Back to the future: Limpergs gedachtegoed in andere tijden

Hans Leenaars en Edo Roos Lindgreen

SAMENVATTING In dit artikel wordt gezocht naar de wetenschappelijke belangstelling van Limperg voor het vakgebied 'Bestuurlijke informatieverzorging' en meer in het bijzonder voor de wijze waarop organisaties en processen worden beheerst. Geconstateerd wordt dat – voorzover Bestuurlijke informatieverzorging aan de orde is – het efficiency-vraagstuk Limperg meer interesseerde dan de vraagstukken, die bij de beheersing van organisaties en processen centraal staan. Toch zijn er enige relevante aanknopingspunten in het werk van Limperg te vinden. Na bespreking hiervan vervolgt het artikel met de verschillende wijzen waarop arbeidsdeling of functiescheiding de beheersbaarheid van organisaties en processen in de tijd van Limperg en van vandaag dient. Ten behoeve van een verdere concretisering wordt de implementatie van moderne functiescheiding in een ERP-pakket toegelicht. Ten slotte wordt geconcludeerd, dat, hoewel Limperg niet tot uitwerking is gekomen, hij het belang van arbeidsdeling voor de controle heeft onderkend.

1 Inleiding

De wereld van Limperg was in veel opzichten een andere dan de onze. Het was een wereld zoals die wordt geschetst in boeken en films die zich afspelen in het begin van de vorige eeuw: paardentrams, kostuums, donker hout. Een wereld zonder plastic, zonder televisie, zonder informatietechnologie. Maar het was ook een wereld vol technologische ontwikkelingen en economische problemen. Die problemen maakten volgens velen strenge besparingen op de bedrijfsuitgaven noodzakelijk, besparingen die konden worden gerealiseerd door efficiënter te werken. Limperg lijkt door deze noodzaak haast gebiologeerd. Indien men het dagboek van zijn reis door de Verenigde Staten doorleest, dan valt al snel op dat het fenomeen, waarin Limperg het meest is geïnteresseerd, de standaardkostprijscalculatie betreft. Natuurlijk weerspiegelt dit dagboek ook de overheersende aard van de economische bedrijvigheid in het Amerika van die tijd: de industriële productie, maar de belangstelling van Limperg is zeer diepgaand.

Prof. Dr. J.J.A. Leenaars is lid Raad van Bestuur van NV Bank Nederlandse Gemeenten. Prof. Dr. E.E.O. Roos Lindgreen is partner van KPMG. Beiden zijn daarnaast als hoogleraar verbonden aan de Universiteit van Amsterdam.

Hoe hoog de nood ook in Nederland was, blijkt uit de oprichting, in 1925, van het Nederlandsch Instituut voor Efficiency, een vereniging die tot doel had 'het verzamelen en verbreiden van kennis omtrent efficiency en in het bijzonder het samenbrengen en bevorderen van samenwerking van alle lichamen en personen, die bereid zijn aan de verwezenlijking van het doel mede te werken'. Het biografisch woordenboek (De Vries, 1994) vermeldt Limperg als oprichter van het Instituut. Aangezien automatisering het middel bij uitstek is om efficiency te bevorderen, zou het in de context van dit artikel aardig zijn geweest om stil te staan bij het belang van de efficiencybeweging en de grote betrokkenheid van Limperg hierbij. Die betrokkenheid zou meer dan voldoende zijn om Limperg, met terugwerkende kracht en met enige fantasie, tot vooroorlogs boegbeeld van de automatisering te verklaren. Maar helaas, in de notulen van de oprichtingsvergadering, gedateerd 12 december 1925, komt de naam Limperg niet voor. Op de lijst van aanwezigen staan wel veel andere accountants, waaronder ene Klijnveld. Maar Limperg ontbreekt.

Ook in andere bronnen hebben wij geen gegevens kunnen vinden waaruit zou blijken dat Limperg een meer dan zijdelingse relatie met de efficiency-

