Richt jij de autorisaties even in?

De complexiteit van het SAP R/3-autorisatieconcept

A. Vreeke en D.M. Hallemeesch

In de praktijk blijkt dat veel organisaties moeite hebben met het inrichten van de logische toegangsbeveiliging (autorisaties) in de SAP R/3-omgeving. Na het in productie nemen van het systeem regent het dan ook klachten ten aanzien van de autorisaties. Gebruikers kunnen niet inloggen, kunnen hun werk niet uitvoeren of kunnen juist te veel, en rapportages blijken onvolledig. Voor de acceptatie van het nieuwe systeem door de eindgebruikers kan dit zeer negatieve gevolgen hebben; daarnaast loopt de organisatie direct risico's voor de betrouwbaarheid van de gegevensverwerking.
De valkuilen waarin organisaties lopen bij het opzetten, inrichten en beheren, zijn echter te voorkomen. Dit artikel gaat in op de door KPMG IRM gesignaleerde knelpunten uit de praktijk en komt met tips voor de praktijk.

Inleiding

Veel van de oorzaken van de knelpunten ten aanzien van de inrichting van de beveiliging zijn te verklaren uit de volgende uitroep die in de praktijk tijdens een projectoverleg nogal eens te beluisteren valt:

> *O ja, richt jij ook nog even de autorisatieprofielen in, dan kunnen de gebruikers inloggen.*

Als deze uitroep van de projectmanager onder de loep wordt genomen, vallen de volgende woorden op:

* *O ja:* Dit verwijst naar het moment van de vraag. Nog net op tijd vlak voor het einde van het project. Op de valreep dus.

* *Richt*: De nadruk op de inrichting. Over het beheren van de gebruikersgegevens en toegangsrechten is dan nog niet nagedacht.

* *Jij:* De technisch beheerder wordt gevraagd de autorisaties in te richten. Vaak wordt hem als advies meegegeven dat hij/zij het één op één moet overnemen van het oude systeem. Dit terwijl het ERP-systeem misschien wel ter vervanging komt van vier op zichzelf opererende systemen. Daarnaast is de technisch beheerder niet altijd actief aangesloten met de project- en gebruikersorganisatie. Het inrichten van de beveiliging wordt als een vanuit de techniek gedreven activiteit gezien.

* *Ook:* De technisch beheerder heeft het aan het eind van het project normaal gesproken erg druk. Er zijn meerdere omgevingen actief (bouw, test, opleiding, acceptatie), er dienen veel transporten te worden uitgevoerd en ook de conversie dient te worden opgestart. Het inrichten van de beveiliging moet ook nog gebeuren!

* *Nog even:* Dat is toch niet zoveel werk? Dat is zo gebeurd. De omvang en complexiteit wordt door de projectmanager onderschat. Hierdoor ontbreekt het naast de benodigde betrokkenheid van het projectmanagement ook aan de benodigde resources vanuit de werkgroepen en aan budget.

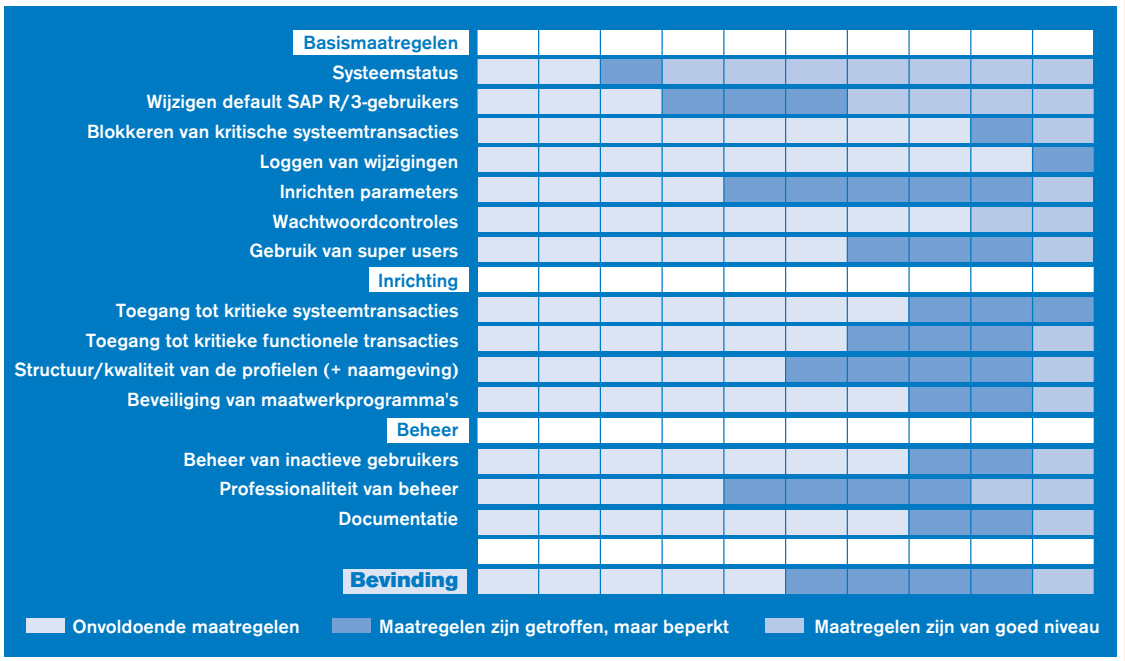
* *Dan kunnen de gebruikers inloggen:* Het inrichten van autorisaties wordt hier niet gezien als een maatregel van interne controle. Het waarom van de wijze waarop de autorisaties dienen te worden ingericht is dan geen afweging op basis van (proces)risico's, maar wordt meer gevoed vanuit de tijd en kunde van de technisch beheerder en de daarmee samenhangende mogelijkheden uit de techniek.

