➢ Artikel vom 7. November 2018

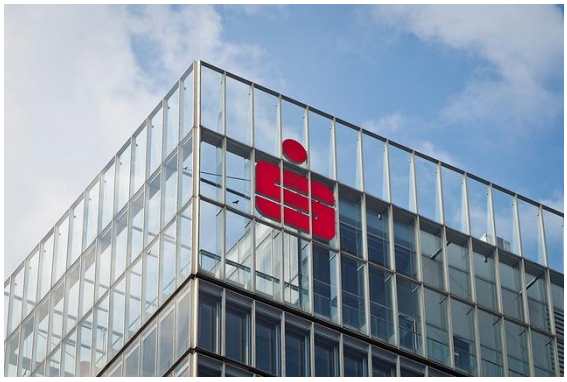
IT-Berechtigungen unter OSPlus MaRisk-konform und komfortabel rezertifizieren

Die wiederholte Kontrolle von IT-Berechtigungen ist umfangreich und arbeitsintensiv, aber aufsichtlich gefordert. OSPlus bietet einen Musterprozess an, der die Rezertifizierung in weiten Teilen automatisiert und auf einem passenden Sollrollenkonzept aufbaut. Bei der Erstellung und Optimierung unterstützen die Mitarbeiter von Beckmann & Partner CONSULT.

Die Aufsichtsbehörden legen bei der Bewertung von Risiken der Kreditinstitute auch immer größeren Wert darauf, IT-Risiken zu erkennen und zu minimieren. Dabei rücken neben den Prozessen für eine aufgabenorientierte Vergabe von IT-Berechtigungen insbesondere auch die regelmäßige und anlassbezogene Überprüfung der IT-Berechtigungen der Mitarbeiter in den Fokus.

Anforderung der MaRisk

Gemäß dem Minimalprinzip darf kein Mitarbeiter über IT-Berechtigungen verfügen, die er nicht zwingend zur Erfüllung seiner Aufgaben benötigt (MaRisk, Modul AT 7.2). Ansonsten entsteht Risiko vor allem aus möglichen Schäden, die aus der - wenn auch versehentlichen - Verwendung von kritischen IT-Rechten oder zu weitrechenden Berechtigungsvergabe resultieren können. So kann beispielsweise ein Mitarbeiter mit Administrator-Rechten erhebliche Schäden im IT-System – und daraus resultierende wirtschaftliche Schäden - verursachen, ohne dass er sich dessen überhaupt bewusst sein muss. Die Folge ist die aufsichtsrechtliche Anforderung zur regelmäßigen als auch anlassbezogenen Überprüfung der vergebenen IT-Berechtigungen, die sogenannte Rezertifizierung.



Bereichsübergreifende Kenntnisse nötig

Die Rezertifizierung zielt darauf ab, das Verhältnis von Mitarbeiter zu seinen IT-Berechtigungen zu verifizieren. Verantwortliche Rezertifizierer kennen dabei oftmals nur eine kleine Teilmenge der dazu nötigen Informationen. So kennt zum Beispiel der Fachvorgesetzte des zu rezertifizierenden Mitarbeiters zwar die Aufgaben seines Mitarbeiters, dafür aber nicht unbedingt die Eigenschaften, Funktionsweisen und Auswirkungen der IT-Berechtigungen. Und die IT-kompetenten Kollegen kennen zwar die Eigenschaften der IT-Berechtigungen, nicht aber das Aufgabenfeld eines jeden Mitarbeiters. Um das Minimalprinzip einzuhalten, sind aber beide Kenntnisse - des klar abgegrenzten Aufgabenbereichs des Mitarbeiters sowie das detaillierte Verständnis der IT-Berechtigungen - unabdingbar. Die Herausforderung für Rezertifizierer wird umso größer, je mehr externe Anwendungen benutzt werden. Denn die Rezertifizierung muss konkret für jeden Mitarbeitenden klären: Benötigt dieser Mitarbeitende zwingend die Berechtigung XY? Es stellen sich dabei folgende Einzelfragen:

- Welche Berechtigungen benötigt Erika Mustermann unbedingt zur Erfüllung der ihr übertragenen Aufgaben, welche benötigt sie nicht?
- Welche Aufgaben übt Frau Mustermann eigentlich aus?
- Welche Anwendungen werden dafür genutzt?
- Welche Berechtigungen innerhalb der Anwendungen werden dafür benötigt?

Dem Minimalprinzip steht darüber hinaus noch die integrierte Betrachtung, das heißt das Zusammenspiel von verschiedenen Berechtigungen, gegenüber. Die Aufsichtsbehörden fordern, dass eine Rezertifizierung auch immer darauf abzielt, sich widersprechende beziehungsweise ausschließende IT-Berechtigungen aus unterschiedlichen Anwendungen im Paket und integriert zu verifizieren, um insbesondere Funktionstrennungs- oder Interessenskonflikte zu vermeiden. Somit sollten einzelne Anwendungen nicht losgelöst und unabhängig voneinander rezertifiziert werden. Besondere Schwierigkeiten können darüber hinaus noch entstehen, wenn Mitarbeitende ihre Kolleginnen oder Kollegen vertreten oder Mitarbeitende ihre Stelle wechseln.

