bm
bank und markt

53. Jahrgang | Fritz Knapp Verlag | die-digitale-bank.de

5

15. Mai 2024

DIE DIGITALE BANK

Digitaler Sonderdruck

Berechtigungsmanagement strategisch automatisieren

Von Olaf Pulwey

ZIELGRUPPENORIENTIERUNG

– Captives – Private Banking
– Barrierefreiheit – Finanzbildung

Berechtigungsmanagement strategisch automatisieren

Von Olaf Pulwey

Um die Integrität ihrer IT zu gewährleisten, hat die Bankenbranche einiges an Regulatorik zu beachten. Dazu gehört ein weitreichendes Berechtigungsmanagement um unberechtigten Zugang oder Zugriff auf Daten zu vermeiden. Diese Rechte müssen in regelmäßigem Turnus erneuert werden. Die Rezertifizierung ist also eine Daueraufgabe, die eine Automatisierung wiederkehrender Prüf- und Dokumentationsprozesse nahelegt, so Olaf Pulwey. Dann können zuvor definierte Soll-Ist und Soll-Soll-Abgleiche so abgewickelt werden, dass die Compliance-Verantwortlichen nur bei Auffälligkeiten eingreifen müssen. Red.

Kaum eine Branche ist so sehr auf die Integrität ihrer Informationstechnologie angewiesen wie das Bankwesen. Entsprechend hoch sind die Anforderungen an Datenschutz, Compliance und IT-Sicherheit. Um unberechtigten Zugriff oder Zutritt zu verhindern, muss ein entsprechend weitreichendes Berechtigungsmanagement etabliert werden. Spätestens bei der Rezertifizierung der vergebenen Rechte entsteht jedoch ein Arbeitsaufwand, der die Automatisierung der erforderlichen Prüf- und Dokumentationsprozesse nahelegt.

Gefahrenlage im Fokus

Konkret geht es um die Ausgestaltung, Dokumentation und Implementierung von Berechtigungen, die den Zugriff auf die unterschiedlichen Softwaresysteme und den Zutritt zur Infrastruktur – allen voran sensible Gebäudeteile oder Serverräume – verlässlich steuern. Dabei ist eine Vielzahl an regulatorischen Vorgaben zu erfüllen, die zum Teil noch durch betriebsspezifische Anforderungen ergänzt werden.

- Aufseiten der externen Regulatorik zählen die Bankaufsichtlichen Anforderungen an die IT (BAIT) und die Mindestanforderungen an das Risikomanagement (MaRisk) zum engeren Kreis der zu beachtenden Richtlinien.

- Mit dem Digital Operational Resilience Act (DORA) der EU kommt nun eine Richtlinie hinzu, die die IT-bezogenen Zugriffs- und Zutrittsrechte aus dem Blickwinkel der Cybersicherheit regelt. Mitte Januar 2025 soll die neue Verordnung auch in Deutschland in Kraft treten. Nach dem fristgerechten Abschluss der DORA-Konsultation im März dieses Jahres sieht derzeit alles danach aus, dass Brüssel den geplanten Starttermin halten wird. Anfang nächsten Jahres werden somit alle im Rechtsraum der EU tätigen Banken dazu aufgefordert sein, ihre aktuelle Praxis normkonform zu rezertifizieren.

Dauerthema Rezertifizierung

Doch ganz abgesehen von DORA besteht ohnehin ein fortwährender Bedarf zur Rezertifizierung der Rechtevergabe. Vor dem Hintergrund der sich permanent wandelnden Bedrohungsrisiken verlangen die verschiedenen Richtlinien turnusgemäße Überprüfungen. Je nach Richtlinie liegt der Rhythmus der erforderlichen Rezertifizierungen zwischen sechs Monaten und drei Jahren.

Abhängig von der Zahl der IT-Systeme, die unter die Richtlinien fallen, ergibt sich ein äußerst komplexes Geflecht an spezifischen Rezertifizierungsvorhaben, die es revisionssicher zu managen gilt. Dabei gilt es revisionssicher nachzuweisen, ob und inwiefern die gelebte Praxis mit den dokumentierten Pflichten übereinstimmt. Passen die vergebenen Berechtigungen, Rollen und Gruppenzugehörigkeiten auch weiterhin zu

Olaf Pulwey, CEO, FOCONIS AG, Vilshofen an der Donau

den Vorgaben der Regulatorik? Und vor allem: Passen sie zur aktuellen Gefahrenlage?