Veel van de knelpunten in de praktijk op het gebied van beveiliging van ERP-omgevingen zijn te herleiden tot (1) de wijze waarop SAP R/3-beveiliging binnen de projectorganisatie is geïntegreerd, (2) de kennis en ervaring van de beheerders, maar met name ook (3) doordat organisaties vanuit een verkeerde invalshoek de structuur van de autorisatieprofielen[1] bepalen. Veel organisaties kiezen voor een honderd procent top-down benadering, terwijl het beter is een top-down met een bottom-up benadering te combineren.

Onderzoeksresultaten SAP R/3-beveiliging

KPMG IRM voert jaarlijks een groot aantal SAP R/3-beveiligingsonderzoeken uit, in de vorm van audits en quick scans op het gebied van de logische toegangsbeveiliging. Onlangs heeft het Competence Center SAP R/3 Security (CC) op hoofdlijnen de resultaten van vijfendertig beveiligingsonderzoeken geanalyseerd. Uit deze analyse blijkt dat op alle gebieden, van de basismaatregelen tot de inrichting en het beheer, bij een groot percentage van de organisaties tekortkomingen zijn geconstateerd. In figuur 1 ziet u de resultaten per deelgebied van het onderzoek. In deze figuur kunt u bijvoorbeeld zien dat bij zeventig procent het beheer van inactieve gebruikers onvoldoende plaatsvindt, bij twintig procent wordt dit redelijk uitgevoerd en slechts tien procent heeft het beheer van inactieve gebruikers onder controle.

1) In dit artikel wordt gesproken over 'autorisatieprofielen'. Ook al is deze term in SAP R/3 sterk verouderd, zij wordt in dit artikel met name als verzamelterm voor profielen, rollen en activiteitgroepen gebruikt om de gangbaarheid van het artikel te verhogen. Waar nodig zullen de termen rollen en activiteitgroepen extra gebruikt worden om voor kenners meer informatie te verschaffen.



Figuur 1. Onderzoeksresultaten op basis van een intern onderzoek naar de resultaten van vijfendertig SAP-beveiligingsreviews.

Per deelgebied worden oorzaken beschreven die debet kunnen zijn aan de slechte scores op de deelgebieden. Daarna zullen aanbevelingen en/of tips als oplossing of ter verbetering worden gegeven per deelgebied.

Basismaatregelen SAP R/3-beveiliging

Oorzaken van het niet goed inrichten van de onderstaande basismaatregelen van informatiebeveiliging van een SAP R/3-omgeving zijn kennistekort of gewoonweg gebrek aan aandacht. Het implementeren van deze basismaatregelen is namelijk een geringe inspanning. Bedoelde basismaatregelen zijn:

* het dichtzetten van de productieomgeving voor wijzigingen (systeemstatus);
* het wijzigen van de default SAP R/3-gebruikers[2];
* het blokkeren van kritische (systeem)transacties;
* het inrichten van de relevante beveiligingsparameters (denk aan wachtwoordlengte, afbreken inactieve sessies, etc.);
* het inrichten van wachtwoordrestricties.

> Het niet beperken van het aantal 'Super'-gebruikers ondermijnt het beveiligingsniveau van de gehele SAP R/3-omgeving.

Het inrichten van bovenstaande basismaatregelen is voor iemand met de benodigde kennis niet meer dan een dag werk (ruim geschat). Het opdoen van de benodigde kennis zal de gemiddelde beheerder een halve dag kosten. Het implementeren van bovenstaande basismaatregelen omvat technisch namelijk niets meer dan het vullen van de juiste tabellen en/of het wijzigen van enkele parameters. Het kan binnen het project echter gebeuren dat de uitvoering van deze activiteiten tussen wal en schip valt. Deze activiteiten liggen op het grensgebied tussen infrastructuurbeveiliging en applicatiebeveiliging. Het is dan aan de technisch beheerder of de autorisatiebeheerder om deze maatregelen te implementeren.

Na live-datum zijn in de productieomgeving vaak relatief grote aantallen gebruikers met 'Super'-rechten actief in het SAP R/3-systeem (voor kenners gebruikers met het autorisatieprofiel 'SAP_ALL'). Dit zijn gebruikers die in het productiesysteem alle transacties kunnen uitvoeren. Dit resulteert direct in zeer grote risico's voor de vertrouwelijkheid en integriteit van de gegevens en de gegevensverwerking. Vanwege de omvangrijke bevoegdheden zijn er ook direct risico's voor de beschikbaarheid van het systeem. Kritische parameters kunnen worden gewijzigd en omvangrijke batchverwerking kan midden op de dag worden opgestart. Het niet beperken van het aantal 'Super'-gebruikers ondermijnt het beveiligingsniveau van de gehele SAP R/3-omgeving.

De 'Super'-gebruikers zijn vaak beheerders, ontwikkelaars of externe consultants. Het is complex om vast te stellen wat de beheerders na het in productie nemen van het systeem precies staat te wachten, om enerzijds problemen op te lossen en/of anderzijds het systeem operationeel te houden. Het creëren van toegesneden (passend bij het takenpakket) autorisatieprofielen voor de productiedatum voor technisch en functioneel beheerders is dan ook een lastige zaak. Ontwikkelaars en/of externe consultants daarentegen hebben in de productieomgeving heel weinig te zoeken. Afgezien van weergavebevoegdheden respectievelijk om te beoordelen of configuraties goed zijn getransporteerd dan wel om gebruikers te ondersteunen hebben deze rollen eigenlijk geen toegangsrechten nodig.

