Veiligheid en flexibiliteit met rollen.

Inleiding

Steeds meer toepassingen worden ontsloten in een publieke of private web-omgeving. Klanten en medewerkers krijgen toegang tot vele toepassingen die zijn verspreid over meerdere locaties.

Met de groei van het aantal ontsloten toepassingen wordt het verlenen van toegang onbeheersbaar en moeten gebruikers veelvuldig inloggen. Dan lijkt het handig om een centraal Identity Management Systeem [1] in te richten dat gebruikers centraal beheert en hen bedient met single sign-on.

Toegangsrechten worden meestal op basis van rollen aan gebruikers toegekend. Een reden hiervoor is dat door de groepering van rechten in rollen de administratieve last wordt beperkt.

Maar rollen bieden meer voordelen. Naast de administratieve eenvoud kunnen rollen de veiligheid van de dienstverlening vergroten en het beheer van toegangsrechten flexibel houden. De invoering van een nieuw IdM systeem biedt kansen om te profiteren van alle voordelen van rollen in plaats van door te gaan op oude voet. Hoe dat kan en welke rollen nodig zijn wordt in dit artikel getoond aan de hand van een gebruikelijk portal scenario.

Het portal scenario

Resources en toepassingen

Voordat we verder ingaan op het portal scenario en de benodigde rollen is het nodig om de begrippen resource en toepassing te definiëren.

Toepassingen kunnen bij elkaar horen of maken zelfs deel uit van hetzelfde informatiesysteem. Zo'n bij elkaar horende groep toepassingen noemen we een resource. Wat exact de grenzen van een resource zijn wordt door de organisatie zelf bepaald. Of overwegingen hierbij van organisatorische of technische aard zijn doet nu niet terzake; de grenzen van een resource kunnen samen vallen met een fysiek systeem maar dat hoeft niet. Wel essentiëel is dat een resource dé ingang voor één of meer toepassingen is.

Een toepassing is op zijn beurt weer een verzameling applicatieve functies met data die een gebruiker als een logisch geheel kan aanroepen.

Portal met SSO

Om de gebruiker zo gemakkelijk mogelijk toegang te geven tot zijn toepassingen wordt een portal ingericht. Op de portal kan de gebruiker inloggen waarna zijn persoonlijke pagina wordt gepresenteerd. Deze persoonlijke pagina toont de links naar de toepassingen waar de gebruiker heen kan surfen. Wanneer bij het inloggen ook single sign-on wordt geboden hoeft de gebruiker niet opnieuw in te loggen voor deze toepassingen: de portal werkt als centrale toegangspoort met SSO.

De persoonlijke pagina op de portal toont in principe alleen de toegestane toepassingen. Toch wordt doorklikken vanuit deze pagina en het direct toegang krijgen tot toepassingen zonder verdere controles als onveilig beschouwd. Een foute opbouw van de persoonlijke pagina en gebruikers hebben toegang tot toepassingen waar ze geen recht op hebben. Daarnaast is het altijd mogelijk dat gebruikers direct naar een toepassing surfen en dat niet via de portal doen waardoor überhaupt geen toegangscontrole zou plaatsvinden. In andere woorden, bij het benaderen van een toepassing moet altijd controle plaatsvinden.

Bij het benaderen van een toepassing passeren gebruikers altijd eerst de virtuele grens van de resource waarbinnen de toepassing zich bevindt. Bij de resourcegrenzen wordt gecontroleerd op een geldige identiteit, met andere woorden er wordt geauthenticeerd. Het centrale SSO-mechanisme van het IdM systeem voert de authenticatie uit aan de hand van een geldige SSO-sessie die de gebruiker bij het inloggen op de portal heeft gekregen[2].

Veiligheid en flexibiliteit met rollen

Soorten rollen

Het NIST onderscheidt in haar standaards voor Role Based Access Control twee soorten rollen: de Role Group en de Functional Role[3]. De Role Group weerspiegelt de organisatiestructuur en de Functional Role is een groepering van permissies of specifieke toepassingsrechten.

Een voorbeeld van een Role Group is een arts en een voorbeeld van een Functional Role is een toegangsrecht tot de agenda. De soorten rollen die nu aan de orde komen zijn Functional Roles.

[1] Identity Managmenent is het beheer van electronische identiteiten en toegangsrechten *[zie kader]*.

[2] Als er geen geldige SSO-sessie is wordt de gebruiker gevraagd om (nogmaals) in te loggen.

