bank objekte

Planung
Einrichtung
Ausstattung
Digitalisierung

Ausgabe 2/2024 · Mai
ZKZ 06039 (Deutschland)
Plus.Zeitung 12Z039463 P (Österreich)
Post-Nr. 02-24 objekte

ISSN 2194-1335
Einzelverkaufspreis € 13,50
28. Jahrgang

Nachhaltig modern

TEAMPLAN®

Sparkasse Märkisches Sauerland Hemer-Menden

Fachthema
Kundennähe gestalten

Special
Akustiklösungen

IT:BANKER
Berechtigungsmanagement

Optimal in die IT-Prozesslandschaft integrieren

Wie IT-Verantwortliche neue rechtliche Anforderungen im Berechtigungsmanagement umsetzen können

Bild: Eakrin/stock.adobe.com

Mit dem Digital Operational Resilience Act (DORA) stehen Kreditinstituten neben der MaComp und BAIT weitere regulatorische Anforderungen im Berechtigungsmanagement ins Haus. Die Entwicklung entsprechender Sollkonzepte verantworten die Banken selbst. Was müssen die Konzepte sowie digitale Tools leisten, damit ein revisionssicheres Rezertifizierungsmanagement gewährleistet ist?

Sollkonzept erforderlich

Im Zugriffs- und Zutrittsmanagement für Software, EDV-Strukturen oder Räumlichkeiten wie Serverräume unterliegen Kreditinstitute strengen Vorgaben. Die in der Regulatorik festgeschriebenen Richtlinien bilden hierbei die rechtlichen Grundpfeiler. Mit DORA steht die Einführung weiterer regulatorischer Anforderungen bevor: Bereits ab Januar 2025 ist mit einer Umsetzung auf Bundesebene zu rechnen. Software- und Zugriffsberechtigungen in Unternehmen sollen nachvollziehbar und auf die vorgeschriebene Weise dokumentiert und im Kontrollfall bestätigt werden können. Das Schlagwort der Stunde lautet: Rezertifizierung. Die Verantwortung für das Erstellen des Sollkonzepts und dessen Durchsetzung trägt das Kreditinstitut. Die Rezertifizierung ist ein sensibler, wiederkehrender Prozess.

Wichtige Konzeptbestandteile

Um ein Sollkonzept erstellen zu können, müssen die Verantwortlichen zunächst die passende Grundlage schaffen. Dafür braucht es Klarheit über das Risikopotenzial einer einzuführenden Software in mehrerlei Hinsicht. Um die Risikoreichweite der Anwendung einschätzen zu können, müssen der Funktionsumfang und die Rechtereichweite der Systeme und Tools ausführlich dokumentiert werden. Aus dieser Risikoeinschätzung ergibt sich die jeweilige Schutzklasse des Systems. Diese ist wiederum maßgeblich für den Turnus der Rezertifizierung. Die Verantwortlichen sollten darauf achten, dass die Ermittlung der Schutzklasse durch jeden Fachbereich einzeln erfolgt. Im Zuge dieses Prozesses gilt es auch, die organisatorischen und fachlichen Verantwortlichkeiten zu klären – inklusive »kritischer Berechtigungen«, also Zugängen für einzelne Personen oder Gruppen, die das System oder die darin enthaltenen Daten grundlegend gefährden könnten. Insgesamt müssen Banken und Sparkassen darauf achten, dass die Software sowohl dem Sparsamkeitsprinzip (maximal effiziente und kostengünstige Prozesse) als auch dem Minimalprinzip (Gewährung ausschließlich unbedingt erforderlicher Kompetenzen) entspricht.

Automatisierter Abgleich schafft Sicherheit

Nach der Konzeption übernehmen in der Regel praxisbewährte Softwarelösungen den Soll-Ist-Abgleich: Sie dokumentieren und überwachen automatisiert und rechtssicher den Status quo auf Grundlage der zugrunde liegenden Konzepte. Das System gleicht das Sollkonzept mit den aktuell aktiven Berechtigungen ab. Die Fachabteilungen erhalten dann bei Auffälligkeiten eine Meldung. Die Prüfung des Sachverhalts tritt im Rahmen der eigentlichen Rezertifizierung ein. Eine Meldung erfolgt etwa bei der Abweichung vom dokumentierten Sollkonzept oder bei umgekehrten Abweichungen. Letztere bestehen, wenn das Sollkonzept Berechtigungen für Mitarbeitende vorsieht, die aber

aktuell nicht aktiviert sind. Es ist nun wichtig, diese Kompetenzen nicht einfach zu erteilen, nur weil sie im Sollkonzept angelegt sind. Schließlich könnte es sein, dass die Berechtigungen im Sinne des Sparsamkeitsprinzips nicht erforderlich sind. Sind hingegen Kompetenzerweiterungen notwendig, die nicht im Sollkonzept vermerkt, zukünftig jedoch vorgesehen sind, müssen die Verantwortlichen das Sollkonzept anpassen und alle Änderungen sorgfältig dokumentieren. Leistungsfähige Softwarelösungen führen bei einer unterjährigen Anpassung des Sollkonzeptes stets einen Soll-Soll-Abgleich durch. Dieser ist essenziell, um festzustellen, ob die Änderungen sowohl den regulatorischen Anforderungen als auch den hausinternen Grundsätzen entsprechen.


Bild: Eakrin/stock.adobe.com

Einfache Integration ist Pflicht

Damit Banken die vorgeschriebenen Regularien maximal effizient, zielführend und durchgängig dokumentiert umsetzen können, sollten sie bei der Wahl ihrer Softwarelösung einige Punkte beachten:

1. Die Lösung muss sich problemlos in Standardsysteme und -umgebungen integrieren lassen
2. Das System ist in der Lage, sowohl einen Soll-Ist- als auch einen Soll-Soll-Vergleich durchzuführen
3. Die Überprüfung der IT-Berechtigungen erfolgt automatisiert in einem schlanken, schnellen Prozess
4. Kritische IT-Berechtigungen, wie die mit hohem Risikopotenzial, sollte die Lösung intelligent identifizieren und abbilden können
5. Für die effiziente Nutzung ist es hilfreich, wenn Banken die gleichen Tools wie die IT-Prüfer:innen der Verbände nutzen

Systeme wie das Funktionspaket »Rezertifizierung« der FOCONIS AG, in der die Lösung Deep Thought von Andermann & Partner aufgehen wird, profitieren zudem von einer großen Verbreitung im genossenschaftlichen Bankumfeld und lassen sich direkt innerhalb der IT-Infrastruktur des Rechenzentrums betreiben.

Fazit

IT-Verantwortliche sind einmal mehr gefordert, neue rechtliche Anforderungen im Berechtigungsmanagement umzusetzen. Dabei dürfen sie die ohnehin schon knappen Ressourcen nicht unnötig belasten. Im Zuge des Rezertifizierungsmanagements braucht es darum wichtige konzeptionelle Vorüberlegungen sowie eine intelligente Software, die stetig, voll automatisiert und risikoorientiert den Status quo untersucht und damit ein hohes Maß an Sicherheit schafft. ■

www.foconis.de


Bilder: foconis

Der Autor: **Olaf Pulwey,** CEO, FOCONIS AG