Informatie veilig beschikbaar stellen in een BI-project

Data-driven autorisatie

Jiri Pleiter

BI-projecten hebben onder meer het doel om informatie voor zoveel mogelijk gebruikers toegankelijk te maken binnen een organisatie. Zo ontstaat tevens de behoefte om bepaalde informatie te kunnen afschermen. Er is een mogelijkheid een autorisatiestructuur te implementeren, waarin verband wordt gelegd tussen de metadata en de rapportagedata. Daarmee wordt data-driven autorisatie gerealiseerd.

Of autorisatie in een BI-project gewenst of zelfs vereist is, kan afhangen van verschillende met elkaar samenhangende factoren. Daar is de schaalgrootte van het project er één van: hoe groter de gebruikersgroep, hoe groter de roep om goede beveiliging.
Het type gebruiker dat wordt bediend speelt een rol; gaat het bijvoorbeeld om financiële controllers binnen dezelfde afdeling of divisie, of betreft het accountbeheerders van concurrerende bedrijfsonderdelen.

> De basis voor autorisatie wordt gevormd door de kostenplaatsen

Een andere belangrijke factor is de ambities die organisatie en opdrachtgever met het project beogen, en dan vooral de mate van uitrol en beschikbaarheidstelling binnen de organisatie. Hoe hoger de ambitie, hoe sterker de behoefte om alles zo goed mogelijk te regelen. Ook wegen de mate van vertrouwelijkheid van gegevens en informatie, en externe voorschriften en wetgeving mee. Tot slot is een rol weggelegd voor het soort tool; het gebruik van web-based tools veronderstelt immers al een grootschalige architectuur, waarbij het onderwerp beveiliging al snel de kop opsteekt.

Eenvoudige autorisatie

Bij het aanbrengen van autorisatie kan men denken aan een eenvoudige afgrendeling van een rapportageomgeving door middel van een login account en een wachtwoord. Maar in de praktijk leeft het verlangen in de organisatie, en zeker bij de personen die er achter de schermen mee moeten werken, om de toegang tot de informatie op een meer geavanceerde manier te verzorgen. Soms wordt op een andere plek in de organisatie al geautoriseerd. Een BI-omgeving hierop laten aansluiten lijkt dan een efficiënte manier om te koppelen met bestaande bedrijfsprocessen.
Een makkelijke vorm van autoriseren is om de applicaties, benodigd voor rapporteren, heel gericht beschikbaar te stellen. Medewerkers zonder geïnstalleerde programmatuur hebben op deze manier geen mogelijkheid om bedrijfsgegevens te benaderen.
Een andere vorm van autoriseren is het invoeren van beveiligde login accounts voor de afnemers van informatie. De nieuwe generatie tools die voor ontsluiting van bedrijfsgegevens en rapportages wordt gebruikt, is veelal gebaseerd op internettechnologie. Alle medewerkers kunnen dan de tool benaderen, maar alleen degenen met autorisatie kunnen aan de slag. In deze gevallen wordt geautoriseerd op toolniveau.

Opzetten van een autorisatiemodel

Als de vraag of autorisatie gewenst is positief is beantwoord, kan worden begonnen met het opzetten van een autorisatiemodel. Autorisatie begint altijd met identificatie. De identificatie wordt uitgevoerd door de tool c.q. de programmatuurschil waarbinnen het BI-systeem is ontwikkeld. Na identificatie moet de login account beschikbaar komen als parameter voor een autorisatieproces.
Er zijn verschillende vormen van autorisatie. Er is de directe vastlegging, waarbij de gebruiker simpelweg wel of niet toegang krijgt tot een rapport of informatie. Dynamisch toegangsbeheer, waarbij de toegang tot de informatie door data wordt gestuurd, heeft als voordeel dat het eenvoudig te beheren is; wordt de getoonde informatie bepaald door de identiteit van de gebruiker, dan is er sprake van inhoudelijk flexibel sturende autorisatie.
Een organisatie, zoals het Albert Schweitzer Ziekenhuis in het verderop te bespreken voorbeeld, kiest voor een combinatie van

deze autorisatievormen. Men wil kunnen sturen vanuit de bronsystemen en de beheerinspanning voor de datawarehouse-beheerder op het vlak van autorisatie minimaal houden. Dat impliceert dat de data voor autorisatie vanuit de bronsystemen moeten worden aangeboden. Deze data moeten worden geleverd, verwerkt en onderhouden, en geven antwoord op de vraag "wie mag wat". In de programmatuur van het BI-systeem moet logica worden ingebouwd waarmee de autorisatiedata worden gekoppeld aan de gestelde gebruikersvraag. De autorisatiegegevens moeten compleet zijn, vastgelegd in een logische structuur en te relateren zijn aan gebruikers.

