KPMG Security Explorer voor SAP R/3
Efficiënt inrichten en beheren van SAP R/3-autorisaties

R.A. Jonker RE RA en ir. R. Ossendrijver

De Security Explorer is een door KPMG Information Risk Management ontwikkeld tool. Dit tool ondersteunt de SAP-beveiligingsspecialisten van KPMG bij de uitvoering van implementatie- en reviewopdrachten. Daarnaast is de uitgebreide rapportagefunctionaliteit bij uitstek geschikt voor autorisatiebeheerders om op een efficiënte en gebruiksvriendelijke manier toezicht te kunnen uitoefenen op de kwaliteit van de geïmplementeerde autorisaties. De functionaliteiten van de Security Explorer worden in dit artikel behandeld.

Achtergrond

De omvang en complexiteit van SAP R/3 en de veelheid van manieren waarop de applicatie kan worden ingebed binnen organisaties, vragen om een op maat toegesneden autorisatieconcept. Het autorisatieconcept binnen SAP R/3 is flexibel en biedt tal van mogelijkheden om bevoegdheden op een gewenst detailniveau in te richten. Deze rijke schakering aan functionaliteit heeft ook een schaduwzijde. Het inrichten en beheren van het autorisatieconcept is complex en mede daardoor een omvangrijke taak. De ervaring leert dat het inrichten van autorisaties gedurende een implementatieproject zonder additionele hulpmiddelen vaak een volledige dagtaak omvat. Ook het beheer van autorisaties inclusief het aanpassen van het concept als gevolg van releasewijzigingen is een veelomvattende en noodzakelijke taak. Ervaringen die zijn opgedaan met de inzet van de KPMG Security Explorer ten behoeve van het inrichten en het beheren van autorisaties wijzen op een aantoonbare tijdsbesparing. Tijdsbesparingen van twintig tot dertig procent zijn zeer realistisch. De investering in een gebruikerslicentie voor de KPMG Security Explorer verdient zich dan snel terug.

Voordat wij in het kader van dit artikel aandacht besteden aan de functionaliteiten van de Security Explorer is het goed eerst stil te staan bij de issues die opkomen bij de inrichting en het beheer van autorisaties. Daarbij hebben wij de insteek gekozen van het waarborgen van de vertrouwelijkheid, integriteit en beschikbaarheid van de in de SAP-databases op te slane of opgeslagen gegevens. Niet zelden zijn deze kwaliteitsaspecten tevens van belang voor de financiële verslaglegging. Binnen vrijwel iedere organisatie met SAP R/3 bestaan de volgende issues rond het autorisatieconcept:

R.A. Jonker RE RA
is partner bij KPMG Information Risk Management en geeft leiding aan een unit die gespecialiseerd is in Business System Controls audit en advisering.

jonker.ronald@kpmg.nl

Ir. R. Ossendrijver
is sinds 2003 werkzaam als junior consultant bij KPMG Information Risk Management. Hij is werkzaam als technisch auditor en houdt zich onder meer bezig met het ontwikkelen van auditsoftware zoals de KPMG Security Explorer en de KPMG Business Controls Monitor.

ossendrijver.ronald@kpmg.nl

Waarborging van functiescheiding

Regels die binnen de organisatie gelden omtrent functiescheiding moeten door het informatiesysteem worden afgedwongen. In de praktijk komt het echter vaak voor dat gebruikers (direct na ingebruikname of in de loop van de tijd) een dusdanige set bevoegdheden toegewezen hebben gekregen dat zij ongewenste combinaties van transacties kunnen uitvoeren. SAP R/3 dwingt functiescheiding niet af en alarmeert zelf niet op doorbrekingen, terwijl toewijzing van bevoegdheden vrij eenvoudig is en functievermenging snel kan ontstaan.

Beheerste toewijzing, wijziging en verwijdering van gebruikersbevoegdheden

De complexiteit van SAP R/3 maakt het voor beheerders moeilijk in te schatten wat de gevolgen van toewijzing van nieuwe bevoegdheden of het verwijderen van bestaande bevoegdheden zijn voor de totale set van bevoegdheden die een gebruiker heeft. Indien vragen bij de beheerder binnenkomen omtrent onvoldoende bevoegdheden is het met de standaard-SAP-rapportages vrij moeilijk (tijdrovend en kennisintensief) om te bepalen waarom de huidige gebruikersbevoegdheden niet alle functionele benodigdheden afdekken.