beweging heeft gehad. De notulen van de oprichtingsvergadering, die plaatsvond in de bekende industriële Club in Amsterdam, besluiten als volgt: 'Nadat de heer J. Hagers enkele opmerkingen had gemaakt, waarin hij erop wees, dat de Duitsche en Belgische zusterorganisaties zeker met belangstelling het werk van het nieuwe instituut zullen volgen, in het licht stelde, dat het Engelsche woord 'efficiency' in den naam moest worden gekozen, omdat geen Nederlandsch woord het begrip volkomen dekt – 'bezuiniging' toch is niet hetzelfde – en voorts betoogde dat het winstmaken als doel voor particuliere bedrijven niet zoo moet worden opgevat, dat de bedrijven 'grijpgieren' zijn – efficiency kan de bedrijfskosten en daarmee de verkoopprijzen doen dalen en zoo de verbruikers ten goede komen – sloot de voorzitter, de heer Ed Gerzon, de bijeenkomst met de opwekking voor het nieuwe instituut belangstelling te kweeken'. Een kort pleidooi voor het maatschappelijk belang van efficiency, waarbij ook hier opvalt hoe uitgebreid, formeel, zelfs plechtig de tijdgenoten van Limperg schreven en spraken – een wijze van communiceren die sterk verschilt van de krachtige termen, korte zinnen en Powerpoint-presentaties van nu.
In dit artikel wordt gezocht naar de wetenschappelijke belangstelling van Limperg voor de beheersbaarheid van processen, die spelen binnen organisaties. De beheersbaarheid van deze processen is een van de belangrijkste objecten van onderzoek van het vakgebied Bestuurlijke Informatieverzorging.
Omdat functiescheiding – traditioneel en modern – een zeer basale rol speelt bij beheersbaarheid, gaan we in paragraaf 2 van dit artikel op zoek naar Limpergs gedachten over functiescheiding, of meer algemeen over arbeidsdeling. In 'modern Nederlands' gezegd: in paragraaf 2 wordt gezocht naar een antwoord op de vraag: 'Wat heeft Limperg met functiescheiding?'
In paragraaf 3 komt moderne functiescheiding aan de orde; en in paragraaf 4 wordt implementatie van moderne functiescheiding met behulp van een ERP-pakket (SAP) toegelicht.

2 Limperg en moderne Bestuurlijke informatieverzorging

Het zou niet fair zijn in Limpergs werk op zoek te gaan naar hedendaagse inzichten in de beheersbaarheid van organisaties en processen en vast te stellen dat dit inzicht ontbrak. Het is ons inziens wel gerechtvaardigd om vast te stellen dat de belangstelling van Limperg vooral uitging naar de vakgebieden kosten en kostprijs, leer van de accountantscontrole en organisatieleer.

Limperg heeft ons een omvangrijk (door Drs. G.D. Ribbius bewerkt) collegedictaat nagelaten, dat de titel 'Leer der organisatie' draagt.
In de delen I en II van dit dictaat, waarin de externe organisatie onderwerp van studie is, komen we weinig aanknopingspunten voor bestuurlijke informatieverzorging tegen; één aantekening is evenwel vermeldenswaard. Arbeidsverdeling, aldus Limperg (het begrip functiescheiding wordt niet gebruikt) leidt onherroepelijk tot hergroepering van soortgelijke taken, hetgeen de interne controle bemoeilijkt. Dit lijkt wat vreemd in Limpergs tijd, omdat het groeperen van taken om redenen van controle gelet op arbeidskosten en de sterke verbijzondering van administratieve activiteiten, niet op overwegende bezwaren zou hoeven stuiten. Toch is deze opmerking wel verklaarbaar uit de oplossing die Limperg kiest; dit zal even verderop in deze paragraaf worden toegelicht.

Deel III (inclusief een supplement) van het dictaat behandelt de 'Technische markt, voorraad en handel' (onderwerp is termijnmarkten), en is voor dit artikel niet interessant.

De delen IV en V hebben de interne organisatie tot onderwerp. In deel IV komt Limperg het dichtste bij de beheersbaarheid (met behulp van informatie) van organisaties, die beoefenaars van het vakgebied Bestuurlijke Informatieverzorging interesseert.
Limperg heeft aandacht voor de controle op de uitvoering, voor directe en indirecte controle en voor steekproeven. Hij onderscheidt constituerende en dirigerende leiding en stelt vast dat de dirigerende leiding controlerende elementen bevat en 'derhalve zichzelve controleert': '…. nodig is een verbijzonderd controleapparaat'. Limperg acht deze – in termen van vandaag – verbijzonderde interne controle mogelijk in de vorm van bijzondere controleurs en door middel van het administratieve controleapparaat. Uit de volgende twee citaten blijkt (het eerste) dat Limperg heel dicht bij de uitwerking van Starreveld komt (een administratie, die in functiescheiding tot stand gebrachte elkaar controlerende deelverantwoordingen op elkaar afstemt) maar ook (het tweede), dat hij volstrekt anders concludeert dan alles wat het vak Bestuurlijke Informatieverzorging heeft voortgebracht.