De autorisatiestructuur

De structuur waarvan gebruik wordt gemaakt voor het vastleggen van autorisatie is een centrale keuze: deze structuur bepaalt hoe universeel autorisatie te sturen is door de data. Meestal wordt gebruik gemaakt van een organisatorische structuur die beschikbaar is in de bronsystemen van de organisatie. Bij het opzetten van het autorisatiemodel moet goed beoordeeld worden op welke wijze deze structuur in de bronsystemen wordt beheerd en of deze vaak aan veranderingen onderhevig is. Het gebruik van structuren uit de bronsystemen introduceert immers afhankelijkheden, die bewaakt en gemanaged moeten worden. Tevens moet rekening worden gehouden met veranderingen over de tijd heen. Een organisatie leeft, en dit zal zijn uitwerking hebben op de opbouw van een organisatorische structuur in het bronsysteem. Aanpassingen kunnen dan een rechtstreeks gevolg hebben voor de autorisatie.

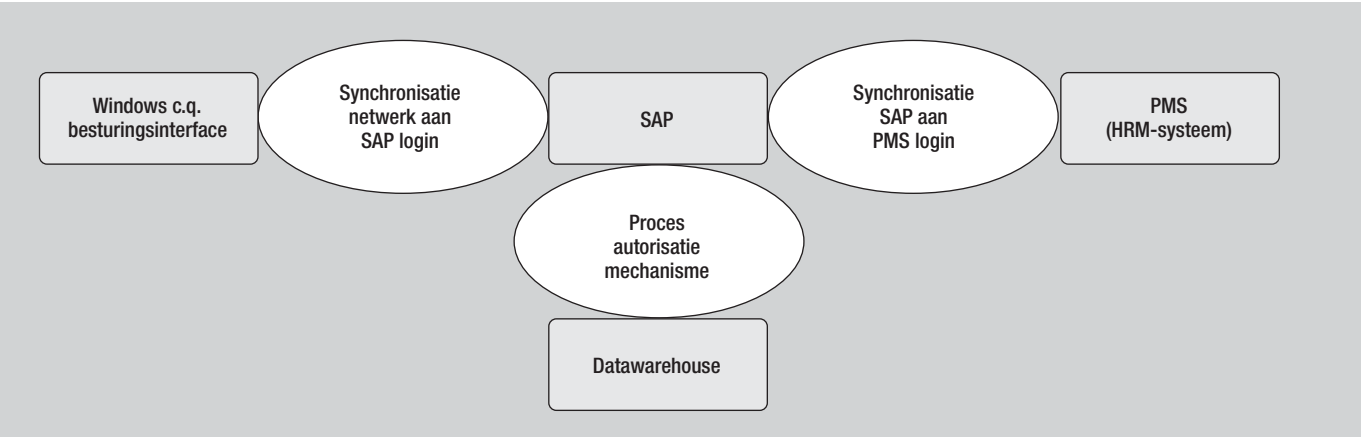
De data en structuur bevatten de factoren op basis waarvan de inhoud van opgevraagde rapportages wordt afgebakend. In de programmatuur van het BI-systeem moet dit worden ingepast. Het gaat er hierbij om dat een mechanisme wordt aangebracht, waarbij een noodzakelijk verband wordt gelegd tussen de metadata en de rapportagedata. Voor iedere vraag naar informatie die door de gebruiker wordt gesteld, moet het bereik van de geraadpleegde gegevens worden afgebakend. De zoekopdracht welke vanuit de gebruikersomgeving aan de database wordt gesteld, moet daartoe worden aangevuld met beperkende voorwaarden. Aan deze eis kan op verschillende niveaus in het systeem invulling worden gegeven, zoals op database-, repository- of rapportageniveau. De repository zal het eerst in aanmerking komen, omdat deze het knooppunt vormt tussen de database-omgeving en rapportage-omgeving.