Lösungsansatz: Aufgabenbezogenes Sollrollenkonzept und kleine Schritte

Der Rezertifizierungsprozess wird so unterteilt, dass einzelne Mitarbeiter gemäß ihrer fachlichen Kenntnisse jeweils direkte Zuordnungen in den einzelnen Rezertifizierungsschritten beurteilen können. Somit kann immer ein kompetenter Mitarbeiter kundig rezertifizieren. Auch hat ein Mitarbeiter für die Rezertifizierung eine überschaubare Menge an Aufgaben zu erledigen. Das Zusammenspiel verschiedener

Schritte sorgt auf diesem Weg dafür, dass insgesamt eine effiziente und nachvollziehbare Rezertifizierung stattfindet. Ausgangslage der Rezertifizierung ist ein risikoorientiertes und aufgabenorientiertes Sollrollenkonzept, das darlegt, welche Aufgaben in verschiedenen Organisationseinheiten wahrgenommen werden. Die ersten zwei von drei Schritten sind dabei völlig anonym in dem Sinne, dass der individuelle, zu rezertifizierende Mitarbeiter keine Rolle spielt. Stattdessen werden die Aufgabentypen betrachtet, die in einem Institut ausgeführt werden. Zu diesen Aufgabentypen können einzelne Teilaufgaben und zu den einzelnen Teilaufgaben können notwendige IT-Berechtigungen als Bündel zugeordnet werden. In einem dritten Schritt kann dann individuell zu einem konkreten Mitarbeiter die Zuordnung zu einer Stelle beziehungsweise Aufgabe geprüft werden. Jeder Schritt ist somit klar abgegrenzt und mit eindeutigen Fachkompetenzen bei überschaubarem Aufwand zu erledigen.

Mustervorgehensmodell unter OSPlus

Dieses aufgaben- und risikoorientierte Mustervorgehensmodell zur Rezertifizierung wurde in der Sparkassen-Organisation mit fachlicher Unterstützung von Beckmann & Partner CONSULT erarbeitet. Das Mustervorgehensmodell baut auf diesem 3-schrittigen Lösungsansatz auf und setzt die Nutzung eines aufgabenorientierten Sollrollenkonzepts voraus. Es hat den Vorteil, dass viele Institute es für sich nutzen können und die Rezertifizierung dabei ihrer jeweils unterschiedlichen Betriebsstruktur gerecht wird. Zusätzlich wird der zeitliche Aufwand deutlich reduziert, da keine Vorbereitungszeit mehr für die Rezertifizierung benötigt wird. Stapelweise Listenausdrucke entfallen. Unabdingbar für die Nutzung des Mustervorgehensmodells ist ein stark aufgabenbezogenes Sollrollenkonzept. Ohne ein solches Sollrollenkonzept ist die Bündelung von IT-Berechtigungen fachlicher „Aufgabenerfüller" und die Zuordnung der „Aufgabenerfüller" (Rechtebündel) zur Gesamtaufgabe einer Planstelle (Stellenfunktion) nicht möglich. Darüber hinaus erlaubt ein Sollrollenkonzept die Implementierung von Vertretungsregelungen auf Basis von Organisationseinheiten.

Die Sparkasse Offenburg/ Ortenau war eine der ersten Sparkassen, die sich zur Anwendung des Mustervorgehensmodells entschlossen hat. So wurde zunächst ein aufgabenbezogenes und anwendungsübergreifendes Sollrollenkonzept im OSPlus abgebildet. Das Sollrollenkonzept wurde dabei an den Anforderungen des Mustervorgehensmodells zur Rezertifizierung ausgerichtet. Für die ca. 850 Mitarbeiter wurden 220 relevante Aufgabentypen identifiziert, die als *Stellenfunktionen* abgebildet wurden. Für die Erfüllung der jeweiligen Aufgabentypen wurden etwa 1.300 aufgabenorientierte Berechtigungspakete als *Funktionsprofile* definiert. Dabei ermöglicht

