WHITEPAPER

ROLE BASED ACCESS CONTROL (RBAC)

TOOLS4EVER
IDENTITY GOVERNANCE & ADMINISTRATION

INHALT

VORWORT

Im Identitäts- und Accessmanagementbereich erscheint der Begriff immer öfter: RBAC (Role Based Access Control). Der Grund: Organisationen wollen zunehmend – teilweise infolge von Normierungen wie z.B. ISO – alle Berechtigungen im Netzwerk strukturiert verwalten und zuweisen. Ermöglichen kann dies die RBAC-Software. Doch wie lässt sich RBAC richtig in der Organisation anwenden?

Das Gewähren bzw. Entziehen von Berechtigungen kennt zwei Problematiken: Bei der Erteilung von Berechtigungen wird regelmäßig eine Kopie eines Kollegen, des "Beispielanwenders", erstellt. Hierbei besteht die Gefahr, dass der neue Mitarbeiter unberechtigt Zugang zu bestimmten Anwendungen und Systemen erlangt. Wenn man eine Kopie eines anderen Mitarbeiters anfertigt, beachtet man zudem zu wenig den Entzug von Berechtigungen. Schließlich ist es wichtiger, dass der Arbeitnehmer zunächst seine Arbeit verrichten kann, und nicht so sehr, dass er vielleicht zu viel tun könnte. Im Rahmen der (ISO-) Normierungen, dank IT-Auditoren, aber auch durch unnötige Lizenzgebühren, u.a. für Microsoft Visio, Projects und Adobe CS, erkennen Organisationen immer mehr die Notwendigkeit, Berechtigungen zu standardisieren. Eine Lösung kann dabei RBAC sein.

Dieses Whitepaper erklärt, was "Role Based Access Control" bedeutet, wie es sich optimal einsetzen lässt und den Ansatz, der von Tools4ever verfolgt wird.

ROLE BASED ACCESS CONTROL – ERKLÄRUNG

RBAC ist eine Methode zur Verwaltung der Berechtigungen innerhalb einer Organisation. Hierbei werden die Berechtigungen nicht einzeln, sondern anhand von RBAC-Rollen gewährt, die sich aus Abteilung, Funktion, Standort und Kostenstelle eines Mitarbeiters in einer Organisation ergeben. Zwar erkennen Organisationen oft die Bedeutung der RBAC, fürchten aber deren Implementierung. Zu Unrecht entstand der Eindruck, RBAC hieße - vor allem in der Verwaltung – viel Arbeit und lange, komplexe Implementierungsperioden.

Die Verantwortlichen für RBAC-Implementierungen glaubten irrtümlich, wirklich alle Mitarbeiter müssten in eine RBAC-Rolle einfließen. Dabei hat oft eine Organisation genauso viele Funktionen wie Mitarbeiter. So entsteht hinsichtlich der Ressourcen eine endlose Liste von Rollen und folglich ein langwieriger Prozess, um allen Mitarbeitern eine RBAC-Rolle zuzuweisen. Daneben stellt sich die Frage, ob wirklich alles und jeder in die RBAC Matrix muss. Brauchen nicht eigentlich nur jene Nutzergruppen RBAC, für die die Berechtigung vom Standpunkt des Risikomanagements, der Regulierung oder der Effizienz sorgfältig einzurichten ist?

Wie dem auch sei: RBAC geht auch anders ... schneller und weniger komplex. Ein RBAC-Spezialist kann Ihnen zeigen, welcher Ansatz erfolgreich ist.

ROLE BASED ACCESS CONTROL – UMSETZUNG

Tools4ever geht bei RBAC von unten nach oben und etappenweise vor. Dabei wird zuerst ein Fundament gelegt, das sich später ausbauen lässt. Wie der Zugriff auf bestimmte Standardanwendungen, wie Microsoft Office und Outlook, der für die meisten Mitarbeiter gilt. Für viele Mitarbeiter können Berechtigungen auf Organisationsebene (Anmelden, Textverarbeitung, E-Mail) bzw. Abteilungsebene (Zugriff auf gemeinsam von der Abteilung genutzte Ressourcen und auf Abteilungsanwendungen) sofort erteilt werden. Dann ist es wichtig, bei den aktiven Arbeitsverhältnissen die 50 meist vorkommenden Kombinationen aus Abteilung und Funktion zu bestimmen.