Kwaliteitsbewaking met betrekking tot de autorisatie-inrichting

De juistheid en de volledigheid van de autorisatie-inrichting dienen voor langere tijd te worden gewaarborgd. Het is dan wel nodig dat de autorisaties beheersbaar zijn. Wanneer beheerders geen duidelijk beeld meer hebben van de status van de autorisaties, of wanneer onderhoud onvoldoende gestructureerd plaatsvindt, zal steeds meer vervuiling in het systeem ontstaan wat de continuïteit in gevaar brengt.

Monitoren van risico's

Een organisatie dient continu op de hoogte te zijn van risico's die ontstaan vanuit de inrichting van bevoegdheden, teneinde hierop te kunnen anticiperen.

De aanpak

De KPMG Security Explorer voor SAP R/3 biedt beheerders en (interne) auditors een breed scala aan rapportagemogelijkheden met betrekking tot bovenstaande aandachtspunten. Ondanks de complexe materie is de werking van de Security Explorer eenvoudig, wat de cliënt na de initiële installatie en een korte training in staat stelt snel, geautomatiseerd en efficiënt de genoemde issues aan te pakken. Doorbrekingen van functiescheidingen kunnen bijvoorbeeld eenvoudig worden opgespoord.

Figuur 1. KPMG Security Explorer voor SAP R/3.

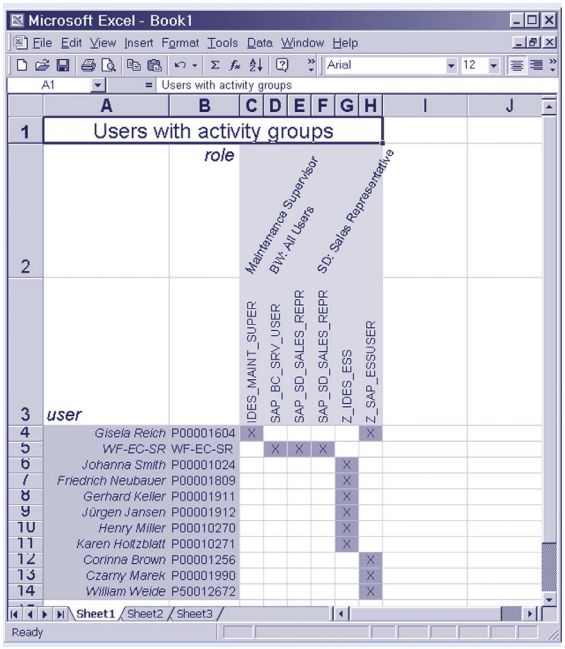
De Security Explorer is een 'weergavetool'. Dat wil zeggen dat het tool geen wijzigingen aanbrengt in de brondata die in de SAP-database zijn opgeslagen. De data die noodzakelijk zijn om de analyses uit te voeren, worden gedownload. Voorts bevat het tool geen alarmen of andere signaalfunctionaliteiten, die automatisch waarschuwen voor afwijkingen en dergelijke. De gebruiker dient de uitkomsten van de data-analyses zelf te beoordelen en te interpreteren. Wél is het tool uitgerust met een aantal standaard-rapportagefuncties, waarmee een groot aantal veelvoorkomende autorisatie-issues kan worden beoordeeld.

De rapportages van de Security Explorer vallen in twee groepen uiteen: *foutsignalerende rapportages*, die risico's als gevolg van onjuistheden of onvolledigheden binnen de autorisatie-implementatie rapporteren, en *systeemrapportages*, die door de gebruiker aangegeven informatie uit het SAP-systeem naar boven halen. Tabel 1 toont een greep uit deze twee groepen rapportages.

Aan de gebruiker kunnen de resultaten op twee manieren worden gepresenteerd: in de vorm van Excel-sheets en in de vorm van Access-rapporten (zie de figuren 2 en 3).

Tabel 1. Enkele Security Explorer-rapportages.

Signalerende rapportages	Systeemrapportages
Doorbrekingen van functiescheiding op gebruikersniveau	Gebruikersbevoegdheden
Doorbrekingen van functiescheiding op rolniveau	Aan gebruikers toegewezen rollen
Inactieve gebruikers	Opbouw van verzamelrollen uit enkele rollen
Gebruikers met kritieke bevoegdheden	Geïnstalleerde patches en support packages

