Statement of the Month – Novell Identity & Security

Düsseldorf im Februar / März 2008

Rollenmanagement – Teamwork zwischen IT und Fachabteilungen gefragt

Viele Unternehmen haben begriffen, dass ihnen Identity Management hilft, den Verwaltungsaufwand zu verringern und Compliance-Aufgaben zu erfüllen. Doch auch innerhalb des Identity Managements gibt es noch unausgeschöpftes Potenzial, etwa dazu wie man die Administration noch effizienter gestalten kann. Marina Walser, Director Identity & Security Management Novell Central Europe, zeigt auf, dass zum Beispiel Rollen ein wertvolles Instrument an die Hand geben, um die Zuweisungsprozesse im Identity Management zu automatisieren.

Wenn man ein neues Aufgabengebiet innerhalb eines Unternehmens antritt, will man meistens sofort richtig durchstarten. Lästig nur, wenn die entsprechenden Ressourcen dann nicht schnell genug zur Verfügung stehen – man verliert dabei nicht nur viel Zeit, sondern leider auch häufig schon viel des Elans, den man am Anfang mitbringt. Umso besser, wenn in der zentralen Administration bereits hinterlegt ist, welche Gruppe oder Rolle auf welche Systeme Zugriff hat. Im Rahmen des Identity Managements muss die Identität dann nur noch mit dieser Rolle kurzgeschlossen werden und schon kann die Post abgehen. Durch ein solches Rollenmanagement lassen sich Provisioning-Prozesse im Identity Management automatisieren, was wiederum die Verwaltung vereinfacht und hilft Compliance-Anforderungen einzuhalten, etwa wenn bei einer anstehenden Rezertifizierung viel leichter belegt werden kann, wer wann was mit welcher Information gemacht hat.

Um die genannten Vorteile nutzen zu können, müssen diese Rollen natürlich zunächst einmal definiert werden – was nicht immer ganz leicht ist. Aus technischer Sicht ist das Problem schnell behoben, denn für Analyse und Management komplizierter Rollenmodelle gibt es heute gut funktionierende Lösungen. Mit diesen lassen sich leicht entsprechende Richtlinien für funktionsbasierte Berechtigungen erstellen und verwalten. Anhand dieser Richtlinien werden bestimmten Benutzergruppen Mitgliedschaften oder die Einrichtung von Konten in verschiedenen angeschlossenen Systemen erlaubt. So können beispielsweise Berechtigungsrichtlinien für den Vertrieb definiert werden, die allen Benutzern der Vertriebsmannschaft Anspruch auf eine bestimmte Mitgliedschaft, ein Lotus Notes-Benutzerkonto und ein Microsoft Active Directory-Konto gewährt.

So viel zur technischen Ebene. Die entscheidende Dimension des Rollenmanagements liegt jedoch woanders: Um zu erfahren, welche Berechtigungen diese Rollen tatsächlich haben sollen, muss man die zentrale Ebene verlassen und in die Einzelsysteme gehen, wo diese Berechtigungen geregelt sind. Das hat zur Folge, dass es zwei Bereiche gibt, die in ständiger Abstimmung stehen müssen, um sicher zu stellen, dass die Gruppen und Rollen in den Systemen mit den Informationen des zentralen Identity Managements übereinstimmen. Diesem Bruch, auf den auch Fachautor Martin Kuppinger verschiedentlich hingewiesen hat, muss man auf organisatorischer Ebene begegnen. Dafür braucht es klare Regelungen zwischen der IT in der Zentrale und den Fachabteilungen an den Systemen – dafür müssen sich beide an einen Tisch setzen.