2) Bij de levering van SAP R/3 wordt een aantal 'default' gebruikers meegeleverd. Deze zijn gecodeerd in het systeem. Deze default gebruikers zijn bijvoorbeeld nodig bij de initiële installatie van het SAP R/3-systeem. De default gebruikers hebben zeer ruime bevoegdheden. De username en wachtwoorden van deze gebruikers zijn algemeen bekend. Ze zijn terug te vinden in de SAP R/3-handboeken en op het internet. Het niet wijzigen van de default wachtwoorden en/of het niet blokkeren van het inloggen van deze gebruikers resulteert in een beveiligingslek.

Tip 1: Creëer autorisatieprofielen voor beheerders als quick win volgens het principe 'alle activiteiten, behalve ...'. Indien het toesnijden van autorisatieprofielen voor beheerders niet lukt voor de productiedatum, creëer dan een zeer ruim autorisatieprofiel, geschoond voor kritische activiteiten. Zo kunt u zeker ten aanzien van de beschikbaarheid en bijvoorbeeld het weergeven van personeelsgegevens zeer eenvoudig de risico's beperken. Kies hier dus voor de *'Alle activiteiten, behalve ....'*-insteek. Maak voor de zeer kritische transacties aparte autorisatieprofielen aan (en isoleer deze), zodat zij heel expliciet kunnen worden toegewezen.

Tip 2: Vervang de ruime bevoegdheden van ontwikkelaars en consultants door weergavebevoegdheden. Vervang de 'Super'-rechten van de ontwikkelaars en externe consultants door autorisatieprofielen toe te kennen die alleen weergavebevoegdheden bevatten.

Tip 3: Gebruik de kennis van uw externe adviseur voor de inrichting van de relevante beveiligingsparameters en voor de in te vullen tabelwaarden. Benut zijn kennis voor het implementeren van de eerdergenoemde basismaatregelen. Vraag uw externe adviseur welke parameters dienen te worden aangepast en welke tabellen dienen te worden gevuld. Deze parameters en het vullen van enkele tabellen zijn namelijk grotendeels organisatieonafhankelijk, uw externe adviseur beschikt vast over instructies en voorstelwaarden. Bewaak wel de aansluiting met uw eigen informatiebeveiligingsbeleid.

De implementatie van de basismaatregel 'logging' is van een andere orde. Zij is namelijk niet direct een beveiligingsmaatregel op het gebied van de logische toegangsbeveiliging en vraagt naast technische ook om organisatorische maatregelen. Uit het onderzoek blijkt dat slechts een zeer beperkt aantal organisaties gebruikmaakt van de loggingfunctionaliteit. Dit terwijl SAP R/3 in staat is voor een aantal zeer kritische tabellen te loggen welke wijzigingen worden aangebracht. De maatregel 'logging' wordt hier behalve in de volgende tip niet verder toegelicht.

Tip 4: Analyseer het optimale gebruik van de loggingmogelijkheden binnen SAP. Denk eerst goed na welke gegevens gelogd dienen te worden, waar deze worden opgeslagen en beheerd en door wie de gelogde data dient te worden geanalyseerd. Activeer de 'logging parameter' (rec/client) niet zomaar, uw tabellen zullen snel vollopen.

Inrichting

Toegang tot kritieke transacties of tot ongewenste combinaties van transacties

Het aantal gebruikers dat toegang heeft tot kritische systeem- en/of functionele transacties of de toegang tot combinaties van functionele transacties is vaak groter dan gedacht. Oorzaken hiervan zijn bijvoorbeeld:

* Fouten in de inrichting van de autorisatieprofielen. Onbedoeld zijn de transacties opengesteld voor een groot aantal eindgebruikers. Specialistische kennis in het project ontbrak waardoor inrichtingsfouten zijn gemaakt.

Het inrichten van het SAP R/3-beveiligingsconcept is namelijk complex. Men kan binnen SAP R/3 als eerste autoriseren op de transacties die een functie[3] (of gebruiker) kan opstarten, en daarna op welke activiteiten en veldwaarden hij/zij binnen die transactie kan en mag invoeren[4]. Bijvoorbeeld: het wel of niet kunnen invoeren van inkooporder is autorisatie op transactieniveau. Indien de gebruiker deze transactie alleen voor de Nederlandse inkooporganisatie mag invoeren, gebruikt men een veldautorisatie. Elke transactie kent een aantal velden waarop men kan autoriseren. In totaal zijn er ongeveer achthonderd veldautorisaties mogelijk voor duizenden transacties en rapportages. De transacties die een functie in de organisatie (of gebruiker) mag opstarten, plus de daartoe behorende veldautorisaties, legt men vast in een autorisatieprofiel. De hoeveelheid veldkeuzen en transacties maakt het direct complex. Hoe meer men van de veldwaarden en autorisatiemogelijkheden afweet hoe beter men gebruik kan maken van de mogelijkheden, of juist ervoor kan kiezen niet gebruik te maken van de technische mogelijkheden. Het foutief of niet invullen van veldwaarden kan resulteren in ongewenste bevoegdheden, vooral als de beheerder met ranges van waarden heeft gewerkt om snel de profielen in te richten.

* De autorisatiestructuur is niet flexibel genoeg, waardoor de toegang tot kritische transacties en/of de toegang tot kritische combinaties niet voldoende kan worden beperkt. Met andere woorden, de autorisatieprofielen zijn te groot waardoor niet voldoende onderscheid per functie kan worden gemaakt. Indien de gebruiker toegang moet hebben tot de ene transactie dan verkrijgt de gebruiker vanwege het grote profiel ook direct toegang tot de andere transacties omdat die in hetzelfde profiel voorkomen. Grote profielen zijn vaak een gevolg van een honderd procent top-down benadering.