HRM-System als Basis

Um diese Kombinationen zu definieren, ist das HRM-System eine gute Ausgangsbasis, ein erster Schritt zum Rollenmodell auf Organisationsebene. Ein Beispiel: Ein Krankenhaus in Erfurt hat eine chirurgische Abteilung, wo eine Krankenschwester tätig ist. Ihre Funktion ist also Krankenschwester. Anhand von Funktion, Abteilung und Standort aus dem HRM-System lässt sich die Organisationsrolle erstellen (siehe Abbildung 1). Dies ist in diesem Fall z.B. "Krankenschwester", "Krankenschwester in Erfurt" und "Krankenschwester Chirurgie". Ist die "Krankenschwester" und die "Chirurgie" definiert, so ist eine Krankenschwester in der Chirurgie automatisch "Krankenschwester" + "Chirurgie" und erhält automatisch alle entsprechenden Rollen.

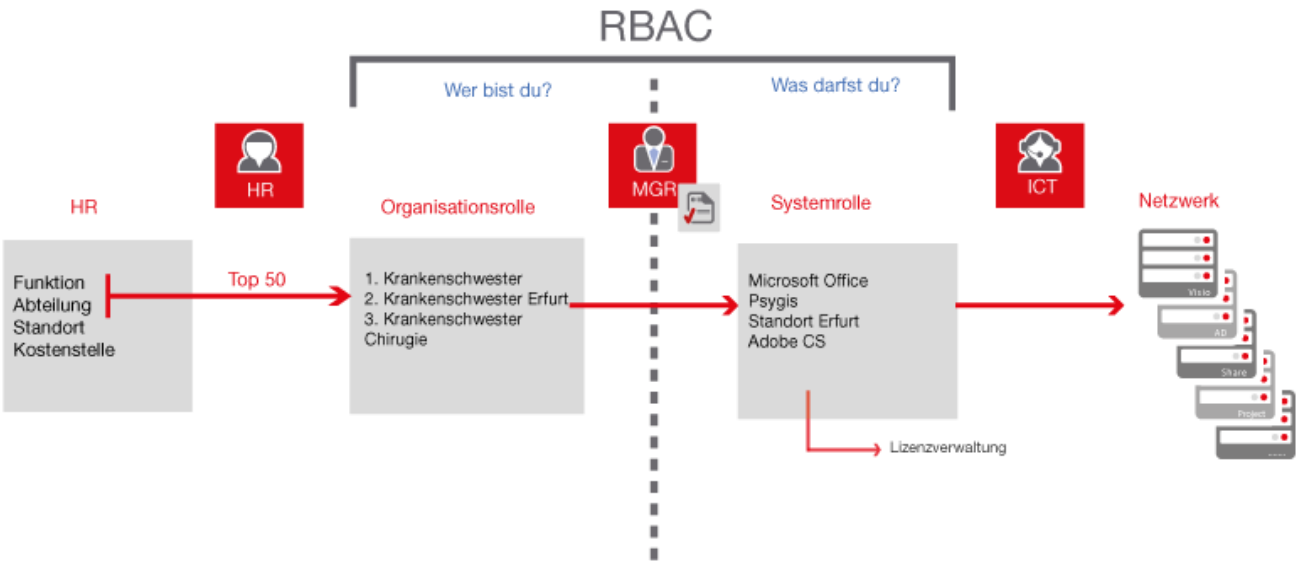

Abbildung 1: HRM-System als Basis

80 % der RBAC-Tabelle ausgefüllt

So lässt sich in den meisten Fällen ganz leicht über 80 % der RBAC-Tabelle ausfüllen. Ein großer Vorteil ist hierbei, dass neue Mitarbeiter in den ersten Tagen schon arbeiten können und dass Zeit verfügbar wird, um spezifische Rechte auf Anwendungs- und Systemebene zuzuweisen.