[3] Zie bijvoorbeeld Role Based Access Control Implementation standard, Version 0.1, January 2006, Draft

Veiligheid met resourcerollen
Na controle van de identiteit bij een resource zoals in het portal scenario beschreven vindt controle plaats of een gebruiker het toegangsrecht voor deze resource heeft. Dit toegangsrecht is vastgelegd als een resourcerol. Controle op een expliciete resourcerol vergroot de veiligheid van de toepassingen binnen een resource. Gebruikers die geen resourcerol hebben kunnen nooit bij één van de toepassingen binnen deze resource komen. Vergelijk het eens met een hotel: alleen als je een ingeschreven gast bent van het hotel, de resource, mag je doorlopen en op zoek gaan naar je eigen kamer, ofwel jouw toepassing.

Flexibiliteit met toepassingsrollen
Toegang tot een resource is de grove benadering van het verlenen van toegang. Binnen resources gelden de gedetailleerde toegangsrechten van de individuele toepassingen: dit is de fijne benadering. Vaak mag niet iedereen alle functies en data in een toepassing benaderen en zijn er zelfs meerdere toepassingsrollen voor één toepassing nodig. Naast de resourcerol bezit een gebruiker dus ook gedetailleerde toepassingsrollen.

Resourcerollen worden altijd vanuit het centrale IdM systeem opgevoerd. Deze rollen zijn immers gekoppeld aan het centrale SSO-mechanisme.

Het toekennen van toepassingsrollen kan, maar het hoeft niet, door een locale organisatie gebeuren; de toegekende rollen mogen in een locaal systeem worden vastgelegd in plaats van het centrale IdM systeem. In deze keuzes tussen locaal en centraal ligt de fexibiliteit verscholen.

Deze flexibiliteit is zeer welkom wanneer het toegangscontrole systeem van de legacy toepassingen moeilijk kan worden aangepast voor aansluiting op het centrale IdM systeem. Ook wanneer een locale organisatie met eigen processen de toegangsrechten voor de specifieke toepassing wil blijven uitgeven is flexibiliteit nodig in het locaal of centraal toekennen van rollen.

Vergelijkbare argumenten gelden voor de autonomie van een project tijdens de ontwikkeling van toepassingen.

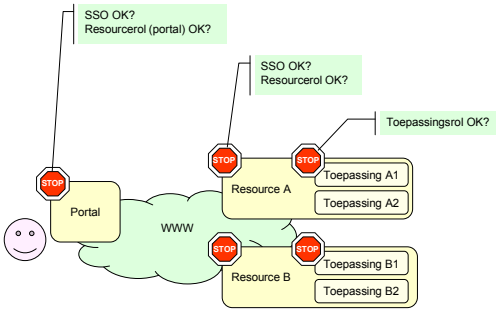
Rollenimplementatie in het portal scenario
De rollen
Het controleren op toegangsrechten heet autorisatie. Het portal scenario toont dat de autorisatie wordt ondersteund met twee soorten rollen:

- Resourcerollen voor de grove autorisatie bij de toegang tot een resource.
- Toepassingsrollen voor de fijne autorisatie binnen een resource.

De portal heeft ook een resourcerol
Hoewel in het spraakgebruik iedereen moet kunnen inloggen op de portal wordt met iedereen toch slechts een selecte groep gebruikers bedoeld. Ook voor de portal is het verstandig om een resourcerol aan te maken in het IdM systeem en deze 'portal rol' toe te kennen aan de selecte groep; de controle op een resourcerol voor toegang tot de portal houdt ongenode gasten immers eenvoudiger buiten de deur.

Door direct vanaf het begin van een IdM project de portalrol te hanteren, wordt een toekomstige implementatie van een tweede portal met een eigen gebruikersgroep ook eenvoudiger.

Implementatie
In de onderstaande figuur zijn de authenticatie en autorisatie in het portal scenario geschetst. Bij de authenticatie wordt de geldigheid van een SSO-sessie gecontroleerd en bij de autorisatie vindt controle op resourcerol of toepassingsrol plaats.



Bij het benaderen van een toepassing hoeft geen authenticatie meer plaats te vinden; de authenticatie, het vaststellen van een geldige identiteit, is al gebeurd bij het passeren van de resourcegrens.

Balans resourcerollen en toepassingsrollen
Bij het ontwerpen van een rollenstructuur moet een balans gezocht worden in de verhouding tussen resourcerollen en toepassingsrollen. In een extreme situatie kan voor elke specifieke functie in een toepassing een aparte resourcerol worden gedefiniëerd: elke functie heeft zijn eigen voordeur.