Revisionssichere Sollkonzepte

Um ein hohes Maß an Sicherheit zu schaffen, braucht es einen strategischen Ansatz. Ausgangspunkt der Rezertifizierung ist ein fundiertes Sollkonzept des Berechtigungsmanagements (englisch Identity & Access Management, IAM). Dessen Leitgedanke besteht darin, die Zugriffs- oder Zutrittsberechtigungen so zu vergeben, dass sie sich anhand der regulatorisch geforderten Dokumentationen nachvollziehen und im Kontrollfall bestätigen lassen. Ein solches Sollkonzept – und zwar für jede einzelne Software oder auch bei der Schlüsselvergabe zu erstellen und umzusetzen – liegt in der alleinigen Verantwortung der Kreditinstitute. Je nach IT-System erledigen sie die dazu erforderlichen Aufgaben komplett in Eigenregie oder lassen sich zum Teil auch von ihren Lieferanten dabei unterstützen.

Zunächst gilt es den Sinn und Zweck der eingesetzten Software sowie die Sensibilität ihrer Funktionen zu beurteilen. Dieser grundsätzlichen Einordnung liegt das gesamte Rollen- und Berechtigungskonzept zugrunde. In gleicher Weise wird mit den Zutrittsberechtigungen für die Räumlichkeiten der Infrastrukturebene verfahren. Prozessschritt für Prozessschritt muss ersichtlich sein, wer welche Rolle besitzt und welche Berechtigungen diese Rolle beinhaltet. Je nach Struktur und Kritikalität der betreffenden IT-Lösung, ergeben sich daraus hochkomplexe Fragestellungen.

Use-Case-bezogene Rechtevergabe

Stets ist präzise festzuhalten, wer organisatorisch und wer fachlich für die Rechtevergabe verantwortlich ist. Zudem folgt die Definitionsarbeit zwei zentralen Grundsätzen: dem Sparsamkeits- und dem Minimalprinzip. Während das erstgenannte Prinzip zu effizienten und kostenschonenden Prozessen führt, stellt das Minimalprinzip sicher, dass die Prozessteilnehmer stets ausschließlich jene Berechtigungen erhalten, die sie zur Ausführung ihrer täglichen Arbeit tatsächlich brauchen.

Um den Definitionsaufwand in Grenzen zu halten, stellen viele IT-Lieferanten Musterkonzepte zur Verfügung. Diese dienen jedoch lediglich als Orientierungsgrundlage für das eigentliche Sollkonzept. Die Verantwortung für dessen spezifische Ausgestaltung trägt allein das Kreditinstitut. Denn auch, wenn davon auszugehen ist, dass jeder seriöse Hersteller den Funktionsumfang seiner Anwendungen und Technologiewerkzeuge so umfassend wie möglich dokumentieren wird, muss die Bank eine solche Vorlage auf Vollständigkeit überprüfen und vor dem Hintergrund der konkret geplanten Anwendungsszenarien (englisch Use Cases) gegebenenfalls ergänzen.

- Hierzu gehören insbesondere auch solche Vorgaben, die den Umgang mit den Zutritts- oder Zugriffsberechtigungen regeln, wenn Mitarbeitende vorübergehend ausfallen und vertreten werden müssen.

- Zudem gilt es Vorkehrungen für den Fall zu treffen, wenn Personen mit kritischen Berechtigungen das Unternehmen verlassen – etwa Administratoren oder leitende Manager.

All diese Fragen muss ein Sollkonzept belastbar beantworten können. Nur dann werden sich die Risiken der zu gewährenden Berechtigungen verlässlich bewerten lassen. Die solchermaßen ermittelte Risikoreichweite führt zur Einstufung des jeweiligen IT-Systems in eine adäquate Schutzbedarfsklasse. Die Klassifizierung erfolgt durch die Fachbereiche, die mit dem System arbeiten. Die gewählte Schutzbedarfsklasse wiederum gibt vor, in welchem Turnus Rezertifizierungen zu erfolgen haben.

