Referenzbericht

Mit der Einführung einer Rollen basierenden Berechtigungsverwaltung (RBAC) erfüllt die Helsana viele regulatorische Vorschriften.

In der Helsana werden sämtliche Berechtigungen der Mitarbeiter in allen Anwendungen durch ein firmenweites Rollenmodell gesteuert.

Die Helsana-Gruppe ist der grösste Krankenversicherer der Schweiz. Sie engagiert sich für eine qualitativ hochwertige und wirtschaftliche Gesundheitsversorgung und ist mit einem Prämienvolumen von 5,51 Milliarden Franken die führende Krankenversicherung der Schweiz.

Seit rund sieben Jahren betreibt die Helsana das durch die SKyPRO realisierte Identity Management System und provisioniert Ihre rund 3'000 internen Mitarbeiter und alle externen Berater in eine Vielzahl verschiedenster Anwendungen. Die von einer externen Firma entwickelten Applikation zur Verwaltung der Berechtigungen konnte Zugriffsrechte aber nur in Form von Gruppenmitgliedschaften abbilden. Sie ermöglichte nicht die Definition eines firmenweiten und Anwendungsübergreifenden Rollenmodelles.

Die Helsana stand vor der Entscheidung entweder das bestehende Berechtigungsverwaltungssystem mit Funktionen zur Rollenmodellierung erweitern zu lassen oder durch eine Standardlösung zu ersetzen. Im Falle eines Ersatzes konnte das Rollenmodul der bestehenden Provisionierungslösung eingesetzt werden oder die RBAC Lösung eines anderer Anbieter evaluiert werden.

Die Herausforderung

Das Rollenmodul muss die Möglichkeit bieten sämtliche Berechtigungen aller Anwendungen in einem firmenweiten Rollenmodell abzubilden. Hierbei darf es nicht darauf ankommen, ob die Anwendung bereits in das bestehende Identity Management System integriert ist. Alle über zugewiesene Rollen erhaltenen Berechtigungen müssen in die entsprechenden Systeme übertragen werden können, entweder automatisch oder manuell über ein Ticket an den HelpDesk.

Die Zuteilung von Rollen muss über verschiedene Mechanismen möglich sein. Es gibt organisatorische Rollen, welche automatisch auf Grund der Abteilung vergeben werden, in welcher ein Mitarbeiter tätig ist. Sogenannte „bedingte" Rollen müssen einem Mitarbeiter automatisch zugewiesen werden, wenn ein Mitarbeiter bestimmte Bedingungen erfüllt.

Ein grosser Teil der Rollen muss aber von den Mitarbeitern selbst beantragt werden können. Ein entsprechender Genehmigungsprozess muss sicherstellen, dass kein Mitarbeiter ohne die Zustimmung der verantwortlichen Personen den Zugang zu einer Anwendung oder Funktion innerhalb einer Anwendung erhält. Es muss jederzeit nachvollziehbar sein, wann ein Mitarbeiter über welche Rechte verfügt hat und wer diese bewilligt hat.

Softwarepakete sollen automatisch über entsprechende Berechtigungs-

Helsana Versicherungen AG

«Mit dem neuen Rollenmodell, der automatischen Verteilung von Rollen und der Möglichkeit dass Mitarbeiter über den Rollen- und Applikationskiosk selbständig Berechtigungen und Software beantragen können, konnte auf der einen Seite der HelpDesk stark entlastet werden und auf der anderen Seite die Sicherheit und die Nachvollziehbarkeit von User Berechtigungen massiv verbessert werden.»

Franz Schnyder
Verantwortlicher Helsana Directory Services

rollen auf die einem Mitarbeiter zugewiesenen Arbeitsplätze verteilt werden können. Zusätzliche Softwarepakete oder die Installation einer bereits genehmigten Software auf einer zusätzlichen Arbeitsstation müssen vom Mitarbeiter beantragt werden können. Nach erfolgtem Genehmigungsprozess soll die Software automatisch durch das vorhandene Softwareverteilungswerkzeug installiert werden.

Aufgrund der Vielzahl von Berechtigungsrollen müssen diese in Kategorien und Subkategorien aufgeteilt werden können. Die Suche nach Berechtigungsrollen muss sowohl über diese Kategorien als auch über die Rollenbeschreibung mit Stichwörtern und Textblöcken möglich sein.

Gewisse Kombinationen von Berechtigungen müssen auf Grund von geschäftskritischen Prozessen gegenseitig ausgeschlossen werden können (SoD Bedingungen, „Segregation of Duties“) oder bedürfen einer speziellen Genehmigung.

Die Lösung

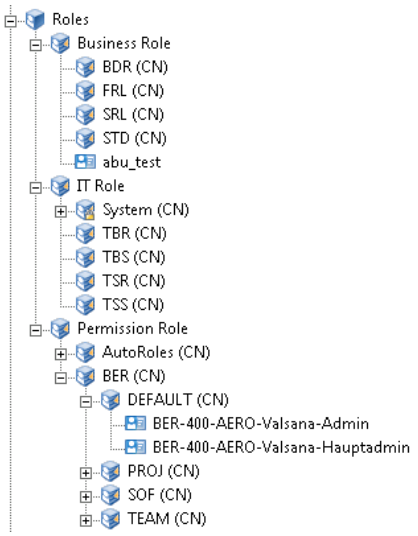
Helsana hat sich nach längerer Evaluation entschieden das im Novell Identity Manager erhältliche Role Based Provisioning Modul (RBPM) für Ihre Zwecke einzusetzen. Ausschlaggebender Grund war nicht die nahtlose Integration in das bereits seit sieben Jahren erfolgreich betriebene Novell Identity Management System. Ausschlaggebend war die Flexibilität der Lösung.

