BILD: ISTOCKPHOTO.COM/ALEX-MIT

**FOKUS: COMPLIANCE**

# Rollenmodellierung: Rechte effizient regeln

Ein gutes Rollenmodell hilft, den Grossteil der Berechtigungen automatisch und einfach nachvollziehbar zu vergeben. Dies erleichtert die Einhaltung der Compliance – und bringt weitere Vorteile.

→ **VON DANIEL KAPPELER**

Schätzungsweise etwa ein Drittel aller IT-Schwachstellen steht im Zusammenhang mit Zugriffskontrollen oder der fehlenden Trennung von Funktionen (Segregation of Duties, kurz SoD). Diese Schwachstellen sind oft direkt oder indirekt auf die Art der Rollenmodellierung zurückzuführen. Häufig führen Ein- und Austritte von Mitarbeitern oder Reorganisationen zu einer unübersichtlichen Rechteverwaltung auf den Systemen und bilden somit eine Gefahr für Betrug.

**Daniel Kappeler** ist ICT Consultant bei WiB Solutions AG → **www.wib.ch**

Viele Firmen sehnen sich deshalb nach einer einfachen, übersichtlichen und automatisierten Zugriffsregelung für ihre IT-Systeme.

Zudem verändert der Einfluss von Cloud Computing Systemlandschaften und Zugriffsmuster in den Firmen. Auch darum werden gute Rollenmodellierungen und möglichst sichere Zugriffsmodelle immer wichtiger. Gefordert sind veränderte Denkmuster sowie neue Anforderungen an das Rollendesign und Zugriffsregelungssysteme.

Die manuelle Rechtevergabe bedeutet auch einen ständig wiederkehrenden Administrationsaufwand für das IT-Team. Um den Prozess effizienter zu gestalten, ist eine Zugriffsverwaltung, basierend auf Rollen und automatisierter Zugriffsvergabe, der richtige Weg. Eine solche Role Based Access Control (RBAC) regelt die Berechtigungsvergabe nach Nutzung sowie hierarchisch nach logischer Rechtezusammengehörigkeit.

## DIE AUSGANGSLAGE: WENIG ÜBERSICHT, UMSTÄNDLICHE PROZESSE

Die typische Situation, bei der Handlungsbedarf besteht, sieht wie folgt aus: Berechtigungen auf den Systemen sind vergeben, aber es mangelt an Übersicht. Die Bearbeitung von Berechtigungen für Zielsysteme kostet viel Zeit und die Automatisierung der Prozessvorgänge ist nicht oder nur erschwert möglich. Schliesslich ist auch die Einhaltung der Compliance, inklusive der klaren Trennung von Funktionen, nicht gewährleistet. Ebenso fehlen Standards für sichere Zugriffe.

## ZIELDEFINITION: WAS SOLL ERREICHT WERDEN?

Wichtig ist, dass vorgängig klar definiert wird, was genau bezweckt werden soll. Folgende Ziele sind nach unserer Erfahrung für viele Kunden zentral:

- **Compliance:** Definition der Ziele für die Einhaltung der gesetzlichen, unternehmensinternen und vertraglichen Regelungen im Bereich der IT-Landschaft. Diese müssen in einem ausgewogen Kosten-Nutzen-Verhältnis festgelegt werden.
- **Funktionstrennung (SoD):** Ein besonderes Augenmerk muss auf die strikte Trennung von sich ausschliessenden Funktionen gerichtet werden. Dazu muss klar definiert sein, welche Rollen sich gegenseitig ausschliessen, welche die Benutzer auswählen können und welche Genehmigungsprozesse für sensible Rollen, wie z. B. die des Buchhalters, notwendig sind. (z. B. Vier-Augen-Prinzip). Wird SoD ungenügend definiert, eröffnen sich Betrugsmöglichkeiten.
- **Risikoreduktion:** Eine standardisierte Rollenmodellierung vermindert das Risiko generell, jedoch definiert der Kunde aufgrund seiner Anforderungen, zu welchem Grad die Minimierung stattfinden soll.
- **Automatisierung der Prozesse:** Im Voraus bekannt sein sollte der gewünschte Automatisierungsgrad und welche Lösung die Anforderungen am besten abdecken kann.
- **Automatische Zuweisung:** Es ist möglich, Rollen nach Benutzerkriterien automatisch an User zu vergeben. Ein gewisser Teil der Rollen wird manuell auf Antrag vergeben. Es soll jedoch eine möglichst hohe Anzahl an automatisch zugewiesenen Rollen (Automatisierungsgrad) erreicht werden. Viele Firmen streben einen Automatisierungsgrad von 80 Prozent an. Ein noch höherer Wert führt möglicherweise zu einem unverhältnismässigen Aufwand für die Rollenerstellung. Sinnvoll ist oft, den Automatisierungsgrad anfangs mit 60 Prozent eher tief zu halten und später zu steigern.
- **Anforderungen und Projektumfang:** Die Art der Anforderungen hat einen grossen Einfluss auf den Projektumfang. Die meisten Projekte scheitern schon beim Projektantrag, da zu viele Ziele mit einem Schritt erreicht werden sollen. Unternehmen mit kleinerem Budget müssen eventuell auf kostenintensive Umsetzungen von Anforderungen verzichten.
- **Effizienz erhöhen und Kosten reduzieren:** Eine gute Rollenmodellierung erhöht die Effizienz in der Rechtevergabe, senkt unmittelbar die Kosten durch einen geringeren administrativen Aufwand und vereinfacht die Durchführung von Audits.