> Autorisatiegegevens moeten compleet zijn en vastgelegd in een logische structuur

Bij het verankeren van de autorisatielogica in het systeem, rijst de vraag of autorisatie op alle rapportages van toepassing moet zijn. Er kunnen bijvoorbeeld rapportages zijn met zo'n algemeen karakter, of op zo'n hoog geaggregeerd niveau, dat autorisatie niet nodig is. Het autorisatiemodel moet daartoe de mogelijkheid bieden. Een voorbeeld hiervan is het aanbieden van geaggregeerde gegevens in een apart deel van de repository. Deze data kunnen in de rapportageomgeving dan vrij beschikbaar komen. Een ander voorbeeld is het anonimiseren van data in het laadproces, waardoor het vertrouwelijk karakter van de data afneemt.

De praktijk

Het Albert Schweitzer Ziekenhuis (ASZ) beschikt sinds een aantal jaren over een datawarehouse-omgeving. Hiermee wordt voorzien in de interne informatiebehoefte via een rapportage- en een analyse-omgeving. Bij de eerste implementatie is gekozen om de scope van de informatie af te bakenen tot één deel van het bedrijfsproces. De focus lag hierbij op productie. De organisatie heeft de wens uitgesproken om het bereik van aangeboden informatie te verbreden met financiële en personele informatie. Het karakter van de nieuw toe te voegen informatiedomeinen brengt met zich mee dat bij deze uitbreiding een autorisatielaag moet worden aangebracht, om te voorkomen dat vertrouwelijke data bij verkeerde personen terecht komen. Deze autorisatielaag zal later ook op de oorspronkelijke implementatie van het datawarehouse moeten kunnen worden uitgebreid.



Afbeelding 1: Kostenplaatsbeheer in SAP- en HR-systeem.

Het ASZ maakt gebruik van verschillende basissystemen voor het vastleggen van bedrijfsgegevens. Het dominerende systeem hierbij is SAP, waarin gegevens over de productie en financiële cijfers worden opgeslagen; daarnaast is er een apart HR-systeem. In beide systemen wordt autorisatie toegepast, zie afbeelding 1. De basis voor autorisatie in deze systemen wordt gevormd door de kostenplaatsen. Als bedrijfsregel geldt, dat het beheer van de kostenplaatsen wordt gestuurd en ingevuld vanuit SAP. De kostenplaatsstructuur vanuit het personele proces is hierop aanvullend. Binnen het datawarehouse dienen deze autorisatiestromen te worden geïntegreerd tot één uniforme autorisatie. Hier ligt het potentieel gevaar dat het beheer van de kostenplaatsen in beide systemen niet synchroon verloopt, waardoor de laadprocessen van het datawarehouse worden geconfronteerd met foutieve data. Door de autorisatie ook per informatiedomein te registreren zal kostenplaatsbeheer in het SAP- en HR-systeem elkaar uit zicht van het datawarehouse niet tegenspreken.

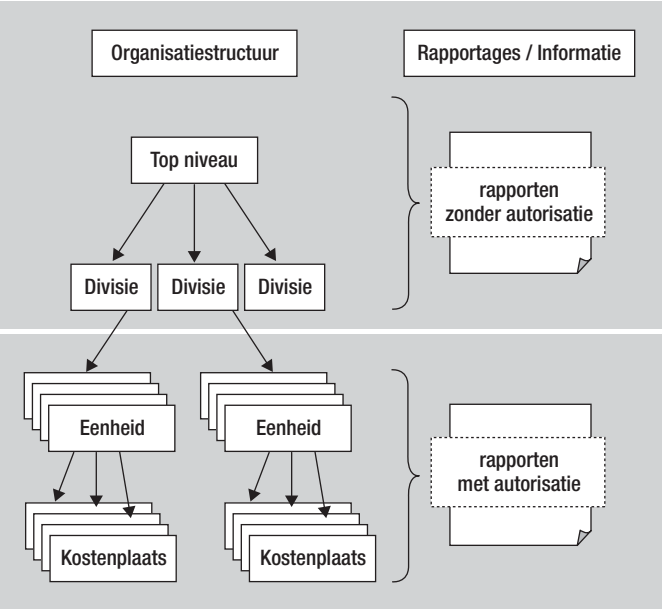
Het ASZ heeft de ambitie om de informatieomgeving te laten uitgroeien tot het middelpunt van informatievoorziening, waarop gebruikers zelf rapportages moeten kunnen afroepen. Dit streven impliceert uitbreiding van de informatiegebieden en dus een grotere gebruikersgroep, hetgeen nieuwe eisen stelt aan een doordachte autorisatielaag.
Om het autorisatievraagstuk gekoppeld aan deze groei te kunnen managen, heeft de organisatie een drietal wensen geformuleerd:
- autorisatie voor toegang tot informatie moet gestuurd kunnen worden vanuit het bronsysteem dat de brondata aanlevert;
- autorisatie moet kunnen worden ingesteld per informatiedomein;
- autorisatie moet flexibel toegepast kunnen worden, zodat het systeem bepaalde informatie vrij beschikbaar kan stellen welke niet is gekoppeld aan een autorisatielaag.