* SAP kan de autorisaties in de toegewezen autorisatieprofielen voor de gebruiker bij elkaar optellen. Zodra een gebruiker meerdere profielen aan zich gekoppeld heeft, zal het SAP R/3-autorisatieconcept in sommige situaties namelijk de autorisaties bij elkaar optellen. Zo kan SAP R/3 de transactiebevoegdheid ontlenen aan profiel A en de veldbevoegdheid aan profiel B. Onder kenners wordt dit het '1 op 1 = 3'-verschijnsel genoemd. Een adequate opbouw van de autorisatiestructuur voorkomt dit. Ondanks het feit dat dit verschijnsel zich in de oude SAP R/3-versies meer manifesteerde, kan het in de huidige versies nog steeds voorkomen.

* Het is niet bekend wat de kritische transacties zijn, het autorisatieconcept is niet vanuit de optiek van de interne controle opgezet, maar met name vanuit het 'kunnen werken'. Hierdoor zijn de bevoegdheden ruim gedefinieerd om vastlopers te voorkomen. Er is nooit expliciet gedefinieerd vanuit het project wat de beveiligingsregels zijn. Beveiligingsregels bestaan onder andere uit een lijst met kritieke transacties en een lijst met kritische combinaties.

* De autorisatieprofielen zijn in het project alleen positief getest. Er is niet expliciet getest of gebruikers te veel bevoegdheden hebben.

3) Bewust is hier gekozen voor het woord functie, om verwarring met het SAP-begrip rol te voorkomen.
4) Bij de inrichting van de autorisaties voor de personeelsadministratie is de transactie minder leidend. Hierbij zijn de activiteiten die men op een verzameling gegevens (infotype) mag uitvoeren het uitgangspunt.

* Een inadequaat beheer heeft ertoe geleid dat vlak na live-datum vastlopers zijn opgelost door het toekennen van 'tijdelijke' profielen of het toekennen van 'extra' profielen. Deze tijdelijke oplossingen zijn echter nooit hersteld of de extra toegekende autorisatieprofielen zijn nooit meer verwijderd.

Tip 5: Test de profielen naast positief ook negatief. Test de autorisatieprofielen ook negatief en test ook de kritische rapportages op volledigheid. Gebruik de negatieve testcases direct als de beveiligingsregels na live-datum. Negatieve testcases worden opgesteld op basis van de eisen vanuit de interne controle. Indien tijdens het beheer na een wijzigingsverzoek een conflict ontstaat met één van de beveiligingsregels, dient namelijk een andere procedure te worden gevolgd. Test kritische rapportages op volledigheid omdat SAP R/3 waarden niet kan afdrukken omdat de gebruiker niet bevoegd is tot het weergeven van de data. Bijvoorbeeld de lijst met boekingen is dan onvolledig, omdat bijvoorbeeld een aantal documentsoorten ontbreekt. Normaliter waarschuwt SAP R/3 hiervoor op het scherm, maar gebruikers klikken hier eenvoudig doorheen.

Bij onvoldoende beheersbaarheid leveren ook flexibiliteit, veiligheid en controleerbaarheid aan kwaliteit in.

Tip 6: Kies een structuur van autorisatieprofielen die voldoende flexibel, beheersbaar, controleerbaar en veilig is. Uit bovenstaande oorzaken blijkt al het belang van een goede structuur van de autorisatieprofielen. Een goede structuur van autorisatieprofielen voldoet aan de volgende vier kwaliteitscriteria:

* **Flexibel**. Wijzigingen in de organisatie, het systeem of de procesgang dienen niet te leiden tot complexe beheeractiviteiten voor het aanpassen van de autorisatieprofielen.
* **Veilig**. Op basis van de set van autorisatieprofielen dienen alle gewenste controletechnische functiescheidingen gerealiseerd te kunnen worden. Ongewenste combinaties van transacties mogen niet in één profiel voorkomen.
* **Beheersbaar**. Indien het autorisatieconcept uit veel kleine autorisatieprofielen bestaat, is deze direct meer flexibel en kunnen eenvoudig de gewenste controletechnische functiescheidingen worden afgedwongen. Een veelvoud aan profielen resulteert echter in een zware beheerlast. Het veel gebruikmaken van veldautorisaties maakt het beheer direct complexer, mede doordat hiervoor vaak ook meer profielen nodig zijn. Door de complexiteit van de werking van het SAP R/3-autorisatieconcept dient een zware beheerlast te allen tijde te worden voorkomen. Dat geldt eveneens voor het onnodig autoriseren op veldwaarden.
* **Controleerbaar**. Alle belanghebbenden zoals beheerders, controllers, lijnmanagers en auditors dienen eenvoudig en snel de informatie over gebruikers en toegangsrechten in die vorm gepresenteerd te krijgen die past bij hun rol in de organisatie. De beheerder heeft behoefte aan informatie die van technische aard is, zoals transactiecodes en veldwaarden. De controller daarentegen heeft genoeg aan informatie op het niveau van rollen en taken.

De kunst is een balans te vinden tussen deze vier criteria. Als men iedereen het 'Super'-profiel geeft, dan zijn de profielen goed te beheren en is het concept goed controleerbaar. Het criterium 'veiligheid' wordt echter volledig niet gerealiseerd. Gaat men echter voor elke transactie en veldautorisatie een autorisatieprofiel aanmaken, dan zal men zeer flexibel zijn in het kunnen toekennen van autorisaties en kan men te allen tijde technisch gezien de combinaties van toegang tot transacties voorkomen. Echter, de beheersbaarheid en controleerbaarheid van het autorisatieconcept zullen zeer sterk te wensen overlaten. Zodra de beheersbaarheid onvoldoende is zal op de korte termijn ook voor de andere criteria aan kwaliteit worden ingeleverd.