Op bovenstaande wijze zijn er geen toepassingsrollen nodig, maar de flexibiliteit in variatie tussen het locaal en decentraal toekenen van rechten verdwijnt en dat is vaak onacceptabel

voor legacy systemen en de locale IdM processen. Ook zal de performance van de centrale authenticatie en autorisatie controle voor toegang tot de grote aantallen resources de nodige aandacht behoeven. Controle op het wel of niet mogen uitvoeren van een specifieke functie tegen een locale rechtendatabase performed beter dan controle tegen een centrale repository.

Impact op het administratie- en het opvoerproces

Wat betekent nu de benadering met resourcerollen en toepassingsrollen voor het administratie- en het opvoerproces?

In de administratie moet duidelijk zijn op welke toepassingen een gebruiker recht heeft. Het gaat de gebruiker immers niet om toegang tot een resource maar om toegang tot een toepassing. Feitelijk worden in de administratie toepassingsrollen gebezigd. Resourcerollen zijn dan ook niet bekend in het administratieve proces!

De benodigde resourcerollen passend bij de geadminstreerde toepassingsrollen worden in het opvoerproces bepaald. Zonder een resourcerol kan een gebruiker nooit toegang tot een toepassing krijgen zoals eerder is uitgelegd. Het opvoerproces moet over een up-to-date mapping van resource- en toepassingsrollen beschikken Het schermt hiermee het administratieve proces af van de vaak technische of beheermatige structuur van de resource implementatie.

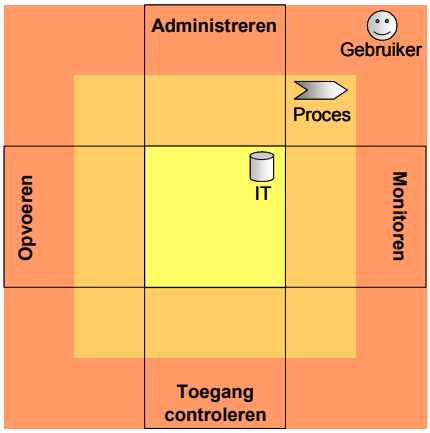
Conclusie

Met twee soorten rollen kan de toegang tot toepassingen veilig worden geïmplementeerd en flexibel worden beheerd: resourcerollen voor toegang tot resources en toepassingsrollen voor rechten binnen deze resources.

Wim Geurts en Guido Bezemer zijn consultant bij Largos. Largos is het adviesbureau voor informatie-beveiliging en risicobeheersing sinds 2001.
Contact: wim.geurts@largos.nl of www.largos.nl

Het identity management procesmodel

Identity management wordt gedefinieerd als het toekennen, beheren en gebruiken van electronische identiteiten, om veilig en gecontroleerd toegang te geven tot specifieke resources. Deze definitie toont al een natuurlijke opdeling in de vier identity management hoofdprocessen: Administreren, Opvoeren, Toegang controleren en Monitoren.



- *Administreren:* Het toekennen (of intrekken) van een electronische identiteit en toegangsrechten aan geïdentificeerde gebruikers.
- *Opvoeren:* Na administratie van de electronische identiteit moet deze met de beoogde rechten opgevoerd (of afgevoerd) worden in de technische identiteiten databases.
- *Toegang controleren:* De toegangscontrole of access control waakt over de resources. Alleen na geslaagde authenticatie én autorisatie wordt een gebruiker toegang verleend.
- *Monitoren:* Onterecht opgevoerde of achtergebleven identiteiten en rechten of het frauduleus gebruik van identiteiten moeten worden opgespoord en gerapporteerd

Van buiten naar binnen zijn in het model de gebruikers, de processen en de IT met identiteiten databases, als aparte lagen geschetst in alle vier de hoofdprocessen. Het model toont belangrijke interacties tussen de hoofdprocessen onderling én de interacties tussen de mens-, proces- en IT-lagen. Onvoldoende begrip en afstemming van deze interacties is een bron voor inconsistenties, niet verwijderde usercodes of incorrecte rapportages.

Hoewel de gebruikte terminologie kan afwijken, hanteren leveranciers en standaards een indeling van identity management systemen die past in het geschetste model.

In een eerder artikel van Largos 'Identity Management: De CD-rom voorbij' wordt dieper ingegaan op het identity management model en de veiligheidsrisico's van een louter technische benadering van identity management.