Im nächsten Schritt werden diese Organisationsrollen in Anwendungs- oder Systemrollen übersetzt, die die restlichen 20 % der RBAC-Tabelle ausmachen. Die Basis wurde gelegt, und nun entstehen weitere Schichten. Die Systemrollen kann dabei ein Manager gut zuteilen. Er - und nicht die HR-Abteilung - ist schließlich für die Berechtigungen seiner Mitarbeiter verantwortlich. Per E-Mail-Benachrichtigung und/oder Web-Formular wird über einen Workflow beim zuständigen Manager nachgefragt, welche spezifischen Rechte und Anwendungen der jeweilige Mitarbeiter benötigt. Dabei hält die RBAC-Software fest, welche Entscheidungen der Manager trifft. Mit diesen Informationen lassen sich zusätzlich leere Abschnitte der RBAC-Tabelle definieren und so ganz ausfüllen. So kann ein führender Mitarbeiter die Rollenvergabe in seiner Abteilung verwalten oder diese Aufgabe an andere delegieren. Auch können anhand der Entscheidung des Managers weitere Workflows gestartet werden. Auf diese Weise kann ein Manager genau bestimmen und verwalten, was in seiner Abteilung oder Kostenstelle passiert.

Detailberechtigungen

Die System- und Anwendungsrollen umfassen die Detailberechtigungen für den Mitarbeiter. Die ICT und die funktionale/technische Anwendungsverwalter (siehe Abbildung 1) ermöglichen den tatsächlichen Zugriff auf das Netzwerk. Diesen Teil (Provisioning) kann man auch automatisieren - mittels Identity-Management-Software.

Der Vorteil dabei ist, dass sich die RBAC auf diese Weise sehr schnell implementieren lässt. Tools4ever kann in 2 Monaten für die Organisationen den ersten Standard erstellen; andere Anbieter arbeiten hieran fast ein Jahr.

Außerdem kann man SoD (Segregation of Duty) bequem realisieren, indem z. B. bestimmte Berechtigungen bei verbotenen Kombinationen aus Funktionen und Abteilungen verweigert werden. Bei einer Reorganisation muss nicht die ganze RBAC-Tabelle neu erstellt werden. Anzupassen ist nur der erste Teil von Abbildung 1 – "Wer bist du" – und das ganz einfach im HRM-System. Nutzt der Manager das HRM-System als Basis und konsultiert es immer wieder, hat er ständig die neuesten Informationen und eine Übersicht mit Funktion, Abteilung, Standort und Kosten seiner Mitarbeiter zur Verfügung. Eine direkte Verbindung mit dem HRM-System ist also nötig, da dieses alle Informationen liefert. Eine solche Verbindung kann Tools4ever mit dem User Management Resource Administrator (UMRA) herstellen.

ROLE BASED ACCESS CONTROL – UMRA

Tools4ever unterstützt Role Based Access Control (RBAC) als Grundlage, um in den Informationssystemen Berechtigungen zuzuweisen. Solange die Beziehung zwischen Funktion/Abteilung/Aufgaben und Ressourcen innerhalb einer Organisation bekannt ist, kann der Provisioning-Prozess darauf basieren. Tools4ever kann die RBAC mittels "User Management Resource Administrator (UMRA)" schnell und ergebnisorientiert implementieren. UMRA umfasst ein einmaliges Toolset, um die RBAC praktikabel auszufüllen, sofort Ergebnisse zu erzielen und eine Basis zum weiteren Ausfüllen der RBAC-Tabelle zu legen.

UMRA und RBAC

Um RBAC zügig und ergebnisorientiert zu implementieren, bietet UMRA mehrere Optionen, um leere, teilweise oder ganz ausgefüllte RBAC-Tabellen zu bearbeiten.

Keine RBAC-Tabelle vorhanden

Ist keine RBAC-Tabelle vorhanden, kommt oft das "Kopieren von Rechten und Anwendungen“ eines bestehenden Users oder aber eine bestimmte Benutzervorlage zum Einsatz. Der Nachteil dieser Methode ist, dass die Rechtenvergabe nicht eindeutig und standardisiert geschieht. Oft passiert es, dass die User mit der Zeit viel zu viele Rechte im Netzwerk haben. Wenn mit UMRA ein Identity Management System implementiert wird, wird die aktuelle Methode (copy user oder template user) meistens erstmal beibehalten. (Die Abhängigkeit von einem RBAC-Projekt verzögert eine IDM-Implementierung sonst oft um Monate oder sogar Jahre). Durch UMRA werden dann die Accounts stets gleichförmig und standardisiert erstellt. Somit wird eine Basis geschaffen, um Daten zum Ausfüllen einer leeren RBAC-Tabelle zu sammeln.