Een inadequate inrichting en/of het niet kunnen vinden van de balans tussen de vier genoemde kwaliteitscriteria wordt veroorzaakt doordat:

* de aansluiting tussen de wensen vanuit het proces (gebaseerd op een risicoanalyse) en de technische realisatie niet is geborgd;
* de inrichting flexibiliteit mist. De organisatie heeft te veel top-down gewerkt bij de analyse van de profielenstructuur.

Tip 7: Gebruik de autorisatiemogelijkheden zo beperkt mogelijk. Het vinden van een balans tussen de vier genoemde criteria zal eenvoudiger worden als men de aansluiting tussen de wensen vanuit het proces en technische inrichting waarborgt. In andere woorden: *Autoriseer alleen op die velden en breng scheiding aan tussen die transacties die vanuit het oogpunt van de 'Interne Controle' noodzakelijk worden geacht en autoriseer niet op velden en/of scheidingen van transacties die vanuit de techniek mogelijk zijn.* Hoe minder eisen er aan het SAP R/3-autorisatieconcept worden gesteld als maatregel van interne controle, hoe eenvoudiger de inrichting en het beheer zullen zijn. Minder eisen zal normaliter leiden tot minder profielen, hetgeen weer ten goede komt aan de beheersbaarheid en de controleerbaarheid. Omdat het uitgangspunt de wensen vanuit de 'Interne Controle' zijn, wordt direct aan het criterium 'veiligheid' voldaan. Het kiezen voor de preventieve systeemmaatregel 'Autorisaties' dient te worden afgewogen tegen andere systeem- en/of organisatorische maatregelen. Zodra men de autorisaties op basis van de technische mogelijkheden inricht, zonder zich af te vragen of ze nu wel daadwerkelijk nodig zijn, zal ook de impact van wijzigingen moeilijker kunnen worden geanalyseerd en de overdracht van het beheer moeilijker verlopen. De legitimatie van de gemaakte keuzen ten aanzien van de inrichting ontbreekt namelijk. Als een bepaalde wens om te autoriseren zal leiden tot een groot aantal extra profielen, onderzoek dan ook of de toegangscontrole tot bepaalde velden kan worden opgelost door middel van transactievarianten, field-exits of validaties.

Tip 8: Creëer een rolgebaseerde inrichting op basis van flexibele bouwblokken. Organisaties volgen voor de opzet van autorisaties vaak een honderd procent top-down traject. Om flexibiliteit in de inrichting te verkrijgen en daarnaast minder afhankelijk te zijn van de feed-

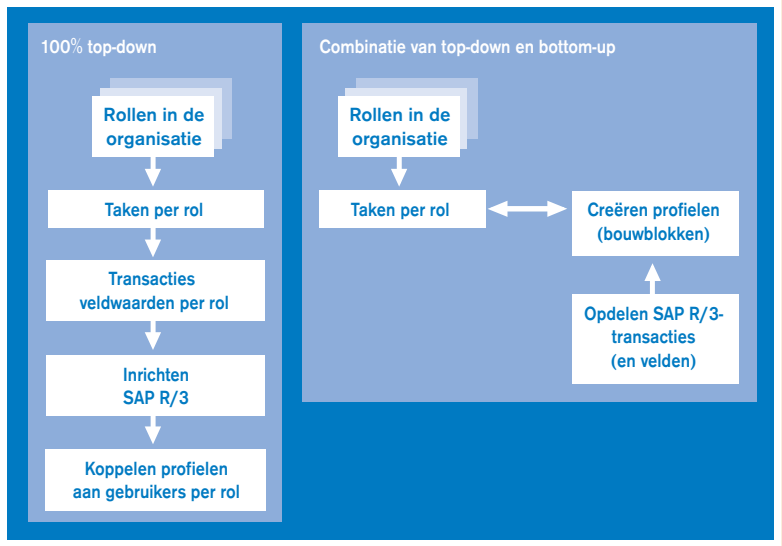
back uit de gebruikers- en/of projectorganisatie is het echter beter om een top-down traject te combineren met een bottom-up traject. Het verschil tussen de twee methodieken[5] is geïllustreerd in figuur 2.

Bij de combinatie worden enerzijds de taken vanuit de processen geanalyseerd en anderzijds worden alle 'te gebruiken' transacties in groepen (bouwblokken[6]) verdeeld. Daarbij is het zaak om transacties die vanuit het oogpunt van de interne controle niet gecombineerd mogen worden onder te verdelen in verschillende bouwblokken. Indien men dit naleeft kan men op basis van de bouwblokken alle gewenste functiescheidingen realiseren. De kunst is de bouwblokken zo groot mogelijk te maken, zonder dat aan veiligheid en flexibiliteit wordt ingeboet. Bouwblokken kunnen op verschillende niveaus worden ingericht, en wel (1) op taakniveau, (2) op taakgroepniveau, (3) op type transactie per (sub)module en (4) op activiteitsniveau per (sub)module (weergeven, muteren, etc.). Natuurlijk zijn ook combinaties mogelijk. In SAP R/3 zullen de bouwblokken verzameld moeten worden tot de rolgebaseerde samengestelde activiteitgroepen (of profielen), die dan gekoppeld zullen worden aan de eindgebruikers.

Verschillen in de praktijk tussen de twee methodieken zijn dat bij de top-down methodiek een wijziging in bevoegdheden van gebruikers gerealiseerd wordt door het wijzigen van een profiel. In de combinatiemethodiek wordt een wijziging in de bevoegdheden van een eindgebruiker gerealiseerd door het koppelen en ontkoppelen van de bouwblokken. Voor het koppelen en ontkoppelen van bouwblokken (lees profielen) is geen transport nodig. Een ander zeer belangrijk verschil dat met name de beheersbaarheid en controleerbaarheid sterk ten goede komt, is dat in de combinatiemethodiek transacties zoveel mogelijk in één bouwblok worden opgenomen.