Citaat 1. '*Men streeft naar een verbijzondering in het administratieve apparaat, waarbij de individuen en de door hen verstrekte gegevens elkaar controleren ...*'
Citaat 2. '*… maar stuit daarbij op de volgende bezwaren:*

- *eene irrationele vermenigvuldiging van de administratieve arbeid,*
- *eene beperking der mogelijkheid van de onderhavige functieverdeling in verband met de grootte der productiehuishouding,*
- *beperkt nuttig effect dier functieverdeling, doordat de individuen in kwestie in het productieproces in te nauwe samenwerking met elkaar staan: de actieve controle (beoordeling van de handelswijze van de gecontroleerde) stuit hierdoor op rangverschil en is absoluut fout, indien uitgeoefend door een functioneel ondergeschikte: zij moet dus wat de hogere organen der dirigerende leiding betreft, aan den leider worden overgelaten.*'

Vervolgens concludeert Limperg, en deze oplossing is de bijzondere slotsom rondom arbeidsverdeling, waarop hierboven in de eerste alinea's van deze paragraaf werd gedoeld, dat deze – in onze termen – interne controle in een nieuwe verbijzondering, in casu door de 'Public Accountant' moet worden uitgevoerd.

De administratie beperkt zich inzake interne controletaken in de zienswijze van Limperg tot:
- de bedrijfsbegroting met conjunctuur- en marktanalyse;
- efficiency- en kostenstandaarden;
- het plannen; en
- de routebepaling.

In deel V ten slotte vinden we nog een hoopvol citaat: 'De actie, dus de beheersing van de handeling in het bedrijf is het wezenskenmerk der interne organisatie …,' maar met de verdere uitwerking wordt geen aansluiting gevonden bij hedendaagse inzichten.
Hoe anders kijken wij anno 2004 aan tegen het belang van interne controle. Hoe zouden door de leiding 'in control statements' kunnen worden afgegeven, als de interne beheersing geen sluitend systeem vormt?

3 Moderne functiescheiding

Hoe kun je in een tijd, waarin de groepering van taken in functies op zijn best secundair rekening houdt met interne controlemotieven, de resulterende functiescheiding gebruiken als fundament voor een adequaat systeem van interne controle en beheersing? Antwoord: door slim gebruik te maken van de mogelijkheden die IT biedt.
Bij de inrichting van organisaties geldt een aantal criteria, aan de hand waarvan individuele taken in door mensen uitgeoefende functies worden gegroepeerd. Deze criteria zijn: het economisch motief, in casu de groepering van – naar waarde – soortgelijke arbeid, kennis, bekwaamheid en ervaring, de span of control, de geografische spreiding van de organisatie en de interne controle.
Omdat de kosten verbonden aan de productiefactor 'arbeid' steeds hoger worden, zijn veel inspanningen gericht op het reduceren van de inzet van deze productiefactor. In essentie geschiedt dit door de substitutie van arbeid door kapitaal, in casu door automatisering. Hierbij hebben allerlei communicatietoepassingen – in de brede zin van het woord – voor uitstoot van arbeid zorg gedragen.
Hoewel het belang van functiescheiding als preventieve maatregel van interne controle niet kleiner is geworden – het tegendeel is eerder juist gelet op steeds snellere bedrijfscycli, grotere financiële belangen en een groeiend aandeel abstracte activiteiten –, leidt de uitstoot van arbeid en de daarmee samenhangende hergroepering van resterende taken tot de vaststelling dat er minder mogelijkheden zijn voor een implementatie van functiescheiding à la Starreveld[1].
Daarbij moet nog worden aangetekend dat een noodzakelijke begeleider van functiescheiding, namelijk procedures: de in termen van detailtaken voorgeschreven betrokkenheid van functies bij bedrijfsprocessen, moeilijker kunnen worden gehandhaafd in een gedurig veranderende omgeving. Procedures hebben immers de neiging om op zijn best met enige vertraging te worden aangepast.
Wat is het belang van functiescheidingen à la Starreveld voor het tot stand komen van betrouwbare, waarheidsgetrouwe informatie (Leenaars, 1993)?

1 Informatie die nodig is voor het besturen, beheersen, doen functioneren en afleggen van verantwoording dient waarheidsgetrouw te zijn.
2 Informatie ten behoeve van deze vier doelstellingen bestaat in belangrijke mate uit inhoudelijk dezelfde bouwstenen.
3 Een belangrijke plaats wordt ingenomen door díe informatie die dient als verantwoording, onder meer jegens het maatschappelijk verkeer. Een voorbeeld van deze informatie is de jaarrekening.
4 Een dergelijke verantwoording is opgebouwd uit deelverantwoordingen.
5 Een belangrijke waarborg voor de waarheidsgetrouwheid van deze deelverantwoordingen wordt verkregen door ze door van elkaar gescheiden functies te laten creëren.
6 Het scheiden van functies zal primair op basis van doelmatige arbeidsverdeling plaatsvinden. Hiermee wordt bedoeld dat taken niet willekeurig tussen functies zullen worden verdeeld.