Im Rahmen der IT-Prüfung durch die interne und externe Revision ergibt sich ein Prüfrhythmus von maximal drei Jahren. Zeigen sich Auffälligkeiten an den im Sollkonzept festgelegten Risikoparametern, kann die Revisionsstelle den Turnus verkürzen. Darüber hinaus können Kontrollen in anderen Bereichen, wie zum Beispiel dem Wertpapierhandel oder dem Kreditgeschäft, weitere Nachweise erfordern. Da sich die verschiedenen Prüfrhythmen somit überlagern, steigt der Rezertifizierungsbedarf immer weiter an. Um uneingeschränkt auditfähig zu sein, ohne die dabei entstehenden Prozesskosten aus den Augen zu verlieren, ist eine weitgehende Automatisierung der Rezertifizierung des Berechtigungsmanagements unabdingbar.

Praxisbeispiel Deep Thought

Wie sich die Prozesse rund um die Rechte-Rezertifizierung automatisieren lassen, lässt sich am Beispiel der Software Deep Thought (Andermann & Partner) zeigen, die nun gemeinsam mit dem Foconis-ZAK Funktionspaket „Rezertifizierung“ die Rezertifizierung des Berechtigungsmanagements automatisiert. Dieses vor allem im genossenschaftlichen Bankensektor verbreitete Expertensystem automatisiert die Dokumentation, Überwachung und Tiefenanalyse aller relevanten Bestimmungen.

Im Zentrum dieses Ansatzes steht eine fortwährende Soll-Ist-Untersuchung, bei der die Sollkonzepte der Anwenderunternehmen mit den aktiven Berechtigungen abgeglichen werden. Da die Kontrolle unter anderem toxische Analysen – auch „Tiefenanalysen“ genannt – umfasst, können Banken risikoorientiert IKS-relevante Sachverhalte aufdecken und mit geeigneten Gegenmaßnahmen belegen.

Abweichungen werden den zuständigen Fachbereichen gemeldet, die sodann den in Frage stehenden Sachverhalt überprüfen und gegebenenfalls rezertifizieren. Die zu kontrollierenden Auffälligkeiten fallen in zwei Kategorien. Zum einen geht es um Abweichungen vom Sollkonzept, die eine Zurücknahme von bereits erteilten Genehmigungen nahelegen. Zum anderen geht es um das Managen umgekehrter Abweichungen.

So kommt es beispielsweise immer wieder vor, dass das Sollkonzept für bestimmte Rollen Berechtigungen vorsieht, die im aktuellen Ist-Zustand (noch) nicht aktiviert sind. Eine normkonforme Aktivierung setzt jedoch die erneute fachliche Prüfung des Sachverhalts voraus. Schließlich kann es gute Gründe für den aktuellen Status geben. So ist zum Beispiel denkbar,

dass bei der ursprünglichen Rechtevergabe das Sparsamkeitsprinzip Vorrang erhielt, da man zu dem Schluss kam, dass die konkret einzurichtende Rolle weniger Zugriffs- oder Zutrittskompetenzen erfordert, als ihr aus rein regulatorischer Sicht zustünde.

Rechte-Rezertifizierung bedingt Software

Automatisierungslösungen führen die zuständigen Fachbereiche durch alle Schritte des jeweils erforderlichen Rezertifizierungsprozesses und unterstützen die normkonforme Dokumentation der damit einhergehenden Prüfarbeit. Gleiches gilt für den sogenannten Soll-Soll-Abgleich, der unterjährige Anpassungen des eigentlichen Sollkonzepts analysiert und Abweichungen transparent aufzeigt. Dabei stellen Banken jederzeit sicher, dass derartige Änderungen der Rahmenparameter sowohl den regulatorischen als auch den unternehmensspezifischen Anforderungen entsprechen.

Compliance zu gewährleisten und zugleich den stetig zunehmenden Regularien effizient zu begegnen, ist das erklärte Ziel der Kreditwirtschaft. Rahmenbedingungen, wie etwa Ressourcenengpässe, fordern Automatisierungsstrategien. Auch im Berechtigungsmanagement und der nachgelagerten Rezertifizierung braucht es Software, die die gesetzlichen Vorgaben zu erfüllen hilft. Eine Managementlösung, die die erforderlichen Soll-Ist- und Soll-Soll-Abgleiche vollständig automatisiert und die Compliance-Verantwortlichen über Abweichungen frühestmöglich in Kenntnis setzt, schafft ein hohes Maß an Sicherheit und Risikobewusstsein. Gleichzeitig stellt die Prozessautomatisierung sicher, dass die administrativen Kosten trotz der permanenten Ausweitung sowohl der Regulatorik als auch der Gefahrenlage in einem kaufmännisch vertretbaren Rahmen bleiben.