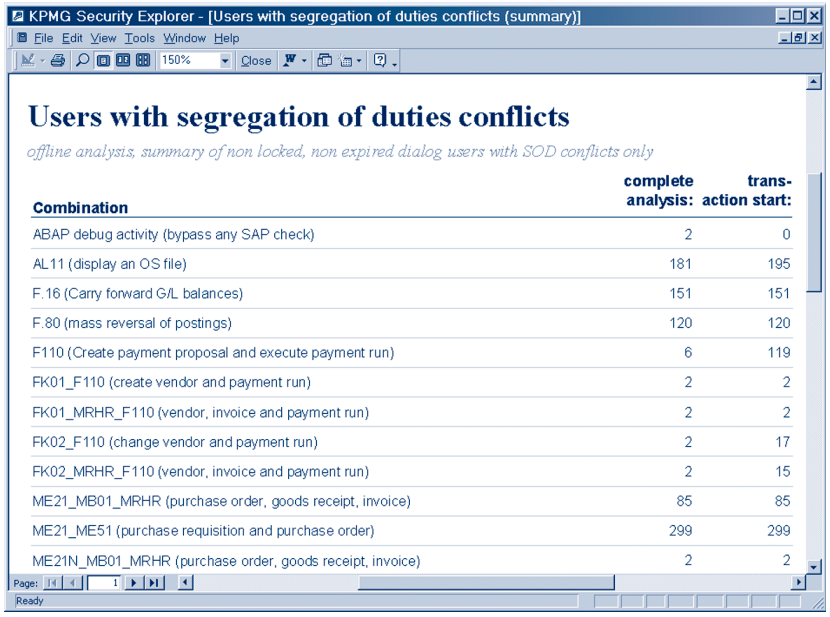


Figuur 2. 'Aan gebruikers toegewezen rollen' (systeemrapportage).

Vanzelfsprekend is het tool uitgerust met zoekcriteria-mogelijkheden, die de gebruiker in staat stellen vanuit diverse invalshoeken de kwaliteit van de ingerichte autorisaties te beoordelen (zie figuur 4).

Als beheertool kan de Security Explorer worden ingebed in beheerprocessen. De autorisatiebeheerder kan dan met vaste regelmaat de in het tool gedefinieerde rapportages, dan wel de eventueel op zijn verzoek in het tool aangelegde specifieke rapportages uitvoeren. Wanneer verzoeken om bevoegdheidstoewijzing of meldingen van onjuistheden in het systeem ontstaan, kan een SAP-beheerder op basis van de systeemrapportages een weloverwogen gepaste actie ondernemen.

Figuur 3. 'Functiescheidings-conflicten binnen het systeem' (signalerende rapportage).



De werking

De installatie van de Security Explorer stelt nauwelijks eisen aan de IT-infrastructuur. Er hoeven geen wijzigingen te worden aangebracht in het SAP-systeem en de software draait op iedere pc met Microsoft Windows, Microsoft Access 2000 (of een gratis beschikbare 'runtime versie' van Microsoft Access) en een installatie van de SAP GUI, de client software van SAP. Verbinding met SAP is slechts noodzakelijk om eenmalig de autorisatierelevante tabellen uit SAP in te lezen. Indien een verbinding met SAP niet mogelijk is kunnen de tabellen ook met de standaard-SAP-transactie SE16 worden opgeslagen en door de Security Explorer worden ingelezen.

Ten behoeve van het inzicht in de werking van de Security Explorer is in figuur 5 een schematisch overzicht opgenomen van de manier waarop autorisaties binnen SAP geregeld zijn.

In de onderste laag zijn de schermen van twee SAP-transacties afgebeeld. We zien dat de bevoegdheden voor het lezen of bewerken van gegevensvelden binnen die transacties verwijzen naar 'autorisatieobjecten'. Deze autorisatieobjecten kunnen via profielen en rollen gekoppeld zijn aan gebruikers. Een gebruiker kan slechts een transactie opstarten of gegevensvelden wijzigen indien de daarvoor vereiste autorisatieobjecten aan hem toegewezen zijn.

Deze informatie is, zoals alles in SAP R/3, opgeslagen in tabellen die continu gewijzigd worden en daardoor altijd de geldende bevoegdheden binnen het systeem weergeven. Wanneer de Security Explorer deze tabellen uit SAP inleest, of wanneer ze geëxporteerd worden met behulp van de SE16-transactie, wordt een 'snapshot' gemaakt van de situatie op dat moment. Alle analyses die daarna over deze gegevens worden uitgevoerd, geven de situatie weer op het moment dat het snapshot gemaakt werd. Figuur 6 laat dit zien.

