EXPERTS IN IDENTITY.
ACCESS. GOVERNANCE.

Geschäftsrollen erfolgreich eingeführt – wie weiter?

Fachartikel von Mihael Zadro, IAM Consultant, IPG GmbH Deutschland

Geschäftsrollen sind bereits in vielen Unternehmen im Einsatz. Wo aber stehen sie im Rollen-Lebenszyklus? Im Allgemeinen wurde einmal ein grundlegendes Konzept erstellt, die Geschäftsrollen gemeinsam mit externen Beratern oder mit eigenem Know-how modelliert und mit jeweils einem Verantwortlichen oder einem Fachbereich abgestimmt und eingeführt. Anschließend kümmern sich Mitarbeitende organisiert in Rollen-Teams, um die Pflege von bestehenden Geschäftsrollen, die Erstellung oder Modellierung von neuen Geschäftsrollen und beraten das Unternehmen in Fragen zur Anwendung des Geschäftsrollen-Prinzips. Die Provisionierung der in Geschäftsrollen enthaltenen IT-Berechtigungen erfolgt im Regelfall durch ein Identity Management Tool, in dem der Rollen-Lebenszyklus umgesetzt ist oder das Rollen-Team übernimmt diese Aufgabe als manuelle Tätigkeit und kümmert sich, dass Mitarbeitende benötigte IT-Berechtigungen erhalten. Weniger betrachtet werden dabei die stetige Weiterentwicklung und die Nutzung von Best Practices auf Basis aktueller bzw. neuer Technologien.

Verbesserungen / Verfeinerungen vornehmen

Erst nachdem die Überführungsphase abgeschlossen ist und sich die neuen Prozesse in der Anwendung des Rollenlebenszyklus etabliert haben, verlagert sich die Arbeit der Rollen-Experten zunehmend auf Verbesserungen und Verfeinerungen am bestehenden Geschäftsrollenmodell. Dafür bedarf es der laufenden Analyse eigener Prozesse und einer unter Umständen zeitaufwändigen Suche nach Optimierungsmöglichkeiten. Veränderungen an den Berechtigungsressourcen müssen ebenfalls laufend erfasst und in bestehenden Geschäftsrollen nachgezogen werden. Was intern sehr zeitaufwändig passiert, kann durch den Zuzug von externen Experten im Bereich Rollenmodellierung wesentlich effizienter und effektiver gestaltet werden. Best Practices werden in die Optimierung miteinbezogen, bereits etablierte Lösungsansätze gegen die eigenen Anforderungen gestellt und mit erprobten Hilfsmitteln die Arbeiten vereinfacht werden.

Rollenkatalog aktuell und schlank halten

Sind Geschäftsrollen organisationseinheitsbezogen modelliert worden, müssen diese an organisatorische Veränderungen angepasst werden können. Zudem empfiehlt sich die regelmässige Überprüfung, ob diese Geschäftsrollen organisationseinheitsübergreifend optimiert oder erweitert werden können. So kann sichergestellt werden, dass praktisch identische Geschäftsrollen nicht in verschiedenen Organisationseinheiten mehrfach vorhanden sind. Mehrfach vorhandene Geschäftsrollen blähen den administrativen Aufwand für das Rollen-Team auf und können zu unnötiger Mehrarbeit führen.

Überwachung von Kennzahlen zeigt Handlungsbedarf

Oft gestaltet sich die „Überwachung“ von Geschäftsrollen, insbesondere die Bewirtschaftung des gesamten Rollenkatalogs, sehr schwierig. Je umfassender der Rollenkatalog ist, desto schwieriger ist es festzustellen, ob Optimierungspotenzial besteht. Dafür werden in der Regel einfache, bereits vorhandene Daten als Kennzahlen genutzt. Dies kann zum Beispiel die regelmäßige Überprüfung der Anzahl zusätzlich zu Geschäftsrollen

vergebener Berechtigungen sein. Diese Kennzahl ausgewertet auf Mitarbeitende, die eine Geschäftsrolle zugewiesen haben, liefert bereits ein Indiz für eine mögliche Prüfung dieser Rolle. Sollte die Zahl stetig steigen, ist das ein Anzeichen dafür, dass die Rolle nicht optimal (vollständig) ist und deswegen nicht optimal genutzt wird. Etwas komplexere Überwachungen, wie zum Beispiel das Monitoring der Anzahl von Geschäftsrollen und in Geschäftsrollen vergebene Berechtigungen über einen Zeitraum, können schon genauere Resultate oder sogar Trends liefern. Sollte sich die Anzahl von Geschäftsrollen erhöhen, während die durchschnittliche Zahl der in Geschäftsrollen enthaltenen Berechtigungen stagniert oder sogar sinkt, ist das auch bereits ein sehr guter Indikator für akuten Handlungsbedarf.

Rezertifizierungen kosten Zeit – Nicht nur die Zeit der Führungskräfte

Zu einem nicht zu unterschätzenden Managementaufwand können nötige, regelmäßige Überprüfungen von Geschäftsrollen und Geschäftsrolleninhalten durch Verantwortliche werden. Je nach Schutzbedarf eines IT-Systems, dessen IT-Berechtigungen in Geschäftsrollen enthalten sind, kann der Zeitpunkt für eine Überprüfung schnell eintreffen. Insbesondere bei einer ersten Überprüfung / Zertifizierung einer Geschäftsrolle oder ihrer Inhalte kann der Beratungsbedarf beim Verantwortlichen durchaus hoch sein. Mit der Zahl der Verantwortlichen steigt auch der Beratungsaufwand beim Rollen-Team. Rezertifizierungen lassen zusätzlich zum Beratungsaufwand auch den Unterhaltsaufwand steigen. Denn ergeben sich aus der Überprüfung Änderungen, müssen auch diese Aufgaben / Aufträge zeitnah umgesetzt werden.

