

Het monster dat RBAC heet

ROLE BASED ACCESS CONTROL

In de wereld van identiteits- en toegangsbeheer komt de term RBAC (Role Based Access Control) steeds vaker voor. Steeds meer organisaties hebben namelijk - deels ingegeven door normeringen - de wens om alle autorisaties in het netwerk op een gestructureerde wijze te beheren en uit te delen. Maar hoe pas je RBAC op een goede manier toe binnen de organisatie? ARNOUIT VAN DER VORST

Tips voor RBAC

- Hanteer een bottom-up en gestapelde methode,
- gebruik het HRM-systeem als basis,
- bepaal de top vijftig combinaties van afdeling en functie van actieve dienstverbanden,
- laat detailautorisaties verlopen via de manager van de betrokken medewerker en
- verrijk de RBAC-tabel via reviews door de security-officer.

Er bestaan twee valkuilen bij het toekennen en ontnemen van autorisaties. Regelmatig wordt bij het toekennen van autorisaties een kopie gemaakt van een 'voorbeeldgebruiker', oftewel een collega. Het risico daarvan is dat de nieuwe medewerker zo onterecht toegang kan krijgen tot bepaalde applicaties en systemen. Daarnaast wordt er te weinig aandacht besteed aan het ontnemen van autorisaties wanneer een kopie wordt gemaakt van een andere medewerker. Het is immers van groter belang dat de medewerker zijn werk kan doen en in eerste instantie niet wat er mogelijk teveel kan worden gedaan. Ingegeven door normeringen en IT-auditors, maar ook gedreven door onnodige licentiekosten voor onder andere Microsoft Visio, Projects en Adobe CS, zien organisaties het belang van op een verantwoorde manier omgaan met autorisaties.

Verkeerde aanpak

RBAC is een methode om het autorisatiebeheer binnen een organisatie in te richten. Volgens deze methode worden autorisaties niet op individuele basis toegelikt, maar op basis van rollen en die rollen zijn weer opgebouwd uit afdeling, functie, locatie en kostenplaats van een medewerker in een organisatie. Hoewel organisaties het belang van RBAC inzien, zijn zij bang voor de implementatie ervan. Onterecht is er een beeld ontstaan dat RBAC heel veel werk op gaat leveren - met name op het gebied van beheer - en dat implementatietrajecten lang en complex zijn. RBAC wordt gezien als een monster en dat is het resultaat van een verkeerde aanpak van de implementatie.

Verantwoordelijken voor RBAC-implematies hebben de illusie gehad dat honderd procent van de medewerkers in een RBAC-rol te vatten is. Er zijn vaak net zoveel functies als medewerkers binnen een organisatie. Daardoor ontstaat er een eindeloze opsomming van rollen ten opzichte van resources en dat betekent een langdurig proces om alle medewerkers een RBAC-rol toe te kennen. Daarnaast is het de vraag of alles en iedereen wel in RBAC moet. Is RBAC eigenlijk niet alleen nodig voor die gebruikersgroepen voor wie de autorisaties vanuit het oogpunt van risicomangement, regelgeving of efficiency zorgvuldig moeten worden ingericht? Hoe dan ook: RBAC kan anders, sneller en minder complex.

het HRM-systeem een prima bron. Dit is een eerste aanzet tot een rollenmodel op organisatieniveau. Een voorbeeld: een ziekenhuis in Leersum heeft een afdeling Chirurgie waarin de functie Verpleger voorkomt. Op basis van functie, afdeling en locatie uit het HRM-systeem kan de organisatirol worden gecreëerd (zie afbeelding 1). Dit is respectievelijk 'Verpleger', 'Verpleger in Leersum' en 'Verpleger Chirurgie'. Wanneer 'Verpleger' en 'Chirurgie' zijn gedefinieerd dan is een verpleger op de afdeling chirurgie automatisch 'Verpleger' + 'Chirurgie' en krijgt hij automatisch de stapeling van de rollen. Op deze manier kan zeer eenvoudig ruim tachtig procent van de RBAC-tabel worden gevuld. Een groot voordeel hiervan is dat nieuwe medewerkers de

RBAC wordt gezien als een monster en dat is het resultaat van een verkeerde aanpak van de implementatie