Daarnaast kan de beheerder ook veel eenvoudiger wijzigingen tijdelijk oplossen door het alloceren van een bouwblok aan een gebruiker. En kan de beheerder bijvoorbeeld alle weergaveblokken verzamelen en zo één groot samengesteld weergaveprofiel maken. Bij de introductie van nieuwe functionaliteit (submodule) behoeft men ook veel minder aanpassingen (misschien enkele veldwaarden) in de bestaande bouwblokken door te voeren, men creëert gewoonweg nieuwe bouwblokken voor de nieuwe functionaliteit. Indien men in een project realiseert dat alle transacties in bouwblokken zijn onderverdeeld, kan men nog op het einde van het project eenvoudig inspelen op 'de laatste wijzigingen'. Let op: hoe meer bouwblokken hoe meer flexibiliteit, maar ook meer beheerlast en minder controleerbaarheid.

Het is niet zo dat het gebruik van de ene methodiek de andere uitsluit. In de praktijk worden zij gecombineerd. De keuze welke methodiek zal worden toegepast, plus de keuze over de inhoud en omvang van de bouwblokken, is de belangrijkste en meest complexe activiteit binnen het project op het gebied van de autorisaties. Andere belangrijke keuzen vloeien direct hieruit voort, zoals die inzake de technische realisatie, het opstellen van het bouwplan en het kiezen van de naamgeving.



Figuur 2. Een volledig top-down traject en een gecombineerd top-down/bottom-up traject.

Tip 9: Isoleer kritische transacties, functioneel en technisch in 'eigen' profielen. Zodra de kritische functionele transacties en kritische technische transacties in één apart bouwblok staan, denk bijvoorbeeld aan betalen, bestellen, goederenontvangst, goederenafgifte, stamgegevensbeheer, etc., dan kunt u deze altijd zeer selectief toewijzen (zie tevens Tip 1). Door voor bijvoorbeeld maatwerk aparte bouwblokken te maken kunt u ook de toegang hiertoe zeer selectief toewijzen.

Voor de controleerbaarheid is het erg belangrijk dat de naamgeving van een profiel iets zegt over de organisatie-eenheid waarvoor het profiel van toepassing is en iets zegt over de inhoud van het profiel (type transacties).

Naamgeving

Naamgeving van autorisatieprofielen (activiteitgroepen en rollen) is erg belangrijk voor de controleerbaarheid en beheersbaarheid van het autorisatieconcept. Uit de verschillende onderzoeken naar SAP R/3-beveiliging blijkt echter dat er weinig aandacht is geschonken aan de naamgeving. Een goede naamgeving is belangrijk voor de beheerder, zodat hij/zij snel de juiste profielen kan vinden inzake bijvoorbeeld het doorvoeren van wijzigingen. Daarnaast geven de rapportages over gebruikers en autorisaties direct meer informatie indien op basis van de naamgeving van de profielen conclusies kunnen worden getrokken over de inhoud van de profielen.

Tip 10: Denk goed na over een heldere naamgeving. De gebruikte naamgevingsconventie van de rollen/profielen moet:
* iets zeggen over de status van het profiel (activiteitgroep), zoals 'master', 'afgeleid', 'kopie', etc.;
* iets zeggen over de organisatorische eenheid waar de inhoud van het profiel betrekking op heeft;
* iets zeggen over de module waar de inhoud van het profiel betrekking op heeft;
* iets zeggen over het type activiteiten (creëren/wijzigen, weergeven, analyseren, kritische taken, etc.);
* toekomstvast zijn.

5) Projectmedewerkers worden vaak in het project voor de eerste keer met het opzetten en inrichten van het autorisatieproject geconfronteerd. Zij kiezen dan vaak voor een honderd procent top-down proces. Bijna alle specialisten op dit gebied combineren een top-down proces met een bottom-up proces.
6) Een bouwblok wordt gemaakt op het niveau van een enkel autorisatieprofiel en/of enkele activiteitgroep. (Technisch gezien is een bouwblok dus een autorisatieprofiel.) Maar om onderscheid te maken tussen de twee methodieken wordt in de honderd procent top-down methodiek over (enkele) autorisatieprofielen gesproken en in het combinatietraject over bouwblokken.

In de latere versies kan het zelfs al raadzaam zijn om in de naamgeving aan te geven dat het profielen zijn voor het standaard SAP R/3-systeem of voor bijvoorbeeld de additionele omgevingen, zoals de Business Information Warehouse-omgeving. Daarnaast kunt u ervoor kiezen om een specifiek karakter op te nemen in de naam van een profiel als het de toegang regelt tot zeer kritische transacties.

Naamgeving van autorisatieprofielen is belangrijk voor de controleerbaarheid en beheersbaarheid van het autorisatieconcept.

Beveiliging van maatwerk

Een ondergeschoven kindje met betrekking tot beveiliging van de SAP R/3-applicatie is het maatwerk. Zo ontstaat de situatie dat voor alle standaardtransacties wel bijvoorbeeld keurig een scheiding is aangebracht tussen de 'landenadministraties', maar dat via het maatwerk een medewerker van het ene land direct mutaties kan aanbrengen in de administratie van het andere land. De verklaring is dat het maatwerk wordt geleverd door programmeurs die in de meeste gevallen vooral gefocust zijn op de werking van het programma en de beveiligingseisen ten aanzien van maatwerk uit het oog verliezen. Vaak wordt vergeten ook binnen deze transacties beveiligingscontroles mee te ontwikkelen. Daarbij heeft de ontwikkelaar de keuze om ook de eigen veldcontroles te ontwikkelen of gebruik te maken van de standaard aanwezige veldcontroles. Hoe het maatwerk zal worden opgestart, is eveneens van groot belang. Ook op dit gebied moet men expliciet de beveiligingsrisico's in ogenschouw nemen.