Het informatiesysteem van de organisatie bestaat uit een professionele architectuur met verschillende componenten. Voor de opslag van alle (meta)gegevens van de informatieomgeving maakt het datawarehouse gebruik van een Microsoft SQL 2000 database. De laadprocessen zijn gemodelleerd in het ETL-tool Cognos DecisionStream. De distributie van informatie naar de afnemers vindt plaats via het intranet van de organisatie, waar de gebruikers via een portal kunnen inloggen om zo in een omgeving te komen waarin de rapportages beschikbaar zijn. Met Cognos ReportNET wordt de informatie gedistribueerd en ook de rapporten gebouwd en beheerd.

Geavanceerde autorisatie op verschillende niveaus

Het ASZ wil informatie over twee lagen kunnen publiceren, zie afbeelding 2. Specifieke, gevoelige informatie dient afgeschermd te worden door een autorisatielaag. Informatie met een algemeen karakter dient wel vrij beschikbaar te zijn. Voor het ontsluiten van de nieuwe brondata zijn nieuwe ETL-stromen ontworpen en gebouwd. Voor het daadwerkelijk beschikbaar stellen van de nieuwe informatie zijn rapporten gedefinieerd en gebouwd, die als standaardrapportages in de portal worden gepubliceerd. Zoekopdrachten naar ad hoc- en standaard-rapportages bevragen gegevens in het datawarehouse. Daarbij wordt iedere zoekopdracht in de repository via een meerlaagse metadata-laag vertaald naar de tabellen en kolommen in de database.

De autorisatiedata worden vastgelegd als metadata in tabellen van het datawarehouse. In de wensen is geformuleerd dat het mogelijk moet zijn om autorisatie te sturen vanuit de invalshoeken ‘informatiedomein’ en ‘organisatiestructuur’. In het technische model is deze wens vertaald naar een structuur van tabellen. Daarin wordt voor iedere gebruiker een kostenplaats geregistreerd waarvoor de gebruiker informatie mag benaderen. Per vastgelegde kostenplaats wordt een koppeling gelegd naar elk informatiedomein waarvoor de gebruiker gegevens mag opvragen. In de metadata-lagen van de repository zijn de autorisatietabellen gekoppeld aan de rapportagetabellen via kostenplaatsen en organisatiestructuur. In de koppelingdefinitie is de gebruiker als parameter opgenomen. Door het invullen van de parameter met de geldende login account wordt de autorisatie verwezenlijkt. Zodoende wordt het mogelijk om autorisatie toe te passen in het



Afbeelding 2: Specifieke, gevoelige informatie wordt afgeschermd door een autorisatielaag.

informatiesysteem, waarbij deze wordt gestuurd door het gebruik van metadata. Er kan per kostenplaats toegang worden vastgelegd, en er kan per informatiedomein toegang worden vastgelegd. Het is mogelijk om informatie buiten de inhoudelijke autorisatie te houden door deze niet te koppelen aan de autorisatiestructuur in het datawarehouse.

Naast de inhoudelijke autorisatie op dataniveau, is parallel een autorisatielaag ingericht op toegangsniveau. In de portal is hiertoe een structuur van gebruikersgroepen ingericht. Op deze laag kunnen de aangeboden informatieobjecten in de portal per gebruiker en groep worden aangeboden of verborgen.