Bekende RBAC-hulpmiddelen

- BMC Control SA en IdM
- CA eTrust
- HP Select Access
- IBM TIM en TAM (Tivoli Identity Manager en Tivoli Access Manager)
- Microsoft Authorization Manager (Azman)
- Novell Access Manager / Identity Manager / Role Based Provisioning Module
- Oracle/Sun Identity Management Suite

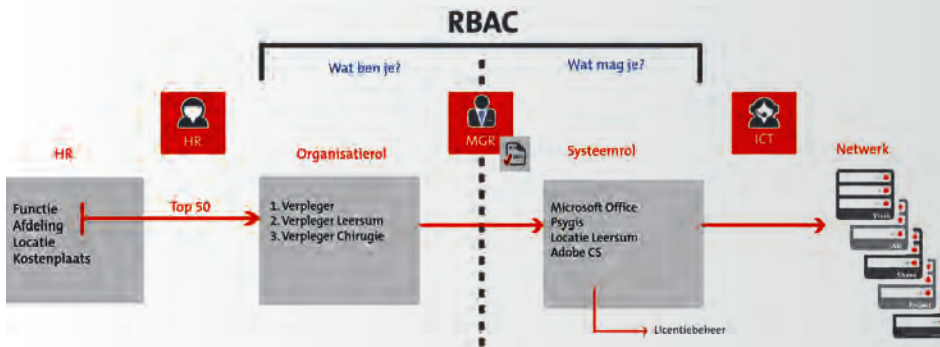
RBAC als lego

Het advies is om bij RBAC een bottom-up en gestapelde methode te hanteren, waarbij eerst een fundament wordt gelegd dat later verder kan worden uitgewerkt. Immers, toegang tot bepaalde standaardapplicaties zoals Microsoft Office en Outlook geldt voor het grootste deel van de medewerkers. Voor een grote groep medewerkers kunnen autorisaties op organisatieniveau (inloggen, tekstverwerken, e-mail) en afdelingsniveau (toegang tot afdelings-share en -applicaties) meteen worden toegekend.

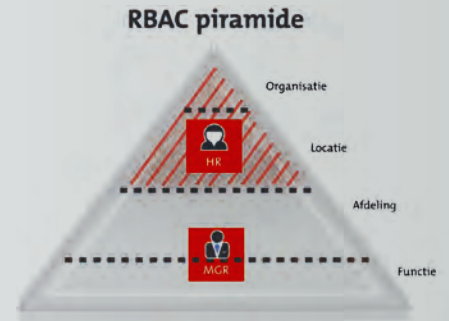
Het is daarom van belang om de top vijftig combinaties van afdeling en functie van actieve dienstverbanden te bepalen. Voor het bepalen van de combinaties is

eerste dagen alvast aan het werk kunnen en dat er tijd wordt gecreëerd voor het toekennen van specifieke rechten op applicatie- en systeemniveau.

Een volgende stap is om deze organisatirollen te vertalen naar applicatirollen of systeemrollen, dus de laatste twintig procent van de RBAC-tabel. De basis ligt er en nu wordt er verder gestapeld. Het toekennen van de systeemrollen kan goed worden uitgevoerd door een manager. Hij is tenslotte verantwoordelijk voor de autorisaties van zijn medewerkers, niet de HR-afdeling. Via e-mailnotificatie of een webformulier wordt via een workflow aan de juiste manager gevraagd wat de specifieke rechten en applicaties voor de betreffende me-



Afbeelding 1. Op basis van functie, afdeling en locatie uit het HRM-systeem kan de organisatie-rol worden gecreëerd.



Afbeelding 2. De methode voor het vullen van een RBAC-tabel is ook samen te vatten in een piramide.

dewerker moeten zijn. Vervolgens kan RBAC-software vastleggen welke keuzes de manager maakt en deze informatie kan worden gebruikt om lege delen van de RBAC-tabel verder te definiëren om uiteindelijk te komen tot een gevulde RBAC-tabel. Het is dus mogelijk om een leidinggevende alle vertalingen van rollen binnen zijn/haar afdeling te laten beheren met de mogelijkheid tot delegatie naar iemand anders. Of dat een actie van een manager via een workflow resulteert in een notificatie naar een licentiemanager. Op deze manier kan een leidinggevende exact bepalen

en beheren wat er binnen zijn/haar afdeling of kostenplaats gebeurt.