Tip 11: Beveilig ook het maatwerk. Binnen het maatwerk is het mogelijk autorisatiecontroles in te bouwen (authorithy checks) en maatwerk kan aan bevoegdheidsgroepen worden gekoppeld. Met behulp van deze koppelingen kan maatwerk gegroepeerd worden in logische groepen. Men kan dan gebruikers expliciet toegang geven tot 'groepen van maatwerkprogramma's'. Toegang tot maatwerk kan verder beperkt worden door maatwerk beschikbaar te maken via transactiecodes of rapportagebomen.

Beheer

Beheer van inactieve gebruikers

Het beheer van inactieve gebruikers is vaak zeer beperkt ingericht. Het percentage slapende gebruikers of gebruikers die nooit hebben ingelogd, is in veel SAP R/3-omgevingen hoog en kan soms oplopen tot wel dertig procent. Slechts weinig organisaties monitoren deze gegevens, ondanks dat dit veel licentiekosten kan besparen. Daarnaast vormen de gebruikers die nog nooit hebben ingelogd een risico vanuit het oogpunt van beveiliging en vervuilen zij de informatie over gebruikers en toegangsrechten. Een direct risico is dat de slapende gebruikers nog vaak het 'initieel' wachtwoord hebben, dat binnen de gebruikersorganisatie bekend is. Behalve door het beperkt monitoren wordt het hoge percentage slapende gebruikers veroorzaakt doordat de integratie met de personeelsadministratie niet is gelegd of doordat de communicatie met de centrale beheerstaf niet voldoet.

Tip 12: Monitor de aanwezigheid van inactieve gebruikers en verwijder deze tijdig. De gegevens over aanlogdata zijn direct te vinden in de tabel (USR02). Print bijvoorbeeld maandelijks een lijst uit met gebruikers die sinds drie maanden niet hebben ingelogd en verwijder deze. Let op dat u deze procedures laat aansluiten bij uw informatiebeveiligingsbeleid.

Professioneel beheer

In de praktijk blijkt dat het beheer niet in voldoende mate professioneel is opgezet. Zelfs duidelijke procedures op het gebied van wijzigings- en incidentbeheer worden vaak niet aangetroffen. Veelal is de beheerorganisatie nog sterk ingericht op basis van de oude situatie voordat men met een geïntegreerd pakket werkte, en daardoor ontbreekt doorgaans de regie en een duidelijke toewijzing van eigendom. Als deze procedures wel zijn ingericht, ontbreken vaak nog de volgende meer complexe procedures:

- impactanalyse op basis van beveiligingsregels;
- impactanalyse over organisatorische eenheden heen (een wijziging in de ene organisatorische omgeving kan van invloed zijn op het gehele SAP-systeem);
- beheer van inactieve gebruikers;
- SAP*-envelopprocedure;
- gebruik van OSS en Earlywatch;
- spoedprocedures voor transport;
- releasemanagement;
- licentiebeheer.

De beperkte professionaliteit van het beheer laat zich tevens herleiden tot de inflexibiliteit van de inrichting en tot de beperkte betrokkenheid in het project van de eigen beheerders bij de inrichting. Daarnaast zien wij dat beheerders enkele additionele SAP R/3-functionaliteiten die hen veel voordelen kunnen opleveren, vaak niet beheersen. Denk hierbij aan het gebruik van CATT, upload- en download-functionaliteit en het gebruik van ondersteunende tools.

Tip 13: Neem kennis van CATT en pas dit toe tijdens het beheer en de inrichting. Train de beheerders in het kundig gebruik van de tabellen in combinatie met Access en Excel, het gebruik van CATT (Computer Aided Test Tool, standaard SAP-functionaliteit) en het 'uploaden en downloaden' van bevoegdheden. Kennis van CATT en het gebruik van de tabellen kunnen met name in grootschalige omgevingen de efficiëntie van de beheeractiviteiten sterk verbeteren. Door middel van het downloaden van de juiste tabellen en een verwerking in Access kan zeer snel de inrichting van de autorisaties worden gedocumenteerd. Het is mogelijk bevoegdheden (profielen) bijvoorbeeld naar diskette te downloaden en in een andere omgeving te uploaden. Dit betekent dat u de organisatieonafhankelijke profielen zoals bijvoorbeeld de complexe beheerdersprofielen van een ander SAP-sys-

teem binnen uw organisatie kunt overnemen. CATT wordt gebruikt voor het massaal afleiden en kopiëren van profielen, het massaal vullen van de waarden voor de organisatieniveaus, het massaal doorvoeren van wijzigingen in profielen, het koppelen van enkele profielen naar samengestelde profielen en het koppelen van (samengestelde) profielen aan eindgebruikers.

Tip 14: Maak goede afspraken over de impactanalyse op de beveiliging bij wijzigingsverzoeken. Naast de implementatie van de andere complexe beheerprocedures raden wij aan om een procedure te implementeren waarin voor de wijzigingen een aparte impactanalyse wordt gedaan op het gebied van de beveiliging. Hiervoor dienen beveiligingsregels te worden opgesteld die een directe relatie hebben met het informatiebeveiligingsbeleid en de risico's vanuit de optiek van de interne controle. Daarnaast dient de impactanalyse te onderzoeken of wijzigingsverzoeken vanuit één deel van SAP R/3 negatieve bijeffecten kunnen hebben in andere delen. Door bijvoorbeeld ruimer te autoriseren voor de ene functie kunnen ook andere functies additionele bevoegdheden krijgen. Het autorisatieconcept kan namelijk op technisch vlak zeer verweven zijn tussen de verschillende rollen.