7 Slechts in uitzonderingsgevallen zal het doelmatigheidsbeginsel bij het scheiden van functies geen primaat hebben. Waar dat het geval is, is sprake van controletechnische[2] functiescheiding.
8 De onder 5 genoemde waarborg krijgt alleen inhoud indien sprake is van gescheiden verantwoordelijkheden; dit impliceert de aanwezigheid van tegengestelde belangen.
9 De interne controle maakt van dit fenomeen gebruik door de deelverantwoordingen op elkaar af te stemmen.
10 Tegengestelde belangen zijn aanwezig, indien een voordeel voor de ene functie zich laat vertalen in een nadeel voor een andere functie. Deze congruentie van voor- en nadelen hoeft niet alleen betrekking te hebben op directe financiële belangen – zoals tussen een afdeling verkoop en een vertegenwoordiger die op provisiebasis werkt – maar ook op carrièremogelijkheden, prestige van een afdeling binnen een organisatie en dergelijke.
11 Wil een dergelijk tegengesteld belang van betekenis zijn voor de interne controle, dus wil het voordeel voor de ene functie dat vertaald kan worden in een nadeel voor de andere functie betekenis hebben, dan dient dit voordeel respectievelijk nadeel te kunnen worden vastgesteld.

Het belangrijkste verschil tussen de inrichting van organisaties uit de tijd van Limperg en Starreveld en van vandaag is het verdwijnen van een groot gedeelte van de onafhankelijke registrerende functie; onafhankelijk van beschikkende en bewarende functies.
Waar de registratie van het bedrijfsgebeuren vroeger plaatsvond door de registrerende functie aan de hand van basisdocumenten, vindt de vastlegging vandaag plaats door productiemachines en applicaties, *die onder controle staan van beschikkende en bewarende functies.*
Als voorbeeld kan een eenvoudige (kantoor)voorraadadministratie gelden: waar vroeger de 'af-mutatie' bestond uit de opdracht van de verkoopafdeling aan het magazijn, welke opdracht door de registrerende functie in de kantoorvoorraadadministratie werd verwerkt, wordt de voorraadadministratie van vandaag gevoed door transacties die door de verkoopafdeling en/of het magazijn worden uitgevoerd.
Waar functiescheidingen noodzakelijk blijven voor het produceren van aantoonbaar betrouwbare informatie ten behoeve van het besturen, beheersen en doen functioneren van organisaties, alsmede ten behoeve van het afleggen van verantwoording, moeten de niet langer toepasbare functiescheidingen à la Starreveld worden vervangen door 'functiescheidingen nieuwe stijl'.

Functiescheidingen nieuwe stijl – in dit artikel ook moderne functiescheiding genoemd – worden gedefinieerd als: het door functionarissen zowel exclusieve als gedwongen gebruik van de computer, in casu van geautomatiseerde activiteiten om bepaalde taken te kunnen uitvoeren, waarbij registratie door volkomen automatisme wordt gewaarborgd.
'Gedwongen' impliceert dat (fysieke) bedrijvigheid niet anders dan met behulp van de computer, in casu van applicaties in gang kan worden gezet of kan worden aangestuurd. 'Exclusief' duidt op het via een toegangscontrolemechanisme toewijzen van bepaalde geautomatiseerde activiteiten (transacties) aan bepaalde (individuele) functionarissen, zodanig dat deze activiteiten uitsluitend door deze functionarissen kunnen worden uitgevoerd.
Waar derhalve functiescheiding à la Starreveld is gebaseerd op procedureel voorgeschreven betrokkenheid van meerdere functionarissen bij bedrijfsprocessen (de waardenkringloop) is bij functiescheiding nieuwe stijl één der partijen steeds een volgens geprogrammeerde regels werkende automaat. Deze automaat is per definitie consequenter in zijn activiteiten dan autonoom denkende en aan gemoedstoestanden onderhevige mensen.
Functiescheiding nieuwe stijl is derhalve in termen van handhaving ('gedurige werking') als preventief middel van interne controle zeer waarschijnlijk sterker dan functiescheiding à la Starreveld.