Praktijkervaring

Op dit moment wordt de Security Explorer gebruikt zowel door KPMG IRM als door enkele van haar cliënten. Tegelijkertijd met het praktijkgebruik wordt de functionaliteit van het tool uitgebreid met ideeën en wensen van gebruikers. Onze ervaring is dat meestal al vanaf het

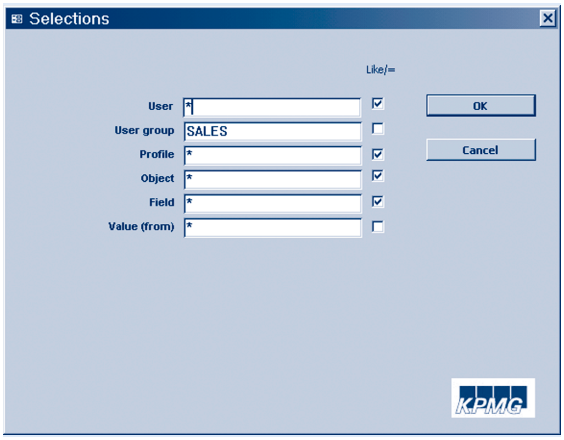
begintraject (tijdens productpresentaties of met het gebruik van de proeflicenties die voor perioden van twee maanden verstrekt worden) suggesties vanuit de cliënt naar voren komen. Tegelijkertijd zijn wij zelf druk bezig om het tool verder uit te rusten met additionele functionaliteiten en het tool technisch verder te optimaliseren. Nieuwe versies van het tool worden dan tegen een vast percentage van de oorspronkelijke licentievergoeding aan onze cliënten aangeboden.

Conclusies

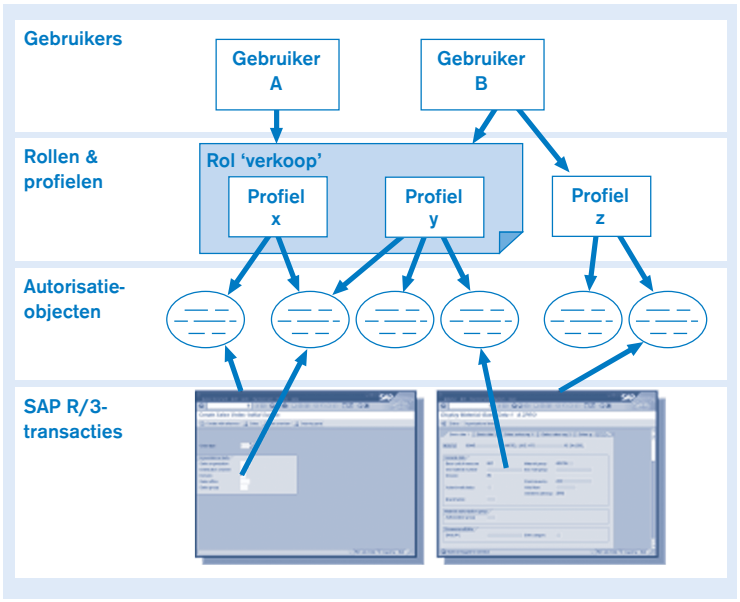
De KPMG Security Explorer maakt zowel het beheer als de audit van autorisaties binnen SAP R/3 efficiënter en doeltreffender door op een gebruiksvriendelijke en flexibele manier te rapporteren over belangrijke aspecten rond de autorisatie-inrichting. Dit gebeurt zonder hoge eisen te stellen aan de gebruikers en de IT-infrastructuur. De Security Explorer is geschikt voor gebruik door implementatiespecialisten, beheerders en auditors. Ervaringen met de Security Explorer wijzen uit dat tijdsbesparingen van twintig tot dertig procent zijn te realiseren bij implementatie- en beheerwerkzaamheden. Door de omvangrijke functionaliteit en de werking van het tool zijn de uitkomsten voorts nauwkeuriger dan bij inzet van standaard-SAP-tools en daardoor draagt het tool bij aan de doeltreffendheid van de inrichtings-, beheer- en auditwerkzaamheden.

Literatuur

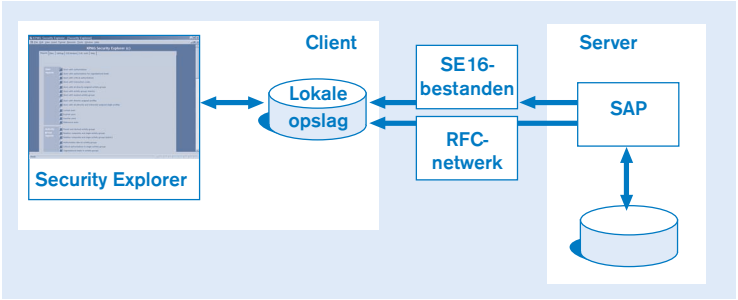
[Vree01] A. Vreeke en D.M. Hallemeesch, *Richt jij de autorisaties even in? De complexiteit van het SAP R/3-autorisatieconcept*, Compact 2001/6.



Figuur 4. Specifieke informatie uit SAP R/3 halen op basis van zoekcriteria.



Figuur 5. Autorisaties binnen SAP R/3.



Figuur 6. Gegevenstransport tussen de Security Explorer en SAP.