Tip 15: Analyseer het nut en de mogelijkheden van ondersteunende tools. Ter ondersteuning bij de inrichting of de controle (audit) op de bestaande inrichting is het gebruik van ondersteunende tools in opkomst. Het gebruik van deze tools heeft inderdaad voordelen. Zo kan de relatie tussen de veld- en de transactieautorisaties inzichtelijk worden gemaakt en kan efficiënt de kwaliteit van de inrichting op detailniveau worden vastgesteld. Het gebruik van deze tools door interne afdelingen (buiten de interne auditdienst) komt echter met name tot zijn recht als de inrichting al van voldoende niveau is. Anders zullen de geconstateerde tekortkomingen niet ongedaan kunnen worden gemaakt. Het op efficiënte en effectieve wijze wijzigen van een oncontroleerbaar, ondoorzichtig autorisatieconcept (spaghetti) is namelijk bijna onmogelijk. Een herinrichting kost dan vaak minder inspanning.

Tip 16: Betrek uw eigen beheerders bij de inrichting van het autorisatieconcept tijdens het project. Beheerproblemen zijn vaak te herleiden tot de beperkte betrokkenheid van de eigen beheerders bij de ontwikkeling (inrichting) van de autorisatieprofielen. Vaak worden uit tijdnood (zie Inleiding) de inrichtingsactiviteiten uitbesteed aan de derde partij. Aangezien de werking van het SAP-autorisatieconcept complex is, zal het voor de beheerders moeilijk zijn de impact van wijzigingen in profielen goed te doorgronden, indien zij niet bij de ontwikkeling betrokken zijn geweest. Het achteraf opleiden en trainen van de beheerders vraagt dan om een forse inspanning.

Documentatie

Er zijn verschillende soorten documentatie met betrekking tot gebruikers en autorisatiebeheer die tijdens de beveiligingsonderzoeken worden beoordeeld. Te denken valt onder andere aan opzetdocumentatie, inrichtingsdocumentatie en toewijzingsdocumentatie. De aangetroffen documentatie is vaak incompleet of verouderd, of er is nooit documentatie opgesteld. Het ontbreken van goede inrichtingsdocumentatie komt met name doordat het SAP R/3-systeem niet goed in de behoefte voorziet om de inhoud van meerdere profielen naast elkaar te presenteren.

Tip 17: Gebruik Access of Excel in combinatie met gegevens uit de SAP-tabellen om uw documentatie up-to-date te houden. Met behulp van een download van de tabellen uit SAP R/3 (bijvoorbeeld USR11, UST04, UST12, UST10S, UST10C) naar MS Access is het zeer goed mogelijk om snel documentatie te maken. Het is dan eenvoudig om het volgende vlot te documenteren:

* de transacties per profiel;
* de waarden van geselecteerde velden per profiel (vaak de organisatieniveaus);
* de koppeling van enkele profielen aan samengestelde profielen.

Indien de beheerder hierin wat handigheid ontwikkelt, kunnen binnen enkele uren deze documenten worden opgeleverd. De queries op deze tabellen kunnen ook als rapportages worden toegevoegd aan de SAP-rapportageboom voor Gebruikers en Autorisatiebeheer. Indien het inrichtingstraject nog vers in uw geheugen ligt, raden wij u aan de belangrijke beslissingen en inrichtingskeuzen alsnog vast te leggen.

Tot slot

In dit artikel hebben wij ons ten dele schuldig gemaakt aan de beperkte focus op de problematiek rondom het beveiligen van ERP-omgevingen. Met name is aandacht besteed aan het opzetten, inrichten en beheren van het SAP R/3-autorisatieconcept. Eén van de maatregelen in de sfeer van SAP R/3-beveiliging slechts, want het beveiligen van de SAP R/3-omgeving omvat een bredere scope. Denk hierbij bijvoorbeeld aan:

* het beveiligen van de bouw-, test-, opleidings- en acceptatieomgeving(en);
* het inrichten van overige integriteitscontroles (customizing, toleranties, validaties, maatregelen, etc.);
* het opzetten en inrichten van procedures, handboeken en werkinstructies als organisatorische maatregelen;
* het gebruiken van rapportages als regressieve controles;
* het beveiligen op het gebied van het besturingssysteem, het netwerk en de database (zie het artikel van Warmoeskerken en Van Dijke in deze Compact).

Na het kiezen van de SAP-internetapplicaties (mySAP) zal de focus van de beveiligingsmaatregelen zich nog sterker richten op de infrastructuur vanwege de introductie van nieuwe SAP R/3-netwerkcomponenten (SAP R/3-middleware, workplace) en de beveiliging hiervan in de zin van firewalls, routers en certificate authorities. Het inrichten van een goede beveiliging zal daarom complexer worden. Een verdergaande integratie van technisch en functioneel beheer op beveiligingsgebied zal dan zijn vereist.

A. Vreeke
is sinds vijf jaar werkzaam bij KPMG Information Risk Management. Zijn aandachtsgebied is informatiebeveiliging in ERP-omgevingen. Voor zijn specialisatie in ERP-beveiliging lagen zijn werkzaamheden op het gebied van Trusted Third Parties (TTP's) en Public Key Infrastructures (digitale identiteitsbewijzen). Met de integratie van digitale identiteitsbewijzen in SAP-omgevingen komen beide werelden samen. Deze integratie vormt het toekomstige werkterrein.

D.M. Hallemeesch
is sinds drie jaar werkzaam bij KPMG Information Risk Management. Hij is betrokken geweest bij een groot aantal complexe implementaties van het SAP-autorisatieconcept. Daarnaast voert hij jaarlijks een aantal aan SAP gerelateerde beveiligingsonderzoeken uit. Binnen het Competence Center is hij het aanspreekpunt op het gebied van de ondersteunende tools en de productontwikkeling.