Dieser Prozess kann aber heute ebenfalls verkürzt und vereinfacht werden. Theoretisch geschieht dies durch den Ansatz der Rollenbasierten Zugriffskontrolle (Role Based Access Control, RBAC). Allerdings ist mit diesem rein theoretischen Ansatz in der Praxis noch nicht viel erreicht. Die Umsetzung des RBAC galt in der Vergangenheit als schwierig und schwer zu managen. Das hat sich mittlerweile geändert: Dazu trägt zum Beispiel der RBAC Standard ANSI INCITS 359-2004 bei, der die grundsätzliche Rollenaufteilung in die drei Bereiche Elementarrolle, Technische Rolle und Organisatorische Rolle vorgibt. Außerdem gibt es heute auch Software-Lösungen – etwa als Teil der Identity Management-Lösung –, die die Brücke zwischen IT und Fachabteilungen schlagen helfen. Diese geben nämlich den Vertretern der Fachabteilungen und/oder der Geschäftsleitung hilfreiche Tools oder ganze Prozesse an die Hand, mit denen sie rollenbasierte Zugriffskontrollen eigenhändig implementieren und organisieren können.

Aber auch wenn man eine solche Lösung in den Dienst nehmen und die entsprechenden Prozesse aufsetzen will – Grundlage ist immer der profunde Austausch zwischen IT und Geschäftsseite. Hier empfiehlt sich ein klassischer Top-Down-Ansatz: Um einen Überblick über die Abteilungen und die Bedeutungen der in diesen vertretenen Funktionen für das Unternehmen zu gewinnen, sollte die IT sich zunächst mit der Geschäftsleitung verständigen. Das hat auch den Vorteil, dass man sich nicht zu sehr im Detail verzettelt, was einem in den Fachabteilungen immer passieren kann. Dann kommt der Austausch mit der Fachabteilung, die Input liefern muss über Funktionen und Aufgaben, die mit einer bestimmten Rolle verbunden sind. Sie liefern das detaillierte Verständnis der Rollen und Funktionen. Und schließlich gehört auch die Personalabteilung mit an den Tisch, denn sie verfügt über die Informationen zu den Lebenszyklen

bestimmter Mitarbeiterrollen und deren rechtliche Einbettung in die Organisation.

Erst wenn diese Informationen eingeholt sind, lassen sich Lösungen effizient in Betrieb nehmen, das heißt: die rollenbasierte Zugriffskontrolle schon auf Ebene der Fachabteilung angehen. Dies führt zu einer Überwindung des Bruches zwischen Einzelsystemen und zentralem Identity Management, was die bekannten Vorteile bringt: Hat man alle Hausaufgaben gemacht, dann sollte sich binnen kurzer Zeit dank der automatisierten Änderungsprozesse eine deutliche Produktivitätssteigerung einstellen. Die Verwaltungskosten sinken, Mitarbeiter bekommen ihre Ressourcen schneller zugewiesen, sind also zufriedener und arbeiten produktiver. Das gesamte komplexe Thema rund um die Berechtigungen wird wesentlich vereinfacht und ist im Sinne von Compliance-Anforderungen bestens nachvollziehbar.

Über Novell
Novell, Inc. (Nasdaq: NOVL) bietet Infrastruktur-Software für das Open Enterprise an. Novell ist eines der führenden Unternehmen bei unternehmensweiten Betriebssystemen für Unternehmen auf Basis von Linux und Open Source sowie bei Sicherheits- und System Management Services, die benötigt werden, um heterogene IT-Umgebungen zu betreiben. Novell unterstützt seine Kunden dabei, Kosten, Komplexität und Risiken zu reduzieren, damit sie sich auf Innovation und Wachstum konzentrieren können. Das Unternehmen mit Hauptsitz in Waltham, Massachussets (USA), beschäftigt weltweit rund 4.700 Mitarbeiter. Seit 1986 ist Novell durch die Novell GmbH in Düsseldorf auch auf dem deutschen Markt vertreten. Von diesem Standort aus werden Vertrieb und Marketing für Deutschland, Österreich und die Schweiz koordiniert - Niederlassungen befinden sich in Berlin, Frankfurt, München, Nürnberg, Wien, Zürich und Genf. Weitere ausführliche Informationen über Novell Lösungen, Produkte und Services stehen im Internet zur Verfügung unter www.novell.com oder www.novell.de.

Pressekontakt:

Lars Basche
Text 100 Public Relations
Tel: +49 - (0)89 - 99 83 70-33
E-Mail: novell@text100.de