Teilweise ausgefüllte RBAC-Tabelle

Eine RBAC-Tabelle vollständig auszufüllen ist sehr aufwendig, sie teilweise auf Abteilungsebene auszufüllen, jedoch ganz leicht. Darüber hinaus sind oft viele Mitarbeiter vorhanden, für die sich die RBAC-Tabelle sehr einfach ausfüllen lässt. Eine so ausgefüllte RBAC-Tabelle ist im Benutzer-Management bereits sehr vorteilhaft. Für einen neuen Mitarbeiter können schließlich alle Gruppen auf Organisationsebene (Anmelden, Textverarbeitung, E-Mail) bzw. Abteilungsebene (Zugriff auf gemeinsam von der Abteilung genutzte Komponenten und auf Abteilungsanwendungen) sofort zugewiesen werden. Der neue Mitarbeiter kann schon in den ersten Tagen arbeiten, und es steht mehr Zeit Verfügung, um die spezifischeren Rechte zuzuweisen. Erkennt UMRA einen nicht ausgefüllten RBAC-Tabellenteil, wird automatisch der Manager des betreffenden Mitarbeiters eingeschaltet und per E-Mail und UMRA (Web-) Formular wird angefragt, welche spezifischen Rechte und Anwendungen der Mitarbeiter benötigt. UMRA legt die Auswahl des Managers fest. Diese Angaben dienen dazu, leere RBAC-Tabellenteile weiter zu definieren.

Gänzlich ausgefüllte RBAC-Tabelle

Eine RBAC-Tabelle vollständig auszufüllen ist sehr aufwendig, aber letztlich ein perfektes Werkzeug, um jedem einzelnen Mitarbeiter die richtigen Rechte und Anwendungen zuzuweisen. UMRA regelt mit der RBAC-Tabelle die Zuweisung von Rechten und Anwendungen für einen neuen Mitarbeiter, sogar auch, wenn sich dessen Rolle und/oder Funktion bzw. die Abteilung ändert. Auch komplexere Situationen werden unterstützt, z. B. bei Mitarbeitern, die Teilzeit in zwei verschiedenen Abteilungen arbeiten; oder wenn ein Mitarbeiter eine Zeit lang für seine ehemalige Abteilung weiter arbeitet usw. UMRA kann die RBAC-Angaben im eigenen System speichern oder auch eine Standard-Software von Drittanbietern verwenden.

ROLE BASED ACCESS CONTROL – SCHLUSSFOLGERUNG

RBAC kann Zugriffsberechtigungen effizient, transparent und überprüfbar definieren. Deshalb sind derzeit viele Organisationen daran interessiert. Die Implementierung muss auf keinen Fall komplex sein. Wir raten, RBAC schichtweise umzusetzen, wobei Berechtigungen auf Organisations- und Abteilungsebene (über das HRM-System) automatisch erfolgen und man sich auf die Top-50-Kombinationen aus Funktion und Abteilung konzentriert. So läßt sich 80 % der RBAC-Tabelle ganz schnell und einfach ausfüllen. Die Berechtigungen der restlichen 20 % auf der Detailebene bereiten den Organisationen indes erhebliche Kopfschmerzen. Um auch sie praktikabel im RBAC-Modell zu meistern, sollte möglichst der Manager des jeweiligen Mitarbeiters die Berechtigungen zuweisen. Er kann die Detailberechtigungen der Mitarbeiter bestimmen und anpassen.

Pyramide

Diese Methode kann auch in einer Pyramide (siehe Abbildung 2) dargestellt werden.