Das Geschäftsrollenmodell soll schnelle Veränderungen ermöglichen und nicht bremsen

Bedingt dadurch, dass Mitarbeitende ihre Berechtigungen über Geschäftsrollen erhalten und nicht mehr direkt in angebundenen Systemen berechtigt werden, können sich Änderungen an der Berechtigungsstruktur in angebundenen Systemen nicht nur auf Geschäftsrollen selbst, sondern auch auf das Geschäftsrollenmodell auswirken. Als Beispiel hierfür kann die Ersteinführung einer Organisationsstruktur basierten Ordner-Freigabe dienen. Unterstützt das etablierte Geschäftsrollenmodell nur die Vergabe von Rollen auf Basis einer Aufgabe oder Funktion von Mitarbeitenden, muss das Geschäftsrollenmodell selbst angepasst werden. Zum Beispiel mit der Einführung von Organisationsrollen. Insbesondere, wenn Änderungen von Berechtigungsstrukturen nicht an das Rollen-Team herangetragen werden, hilft ein Prozess diese zu identifizieren: Eine Berechtigung, die auf einmal in viele verschiedene Geschäftsrollen aufgenommen werden soll, ist ein guter Hinweis sich den Sachverhalt genauer anzuschauen und das Geschäftsrollenmodell entsprechend zu erweitern. Genauso wie viele leere Geschäftsrollen (Rolle ohne zugeordnete Berechtigungen) eines Rollen-Typs für eine Verschlankung des Geschäftsrollenmodells sprechen können. Gelingt es, ein schlankes Geschäftsrollenmodell zu entwickeln und dieses zu managen besitzt das Unternehmen einen wichtigen Enabler, um schnell auf technologische, organisatorische oder strukturelle Veränderungen zu reagieren.

Neben dem Daily Business müssen Neuerungen beachtet werden

Rollen-Experten müssen sich neben den täglichen Aufgaben auch auf Neuerungen im Gebiet des Berechtigungsmanagements konzentrieren. Als Beispiel kann hier die Veröffentlichung der letzten Fassung der Bankaufsichtlichen Anforderungen an die IT (BAIT) mit dem Rundschreiben der Bundesanstalt für Finanzaufsicht (BaFin) Anfang November 2017 herangezogen werden. Das Rollen-Team, eines unter diese Aufsichtspflicht fallenden Unternehmens, muss die eigenen Prozesse und Anforderungen auf nun verschärfte Vorgaben der BaFin hin überprüfen und identifizierte Lücken schliessen.

Zum Beispiel sind die in Rollen enthaltenen IT-Berechtigungen direkt von den erweiterten Anforderungen der BAIT betroffen. Für die betroffenen Unternehmen hat dies folgende Auswirkungen:

1. Wahrnehmung der Verantwortung durch fachlich Verantwortliche

Fachlich Verantwortliche, auch Verantwortliche für Geschäftsrollen, müssen in Zukunft ihre Verantwortung wahrnehmen können. Das bedeutet ein fachlich Verantwortlicher muss seine Rolle „verstehen". Er muss wissen wozu seine Rolle dient und für was die in seiner Rolle enthaltenen Berechtigungen seinen Mitarbeitenden genau berechtigen. Dieses Verständnis ist meist durch kryptische Bezeichnungen von IT-Berechtigungen nicht gegeben. Das Rollen-Team ist somit meist der erste Ansprechpartner, wenn fachlich Verantwortliche für in Rollen enthaltene IT-Berechtigungen verständliche Beschreibungen anfordern.

Ein weiterer Punkt sind die Antragsprozesse. In den BAIT heißt es, dass fachlich Verantwortliche in Antrags-, Genehmigungs- und Kontrollprozesse einzubinden sind und jederzeit die Korrektheit der vergebenen IT-Berechtigungen nachvollziehen können müssen. Die Erfüllung dieser Anforderung erfordert unter Umständen die Anpassung von bereits bestehenden Prozessen.

2. Nachvollziehbarkeit, Dokumentation und Sicherstellung

Sämtliche Prozesse der Einrichtung, Änderung und Deaktivierung von IT-Berechtigungen sind nachvollziehbar und auswertbar zu dokumentieren. Das Rollen-Team muss sicherstellen, dass alle bestehenden Prozesse und Vorgehensweisen dieser Anforderung gerecht werden. Mögen alle Prozesse um die Vergabe von IT-Berechtigungen den anderen Anforderungen gerecht werden, ist diese heutzutage nicht mehr ohne technische Unterstützung erfüllbar.

Wie unterstützt IPG?

Durch langjährige Erfahrungen im Identity & Access Management begleitet IPG ihre Kunden auch in der Zeit nach der Modellierung von Rollen und der Implementierung eines Rollenmodells. Dazu gehört die Unterstützung des Rollen-Teams im Daily Business, aber auch das Coaching des Rollen-Teams in der Beratung von Verantwortlichen. Durch genaue Kenntnisse regulatorischer Anforderungen betreut IPG ihre Kunden auch bei der Analyse bestehender und der Definition neuer Prozesse, um alle Vorgaben effizient erfüllen zu können.

Kontaktieren Sie uns und erfahren Sie mehr über Geschäftsrollen.

Christian Rückert: Sales Manager Germany and Austria
christian.rueckert@ipg-group.com; Telefon +49 170 908 03 53

Arne Vodegel: Sales Manager Germany
arne.vodegel@ipg-group.com; Telefon +49 170 908 04 32

Marcel Weber: Sales Manager Switzerland
marcel.weber@ipg-group.com; Telefon +41 79 907 84 47