«Die meisten Projekte scheitern schon beim Antrag, da zu viele Ziele mit einem Schritt erreicht werden sollen»

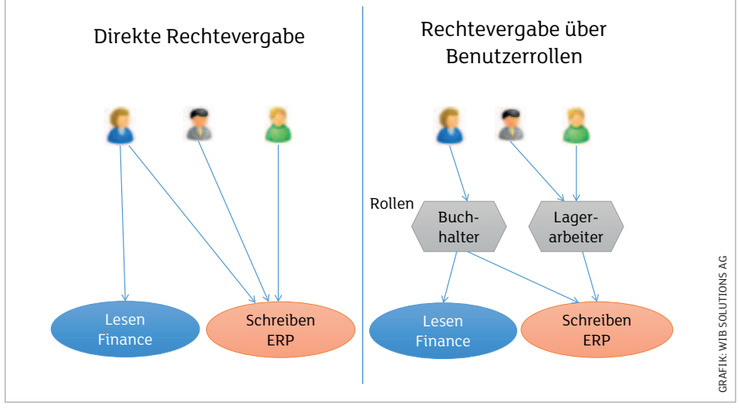
**Daniel Kappeler**

## ECKPFEILER EINER ERFOLGREICHEN ROLLENMODELLIERUNG

Erfahrungsgemäss beinhaltet eine erfolgreiche Rollenmodellierung folgende zentrale Punkte:

- **Stakeholder einbeziehen:** Für den Projekterfolg ist es absolut notwendig, Verantwortliche aus Business und Compliance einzubeziehen. Mitarbeiter aus dem Business werden benötigt, um konkrete Anforderungen zu erheben. Compliance-Verantwortliche müssen den erforderlichen Grad an Sicherheit, Regulierungs- und Auditanforderungen definieren. Zusätzlich werden interne IT-Fachkräfte benötigt, etwa für Tool-Unterstützung oder für die Datenlieferung der existierenden Berechtigungen.
- **Passende Rollentypen:** Die Definition von Rollentypen hängt stark von der Branche und vom Organisationsaufbau ab und ist eine elementare strategische Entscheidung, die sehr früh im Rollenmodellierungsprozess getroffen werden muss. Beispiele für Rollentypen sind «Generelle Rollen», «Funktionsprofile», «Organisationen», «Standorte», «Positionen», «Applikationsfunktionale Rollen», «Projektfunktionale Rollen» oder «Service-Rollen».
- **Top-down und Bottom-up verbinden:** Bei der Top-down-Vorgehensweise werden Rollen aufgrund des Nutzens in der Organisation festgelegt – eine eher betriebswirtschaftliche Perspektive. Bei der Bottom-up-Methode werden die bestehenden Zugriffsrechte geprüft (z. B. aus Active Directory) und daraus Rollen erstellt, also ein technischer Ansatz. Eine gute Rollenmodellierung verbindet beide Vorgehen. Welcher Ansatz stärker gewichtet wird, hängt davon ab, wie hoch der Zufriedenheitsgrad mit den bestehenden Berechtigungsständen ist. Das verbundene Vorgehen wird auch Middle-Out oder Hybridansatz genannt.
- **Verständliches Rollenmodell:** Es ist vor allem zu Beginn der Rollenmodellierung von grosser Bedeutung, die Rollen in Business-, Applikations-, und Systemrollen zu klassifizieren und eine sinnvolle und logische Bündelung von Rollen aufzubauen. Dies bewirkt sowohl eine Trennung von organisatorischer, applikatorischer und technischer Sicht als auch strukturierte Beziehungen untereinander.
- **Validierung:** Das Erstellen von Rollen benötigt immer auch eine Prüfung und Freigabe durch die zuständigen Verantwortlichen. Dafür müssen Validierungsformen definiert werden.
- **Anpassung:** Rollen bleiben nach ihrer Erstellung nicht ewig bestehen, sondern haben einen Lebenszyklus («Role Life Cycle»). Sie müssen kontinuierlich überprüft und überarbeitet werden, um neusten Anforderungen zu genügen.
- **Leitfaden:** Wichtig für den Erfolg der Rollenmodellierung ist es, für das Vorgehen einen klaren Leitfaden zu etablieren und zu beachten.
- **Externes Know-how**: Externe Spezialisten leisten mit ihren Erfahrungen und ihren Best-practice-Ansätzen wertvolle Unterstützung. ←

**Vergabekonzepte**




GRAFIK: WIB SOLUTIONS AG

**Die Rechtevergabe über Benutzerrollen ermöglicht eine teilweise Automatisierung**