Complicaties

Het autorisatiemodel brengt naast zijn voordelen een aantal knelpunten met zich mee, waarmee moet worden omgegaan. Het ASZ wil rapportages die betrekking hebben op een hoog niveau binnen de organiatie buiten het mechanisme van kostenplaats-autorisatie houden. Om dit te kunnen faciliteren zijn aggregatietabellen aangebracht op de basis-feittabellen. Hierin zijn de data geaggregeerd naar een hoog niveau in de hiërarchie van de organisatiestructuur. Het inbrengen van deze extra (aggregatie)-tabellen brengt een aanvullende belasting van het laadproces met zich mee. Daarbij is er de verplichting om de aggregaties bij ieder laadproces nieuw (initiëel) te berekenen, zodoende aanpassingen in de organisatie structuur te kunnen opvangen.
De aggregatietabellen zijn in de rapportage-metalaag opgenomen, zodat door gebruikers gerapporteerd kan worden. Het inbrengen van de aggregatietabellen in deze laag veroorzaakt een toename van de omvang en de complexiteit ervan. Dit heeft effect op de flexibiliteit. Aanpassingen en uitbreidingen zijn mogelijk, maar vereisen een goede bekendheid met het systeem.
Een ander knelpunt is dat standaardrapporten die beschikbaar komen voor de gebruikers zeer complex van aard kunnen zijn. Dit verschilt per soort rapport. Een voorbeeld hiervan is een verzuimrapportage waarbij gevraagd wordt om verzuiminformatie op het niveau van de afdeling (geautoriseerd) af te zetten tegen gemiddelde verzuiminformatie op het niveau van de divisie. Gegevens van verschillende autorisatieniveaus worden met elkaar in verband gebracht, wat zal leiden tot een complex rapport.
Een doordacht beheerbeleid is belangrijk om te voorkomen dat de datawarehouse-beheerder in de problemen komt.
Bij het ontwikkelen van de rapporten ten slotte, is het zaak om de performance in de gaten te houden. De complexheid van de metadatalaag tussen database en rapportageomgeving kan de vertaling van rapportage-zoekopdracht naar SQL nadelig beïnvloeden.

Conclusies

Het afschermen van informatie kan op een dynamische wijze worden opgezet met gebruik van metadata waarbij autorisatie wordt gestuurd vanuit de bronsystemen. Dit vereenvoudigt het proces van autoriseren van gebruikers binnen de organisatie, omdat het beheer slechts op één plek hoeft te worden ingevuld. Een eenvoudiger autorisatieproces komt distributie van informatie binnen een organisatie ten goede. Het implementeren van deze autorisatievorm brengt een groei in omvang en complexiteit van het gehele BI-systeem met zich mee, waarmee op een doordachte manier kan worden omgegaan. Dit kan bijvoorbeeld door het voeren van een stabiel beheerbeleid. Een organisatie met een gezonde ambitie voor het uitbouwen van interne informatievoorziening zal zich hier niet door laten tegen houden.

Jiri Pleiter (j.pleiter@i3.nl) is Datawarehouse Consultant bij i3.

Albert Schweitzer Ziekenhuis

Het Albert Schweitzer Ziekenhuis (ASZ) behoort voor wat betreft omvang tot de top van algemene ziekenhuizen in Nederland. De meer dan 3300 medewerkers en 180 specialisten leveren zorg vanuit vier vestigingen in de regio Dordrecht. Het ASZ behoort tot een groep van ongeveer tien ziekenhuizen die SAP gebruiken als bedrijfssoftware. De turbulente ontwikkelingen in de gezondheidszorg verplichten een organisatie als het ASZ tot een betrouwbare en brede ontsluiting van bedrijfsgegevens. Het ASZ heeft de aanlevering van interne informatievoorziening in het verleden al vorm gegeven door het inrichten van een datawarehouse-omgeving. In de organisatie leeft de ambitie om deze omgeving verder te laten groeien in omvang en kwaliteit. Voor het ASZ vormt een goed autorisatieplan een vanzelfsprekend onderdeel in de groei naar een professionele omgeving.