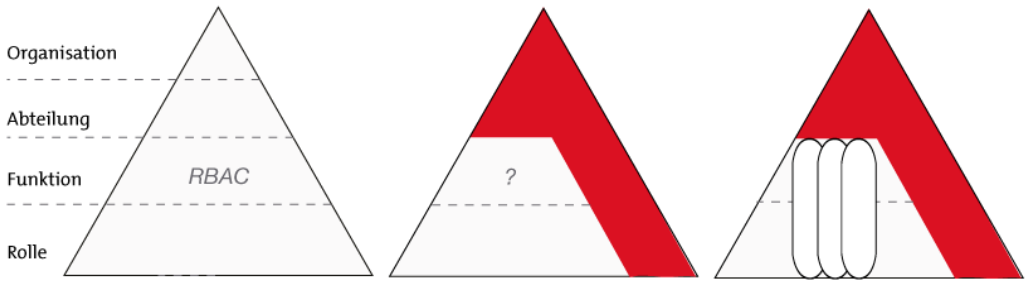

Abbildung 2: RBAC Pyramide

Von oben nach unten: von der Organisation (oben), über Abteilung, Standort, Funktion bis zur Einzelperson (Fundament). Die Pyramide wird ausgefüllt. Die Oberschicht (Organisation und Abteilung) umfasst nur für alle geltenden Berechtigungen. Dieser Bereich kann sofort ausgefüllt werden. Es ist ratsam, in der ersten Instanz bei Abteilung/Funktion das Ausfüllen zu beenden. Die letzten Details werden weiterhin ad-hoc, bspw. durch den Workflow, geregelt. Mit der Zeit sammelt so die Organisation immer mehr Informationen über die getroffenen ad-hoc Entscheidungen der Manager. Der Security Officer kann diese Information dann nutzen, die RBAC-Tabelle von 80 % bis vielleicht weiter auf 100 % zu vervollständigen.

WER IST TOOLS4EVER?

Als führender Anbieter von "Identity & Access Management Software" bietet Tools4ever eine komplette Palette von "Identity & Access Management"-Lösungen, einschließlich Beratungsleistungen und strategische Anwendungen im Bereich von User Provisioning, Password Management, Single Sign On (SSO), Self-Service & Workflow Management, RBAC und Auditing & Compliance. Die Mission von Tools4ever besteht darin, praktikable und kostengünstige Lösungen im "Identity & Access Management" bereitzustellen.

Minimale Investition, maximales Ergebnis

Tools4ever zeichnet sich durch seinen No-Nonsense-Ansatz und die Möglichkeit aus, eine komplette Identity-Management-Lösung in wenigen Wochen gegenüber den z. Zt. anfallenden mehreren Monaten oder gar Jahren zu realisieren. Tools4ever verwendet eine phasenweise Implementierungsmethode, die kurzfristig schnell Ergebnisse liefert. So verfügen Sie über die Flexibilität und den Raum, in ihrem eigenen Tempo in Ihrer Organisation Identity Management schrittweise auf breiterer Ebene einzuführen.

Das Lizenzmodell von Tools4ever baut auf diesem schrittweisen Ansatz auf. So erfolgen die notwendigen Investitionen genau im Gleichschritt mit der Einführung in Ihrer Organisation. Dank dieser Methode und des umfassenden Portfolios ist Tools4ever im Identity & Access Management Bereich so erfolgreich.

Tools4ever arbeitet für kleine Firmen und weltweit agierende multinationale Unternehmen gleichermaßen, für Bildungseinrichtungen und Regierungen im In-und Ausland. Internationale Kunden sind u. a. Citi Group, EDF Electricité de France, Levi's, Motorola, Ericsson, Oracle, Lucent, NASA, Pentagon, verschiedene amerikanische Ministerien, wie Landwirtschaft und Verteidigung, die Universität von Cambridge, GE Plastics, IBM und Marks & Spencer, Heineken. In Deutschland und der Schweiz zählen zu den Kunden z.B.: Sixt, Tupperware, BKW FMB Energie, Nordzucker, ARAG Versicherungen, Ampega Gerling Asset Management, Oberfinanzdirektion Koblenz, Uni Klinikum Münster, Stadt Paderborn, Informatik Dienste der Stadt Bern und viele andere. Schon ab 300 Benutzerkonten liefert unsere Software ein sichtbares Ergebnis.

TOOLS4EVER INFORMATIK GMBH

Herrenstrunden 23a
51465 Bergisch Gladbach
Deutschland

T +49 2202 2859 - 0 F +49 2202 2859 - 299

Information info@tools4ever.de
Sales sales@tools4ever.de
Support support@tools4ever.de