliert dies für die Trennung der Bereiche Markt und Marktfolge.

Kombinationen von Berechtigungen für miteinander unvereinbare Tätigkeiten werden – aufgrund der zum Teil hohen Risiken, die sie bergen – “toxisch“ genannt. Ein praxistauglicher Ansatz zur Vermeidung solcher Kombinationen besteht in der Festlegung sogenannter SoD-Trennkriterien. Man kann SoD-Trennkriterien als maximale Tätigkeitsbereiche auffassen, die vereinbar oder unvereinbar sein können. Sämtliche Tätigkeitskombinationen aus einer toxischen

SoD-Trennkriterien	Markt	Marktfolge	Handel	IT-Benutzer-management	IT-Berechtigungs-management
Markt					
Marktfolge	SoD-Regel 1				
Handel					
IT-Benutzer-management					
IT-Berechtigungs-management				SoD-Regel 2	

SoD-Regeln	Name	Eigner	Beschreibung	...
SoD-Regel 1	...	...	...	...
SoD-Regel 2	...	...	...	...
...	...	...	...	...

Abbildung 1: SoD-Regeln beschreiben toxische Kombinationen von SoD-Trennkriterien

Trennkriterienkombination sind dann selbst wieder toxisch. Die SoD-Trennkriterien werden in der sogenannten SoD-Matrix gegeneinander aufgetragen. Bilden zwei Trennkriterien eine toxische Kombination, wird der Schnittpunkt der entsprechenden Zeile und Spalte markiert und in einer sogenannten SoD-Regel beschrieben (vgl. schematische Darstellung in Abbildung 1).

Nach der Erstellung der SoD-Matrix und des SoD-Regelkatalogs werden den im Provisionierungssystem hinterlegten Berechtigungen gegebenenfalls SoD-Trennkriterien zugewiesen; Berechtigungen ohne Trennkriterium sind SoD-neutral. Anhand der zugewiesenen Trennkriterien und der SoD-Matrix können nun toxische Berechtigungskombinationen sofort identifiziert und damit vermieden werden.

RBAC: TRANSPARENZ UND EFFIZIENZ DURCH BERECHTIGUNGSBÜNDELUNG

Die Rollen eines RBAC kapseln die Einzelberechtigungen, indem diese nicht mehr direkt den Nutzerkonten zugewiesen werden, sondern den Rollen, die über die Konten den Nutzern zugeordnet sind. Während die MaRisk (AT 7.2, Tz. 2) die Etablierung eines Rollenmodells für die Berechtigungsvergabe zuläss („...; die Zusammenfassung von Berechtigungen in einem Rollenmodell ist möglich."), die ISO-Norm 27002 (Abschnitt 9.2.2) empfiehlt, ein solches zu erwägen („Consideration should be given to establishing user access roles based on business requirements that summarize a number of access rights into typical user access profiles."), fordern die BSI-Grundschutzkataloge ein Rollenmodell (M 2.30): »

» „Es sollte eine begrenzte Anzahl von Rechteprofilen festgelegt werden. Ein neuer Benutzer wird dann einem solchen Profil zugeordnet und erhält damit genau die für seine Tätigkeit erforderlichen Rechte."

» RBAC macht es leichter, das „Need-to-know"-Prinzip umzusetzen, gemäß dem jedes Mitglied der Organisation genau diejenigen Berechtigungen haben soll, die für den betreffenden Aufgabenbereich nötig sind. «

Der BSI-Text nennt bereits zwei der Vorteile, den ein fachliches Rollenmodell dem IAM bringt: Es ist leichter, einem neuen Träger einer Geschäftsrolle ein ganzes Berechtigungsprofil (im Sinne einer fachlichen Rolle = IAM-Fachrolle) zuzuweisen als sämtliche Einzelberechtigungen des Profils. Dies spart auch erheblichen administrativen und IT-Aufwand. RBAC macht es leichter, das „Need-to-know"-Prinzip umzusetzen, gemäß dem jedes Mitglied der Organisation genau diejenigen Berechtigungen haben soll, die für den betreffenden Aufgabenbereich nötig sind.

Weitere Vorteile von IAM-Fachrollen sind:

- Wie die Zuweisung wird auch der Entzug von Berechtigungen, zum Beispiel bei einem Wechsel des Aufgabenbereichs, durch ein RBAC stark vereinfacht.
- Wenn sich die Berechtigungen ändern, die für die Ausübung einer Geschäftsrolle nötig sind, geschieht dies nur an der IAM-Fachrolle und nicht an den Konten sämtlicher Rollenträger.
- Höhere Transparenz über die Zusammensetzung der Berechtigungen einer Person in der Organisation
- Die Rezertifizierung (periodische Prüfung der Angemessenheit der vergebenen Berechtigungen in Bezug auf die zu erledigenden Aufgaben) wird aufgrund der erhöhten Transparenz viel schneller und effizienter; ohne ein RBAC erfolgt hierbei häufig mangels Durchblick ein Durchwinken ohne (genauere) Prüfung.

Die Krux bei der Einführung eines RBAC ist der passende Zuschnitt der Rollen. In der Praxis hat sich ein Vorgehen in drei Schritten bewährt:

- Erstellung (falls noch nicht vorhanden) eines Inventars der für die Rollenbildung relevanten Applikationen; Ermittlung, welche Zugriffe es dort gibt und wer diese Zugriffe haben sollte (Sachbearbeiter, Administrator, Revisor etc.) mithilfe der Applikationsverantwortlichen

- Interviews mit den Führungskräften der Organisationseinheiten: Welche Applikationen, Laufwerke etc. benötigen die Aufgabenträger für die Erledigung ihrer Arbeit?