jedes Funktionsprofil die Erfüllung einer Teilaufgabe und wurde mit sprechenden und nachvollziehbaren Profilbeschreibungen ausgestattet. Marcus Heitz, Leiter der DV-Organisation der Sparkasse Offenburg/ Ortenau, sagt: „Eine Menge Arbeit. Natürlich muss zunächst intern das Bewusstsein für ein stringentes, auf den Notwendigkeiten beruhendes Sollrollenkonzept geschaffen werden. Dabei ist die Einbindung der Fachabteilungen wichtig. Ohne TOP Mitarbeiter im Projektteam geht dies nicht", so Heitz weiter. „Dabei waren Mitarbeiter aus der Betriebsorga und der DV Organisation eingebunden. Wir mussten uns sehr gut und detailliert mit allen unseren Anwendungen, unseren Strukturen und Konzepten auseinander setzen. Diese konzeptionellen Aufwände sind nicht zu unterschätzen und können 'nicht einfach nebenbei' geleistet werden. Allerdings stellt diese Vorbereitung den wichtigsten Erfolgsfaktor für langfristig effiziente Prozesse im IT-Berechtigungsmanagement und schlanke, aber qualitativ gute Rezertifizierungen dar." Die Sparkasse Offenburg/ Ortenau habe sich gut überlegt, ob sie als eine der ersten Sparkassen diese neue OSPlus-Funktionalität einsetze. „Wichtige Informationen und Hilfestellungen für den Aufbau unseres IT-Berechtigungsmanagements erhielt unsere Sparkasse durch die Teilnahme an den angebotenen Einführungsunterstützungen der Finanz Informatik.", so Heitz.

Umfassende Expertise von Beckmann & Partner CONSULT

Beckmann & Partner ist zertifizierter Partner der Finanz Informatik und besitzt einzigartige Expertise in der Anwendung und der Umstellung auf das Mustervorgehensmodell und den IT-gestützten Rezertifizierungsprozess unter OSPlus. „Die letzte Sicherheit für die Nutzung des neuen Workflows haben wir uns verschafft, indem wir uns Beratung bei Beckmann & Partner CONSULT aus Bielefeld geholt haben.", so Heitz weiter. „Christian Kampmeier, einer der Berater dieses Hauses, ist seit langen Jahren an der Entwicklung von OSPlus beteiligt und sein Spezialgebiet sind alle Themen rund um die Basisadministration von OSPlus. Seit diesem Jahr ist Beckmann & Partner zertifizierter Referenzpartner der Finanz Informatik für genau dieses Themengebiet. Auch auf Empfehlung von unserem zentralen IT-Dienstleister haben wir diesen Beratungsauftrag gern bei Beckmann & Partner platziert." Die Mitarbeiter von Beckmann & Partner CONSULT haben bereits die Entwicklung des Mustervorgehensmodells mit begleitet und gemeinsam mit der Finanz Informatik über 185 Sparkassen aktiv bei der Einführung unterstützt. „Christian Kampmeier und sein Kollege Ludwig Neukart waren zwei Mal bei uns vor Ort. Im ersten Termin haben wir 'unsere Hausaufgaben kontrolliert'. Wir haben unsere Datenbasis gesichtet und durchgearbeitet. Die Berater haben uns noch wertvolle letzte Tipps gegeben, so dass wir am Ende dieses Tages die Entscheidung treffen konnten, die Rezertifizierung mit Hilfe des neuen Workflows durchzuführen. Dann haben wir in einem zweiten Termin

alle unsere Rezertifizierungsverantwortlichen und ausgewählte Multiplikatoren ins Boot geholt. Die Berater von Beckmann & Partner haben die aufsichtsrechtlichen Anforderungen, die prüferische Erwartungshaltung sowie die OSPlus-Funktionalitäten im Rahmen einer Anwenderschulung präsentiert und wir sind den Ablauf Schritt für Schritt durchgegangen. Wir hatten ausreichend Raum für Fragen und auch für Detailgespräche vorgesehen, so dass dieser Tag sehr erfolgreich gestaltet wurde und wir alle motivieren konnten, unser Vorhaben zu unterstützen.", resümiert Heitz. Sein Fazit: „Es hat sich gelohnt. Nicht zuletzt wegen der guten Unterstützung durch die Finanz Informatik und durch Beckmann & Partner CONSULT ein erfolgreiches Projekt."

Ansprechpartner:
Dr. Pascal Aßmuth, Christian Kampmeier, Ludwig Neukart
Bankfachberater

Beckmann & Partner CONSULT
Telefon: 0521 25290 0
sparkassenberatung@beckmann-partner.de
https://www.beckmann-partner.de

Beckmann & Partner CONSULT ist Beratungsmanufaktur für bankfachliche Themen. Hier sind Informatiker mit Bankwissen und Banker mit Informatikwissen im Einsatz. Unsere Spezialität sind Businessanalyse, Projektmanagement und Softwareentwicklung. Dabei liegt unserem Sparkassenteam die Weiterentwicklung von OSPlus besonders am Herzen. Die Mitarbeiter und Mitarbeiterinnen schulen seit der produktiven Bereitstellung der Anwendung in 2015 den OSPlus-gestützten Rezertifizierungsprozess in Sparkassen und die bedarfsgerechte Administration des gesamten Rezertifizierungsprozesses. Auch in 2018 bringen sie ihre Expertise und Erfahrungen zielgerichtet ein und bieten umfangreiche Unterstützungs- und Einführungsangebote für Sparkassen an.

Vom 20. bis zum 22. November 2018 findet das FI-Forum statt - die Hausmesse der Finanz Informatik. Hier finden Sie Beckmann & Partner auf Stand P81.