Das erarbeitet firmenweite Rollenmodell mit über 10'000 Rollen konnte mit allen Spezialitäten der Rollenhierarchien, Kategorien und Subkategorien, Mehrsprachigkeit in das System über einfache Textfile Imports eingelesen werden.

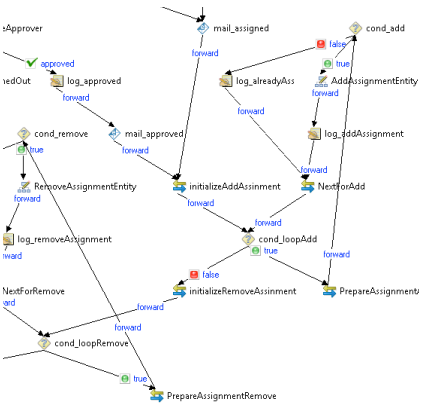
Die Vergabe der Rollen kann automatisch auf Grund von organisatorischen Strukturen erfolgen, dynamisch durch Bedingungen, die frei definiert werden können oder durch den Mitarbeiter selbst über einen Rollenkiosk in Form eines Web Portals.

Das RBPM Modul erlaubte die Implementierung aller notwendigen Genehmigungsprozesse zur Beantragung von zusätzlichen Berechtigungsrollen und Softwarepakete. Sämtliche Genehmiger werden via Mail auf Ihre Aufgaben hingewiesen und erhalten im Mail einen Link zum Portal, in welchem Sie Ihre Aufgaben wahrnehmen müssen. Sollten Prüfer Ihre Aufgabe nicht im vordefinierten Zeitraum wahrnehmen, werden Sie via Mail gemahnt oder der Genehmigungsprozess wird an einen Vorgesetzt eskaliert.

Abwesenheiten von Mitarbeitern durch Ferien oder Ausbildung können über Delegierungen und Stellvertretungen geregelt werden. Somit bleiben anstehende Genehmigungsprozesse nicht unnötig lange liegen oder werden ggf. vom System automatisch wegen Zeitüberschreitung abgelehnt.



Ein der Organisation angepasstes strukturiertes Rollenmodell vereinfacht die Verwaltung der Rollen und bietet eine übersichtliche Darstellung der Berechtigungen.



Genehmigungsprozesse helfen bei der Einhaltung von Richtlinien und garantieren die Nachvollziehbarkeit.

Wechselt ein Mitarbeiter die Abteilung wird automatisch ein Rollen Rezertifizierungsprozess gestartet. Sämtliche dem Mitarbeiter individuell zugewiesenen Rollen müssen vom neuen Vorgesetzten bestätigt werden.

Die Zuteilung der jeweiligen Berechtigungen, die ein Mitarbeiter auf Grund seiner zugeteilten Rollen erhalten hat, erfolgt auf zwei Arten. Ist ein System in das Identity Management System integriert, werden die benötigten Gruppenmitgliedschaften, Profile oder applikationsspezifischen Rollen sofort zugewiesen. Bei einem nicht integrierten System erfolgt die automatische Auslösung eines Tickets auf dem bestehenden Ticket System. Ein für diese Anwendung verantwortlicher Administrator weist dem Mitarbeiter auf Grund der im Ticket enthaltener Informationen manuell die entsprechenden Berechtigungen zu. Er Bestätigt danach das Ticket.

Der Mitarbeiter ist jederzeit darüber informiert wo sich sein Antrag aktuell befindet. Er sieht welche Genehmigungen ausstehend sind oder welches Ticket auf Grund seines Antrages noch pendent ist.

Der Kundennutzen

Die Zuteilung von Berechtigungen erfolgt heute zum grossen Teil automatisch auf Grund von organisatorischen Strukturen oder Bedingungen, die ein Mitarbeiter erfüllt. Nur ein kleiner Teil der Berechtigungen muss vom Mitarbeiter, Vorgesetzten oder vom HelpDesk nachträglich beantragt und genehmigt werden.

Zusätzliche Berechtigungen oder Softwarepakete können vom Mitarbeiter selbst beantragt und von den entsprechenden Stellen genehmigt werden. Dadurch ist der HelpDesk von diesen Tätigkeiten stark entlastet worden.

Sämtliche Rechte eines Mitarbeiters sind jederzeit nachvollziehbar. Zu welchem Zeitpunkt ein Mitarbeiter über welche Berechtigungen verfügt hat und wer diese genehmigt hat, kann sofort ermittelt werden.

SKyPRO Lösung

- *Novell Identity Manager v4*
- *Role Based Provisioning Modul*
- *User Self Service Portal*
- *Diverse Workflows*

Realisationszeit

April 2011 – März 2012

Ihre Ansprechpartner

Helsana Versicherungen AG
Ringstrasse 12
8600 Dübendorf

SKyPRO AG
Herr Roger Zimmermann
Gewerbestrasse 7
6330 Cham

Telefon:
041 741 47 70

eMmail:
roger.zimmermann@skypro.ch