- Definition eines Katalogs fachlicher Rollen und Festlegung der zugehörigen Berechtigungen. Hier ist entscheidend, bewusst die Anzahl der Rollen und (bei Vererbung) der Schichten gering zu halten sowie Standards zu setzen und diese durchzusetzen.

SOD & RBAC: DURCHDRINGUNG BEI BERECHTIGUNGSVERGABE UND -BÜNDELUNG

Der Kommentar der Bundesanstalt für Finanzdienstleistungsaufsicht – BaFin – zur Teilziffer 2 von AT 7.2 (technisch-organisatorische Ausstattung) der MaRisk zeigt die Verschränkung von RBAC und SoD: „Insbesondere bei Berechtigungsvergaben im Rahmen von Rollenmodellen ist darauf zu achten, dass Funktionstrennungen beibehalten beziehungsweise Interessenkonflikte vermieden werden."

Diese Verschränkung betrifft zwei Aktivitäten:

1. Bei der Bündelung von Einzelberechtigungen (insbesondere zu IAM-Fachrollen), also bereits bei der Berechtigungserstellung, muss gewährleistet werden, dass keine toxischen Kombinationen verbaut werden. Dies lässt sich durch einen entsprechenden Mechanismus im Provisionierungssystem gewährleisten, der für die Aufnahme einer toxischen Kombination in ein Berechtigungsbündel per Workflow das Vorhandensein einer Ausnahmegenehmigung erzwingt.

2. Bei der Vergabe neuer Berechtigungen muss einerseits geprüft werden, ob die Gesamtheit der neuen Berechtigungen eine toxische Kombination enthält. Andererseits müssen die neuen Berechtigungen auch gegen die bereits gewährten Berechtigungen auf Toxizität hin geprüft werden. Auch hierbei ist eine Verletzung des SoD-Prinzips nur bei Vorliegen einer Ausnahmegenehmigung möglich.

Im Rahmen der Rezertifizierung werden auch die erteilten SoD-Ausnahmegenehmigungen periodisch überprüft. Berechtigungsbündel und Berechtigungsvergaben aus der Zeit vor der Implementierung der SoD werden im Nachhinein auf SoD-Verletzungen hin geprüft und gegebenenfalls bereinigt. ■

Ansprechpartner:

Martin Mertens
Principal IT Consultant,
Automobilbanken & Bausparkassen
martin.mertens@msg-gillardon.de

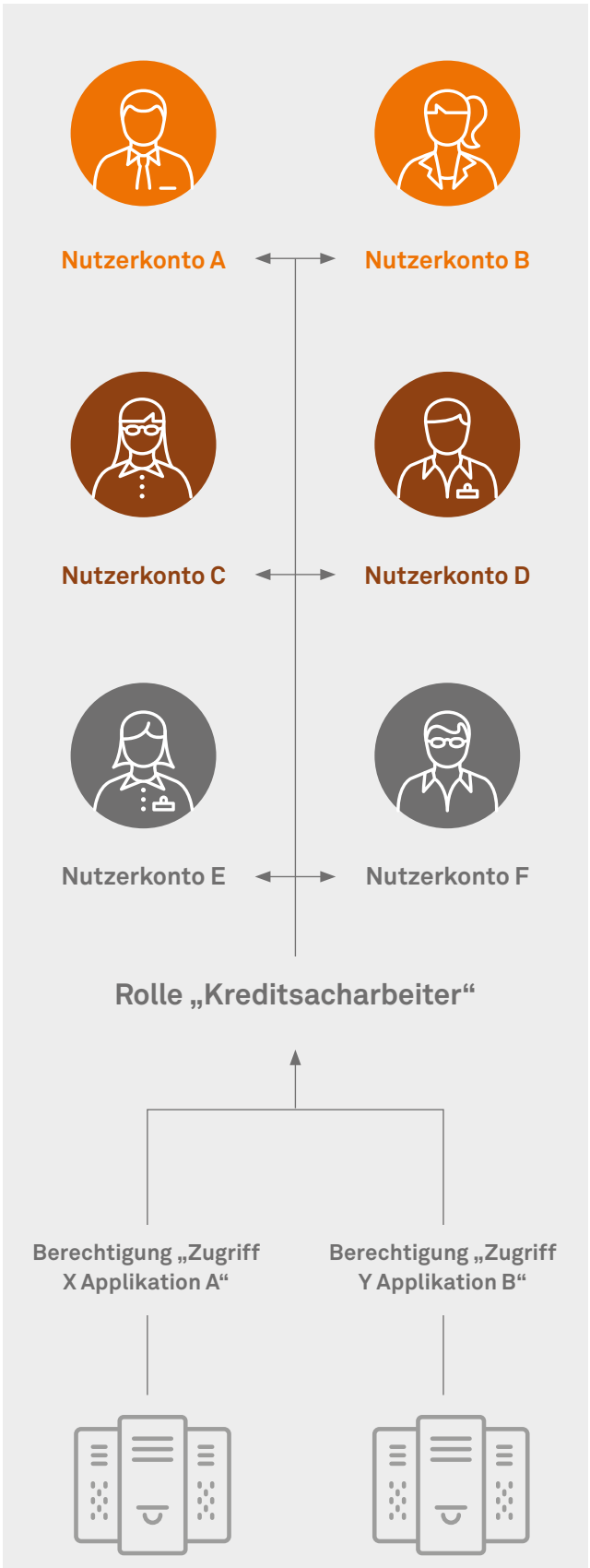

Abbildung 2: Berechtigungskapselung durch Einsatz eines RBAC