Detailautorisaties

De systeem- en applicatirollen bevatten de detailautorisaties binnen de betreffende applicatie zodat de rol kan worden uitgevoerd. De verantwoordelijkheid voor het daadwerkelijk toegang verschaffen tot het netwerk ligt bij ICT en Functioneel/Technisch Applicatie Beheer (zie wederom afbeelding 1). Het is ook mogelijk om dit gedeelte te automatiseren (provisioning) met identitymanagementsoftware.

Het voordeel van een RBAC-implementatie op deze manier is de snelheid van de implementatie. Binnen een tweetal maanden kan een eerste standaard worden neergezet. Daarnaast is het mogelijk om gemakkelijk SoD (Segregation of Duty) te krijgen door bijvoorbeeld bepaalde autorisaties te weigeren bij verboden combinaties van functies en afdelingen. In geval van een reorganisatie is het niet nodig om de gehele RBAC-tabel opnieuw te maken. Slechts het eerste 'Wie ben je'-gedeelte uit afbeelding 1 dient te worden aangepast en dat kan eenvoudig in het HRM-systeem. Door het HRM-systeem als basis te nemen en keer op keer te raadplegen, beschikt de manager continu over de meest actuele informatie en een gevulde dashboard met de functie, afdeling, locatie en kostenpost van zijn medewerkers. Een directe koppeling met het HRM-systeem is dus noodzakelijk omdat dat de bron is van alle informatie. Er zijn diverse leveranciers die een dergelijke koppeling kunnen verzorgen.

Piramide

Deze methode is ook te vatten in een piramide (zie afbeelding 2). Van boven naar beneden van organisatie (top), via afdeling, locatie, functie naar individu (grondlaag). De piramide wordt ingevuld en op de toplaag (organisatie en locatie) zijn er alleen autorisaties die voor iedereen gelden. Dit gedeelte kan direct worden ingevuld. Het advies is om in eerste instantie bij afdeling/functie op te houden met invullen. De laatste details zullen altijd ad hoc via bijvoorbeeld workflow geregeld blijven. Vervolgens kunnen organisaties de piramide verder invullen en daarmee ook de RBAC-tabel. ♦

Standaard

Het Amerikaanse NIST heeft een standaard voor RBAC gedefinieerd. Zie ook: <http://csrc.nist.gov/groups/SNS/rbac/>. De meeste producten op de markt zijn in staat om de standaard te volgen.

CONCLUSIE

RBAC staat op dit moment sterk in de belangstelling bij tal van organisaties, want met deze toegangsmethode kunnen autorisaties efficiënt, transparant en controleerbaar worden ingericht. Het implementeren van RBAC hoeft zeker niet complex te zijn. Het advies is om RBAC op een gestapelde manier te benaderen, waarbij autorisaties op organisatie- en afdelingsniveau automatisch verlopen (via het HRM-systeem) en waarbij gericht wordt op de top vijftig combinaties van

functie en afdeling. Op die manier kan tachtig procent van de RBAC-tabel zeer snel en eenvoudig worden gevuld. De autorisaties van de overige twintig procent op het gedetailleerde niveau geven organisaties veel hoofdbreken. Om ook deze twintig procent pragmatisch binnen het RBAC-model af te handelen is het advies om de toekenning van autorisaties te laten verlopen via de manager van de betrokken medewerker. Een manager kan de detailautorisaties van de medewerker

bepalen en aanpassen.

Door gebruik te maken van het RBAC-model verzamelt de organisatie door de tijd heen steeds meer informatie over keuzes en aanpassingen die gemaakt worden met betrekking tot het maken van autorisaties. Via een reviewslag van de security-officer kan deze informatie gebruikt worden om de RBAC tabel verder te verrijken en de tachtig procent te laten groeien tot wellicht honderd procent. Kennis en feedback vanuit de organisatie helpen het RBAC-monster te verslaan.

Arnout van der Vorst
(a.van.der.vorst@tools4ever.com) is Managing ICT-consultant bij Tools4ever.