In de zin van 'beschikken, bewaren en registreren' zou ook kunnen worden gezegd dat functionarissen in een (vergaand) geautomatiseerde omgeving beschikken over gegevens.
Het wijzigen, toevoegen en verwijderen van gegevens dient derhalve aan eisen van functiescheiding te voldoen. De implementatie van functiescheiding nieuwe stijl kan met behulp van een functieverdeelstaat en een transactie-impactanalyse zichtbaar worden gemaakt (Leenaars, 1993).
Het is ten slotte nog van belang om op twee begrippen te wijzen, die voorwaarden zijn voor het hierboven bedoelde exclusieve gebruik van bepaalde geautomatiseerde activiteiten door bepaalde (individuele) functionarissen.

Deze begrippen zijn authenticatie en autorisatie.
Authenticatie is een proces met behulp waarvan een functionaris bewijst dat hij degene is voor wie hij zich uitgeeft. Anders gezegd: identificatie van jezelf jegens een computer, en de verificatie van de aangenomen identiteit door die computer.
Autorisatie is een proces waarin bevoegdheden wor-

den toegekend. Autorisatie wordt geïmplementeerd met behulp van een toegangscontrolemechanisme. Het moge duidelijk zijn dat het hierboven genoemde gedwongen en exclusieve gebruik van de computer, in casu van geautomatiseerde activiteiten en het 'beschikken over gegevens' alleen dan tot een sterk preventief middel van interne controle leidt als de authenticatie- en de autorisatiemechanismen deugdelijk zijn uitgevoerd.
Dit komt in de volgende paragraaf, waar als voorbeeld SAP wordt gebruikt, in enig detail aan de orde.

4 Functiescheidingen in ERP-systemen

De grootschalige invoering van systemen voor Enterprise Resource Planning (ERP), zoals SAP, J.D. Edwards, Peoplesoft of Oracle, is een van de belangrijkste IT-ontwikkelingen in middelgrote en grote organisaties van de laatste tien jaar. Deze systemen integreren een breed scala aan ondersteunende functies voor de meest uiteenlopende bedrijfsprocessen, zoals logistiek, financiële administratie, personeelszaken, planning en productie. Kenmerkend voor ERP-systemen zoals SAP is dat zij gebaseerd zijn op een centrale gegevensopslag, die kan bestaan uit tientallen databases met daarin duizenden tabellen, en waarin alle relevante gegevens slechts één keer zijn opgeslagen. Dit heeft grote voordelen voor de efficiency, de uitwisselbaarheid, de uniformiteit en de consistentie van de gegevens en verwerking van die gegevens. Aan het gebruik van ERP-systemen zijn, in vergelijking met traditionele informatiesystemen, echter ook specifieke risico's verbonden (Vaassen, 2003). De grotere onderlinge afhankelijkheid tussen bedrijfsprocessen maakt een ERP-systeem en daarmee de onderneming gevoeliger voor verstoringen; tegelijkertijd leidt de geïntegreerde architectuur van het ERP-systeem tot een verhoging van het risico dat een onbevoegde via een tekortkoming in één module toegang krijgt tot het gehele systeem.
Authenticatie binnen ERP-omgevingen is doorgaans gebaseerd op het gebruik van gebruikersnamen en wachtwoorden. Deze simpele techniek biedt vele voordelen – waaronder relatief gebruiksgemak en lage aanschafkosten – maar kent ook tal van nadelen, waaronder de beperkte mate van bescherming die wordt geboden. Onderzoek wijst uit dat grofweg 25% van alle gebruikte wachtwoorden eenvoudig te achterhalen is; wat dit betekent voor de beoogde functiescheidingen, laat zich raden. Nieuwe authenticatietechnieken als smartcards, public-key infrastructures en biometrie zijn voorhanden, maar worden in de praktijk nog zelden toegepast.

Autorisatie binnen een ERP-omgeving is gebaseerd op het aloude principe van een competentietabel, waarin de toegangsrechten van subjecten (gebruikers) tot objecten (functies en gegevens) in het systeem gedefinieerd zijn. In ERP-land wordt niet gesproken van competenties, maar van 'autorisaties', welk taalgebruik wij hier zullen overnemen. Het inrichten en onderhouden van autorisaties in ERP-omgevingen is een complexe aangelegenheid; wij bespreken deze problematiek hieronder bij de tweede fase van implementatie van ERP-systemen verder.

Hoe zou Limperg hebben aangekeken tegen de werkzaamheden van de accountant – en dan met name rond het aspect functiescheidingen – in dit soort vergaand geautomatiseerde omgevingen?
Laten wij bij het beantwoorden van deze vraag onderscheid maken tussen twee fasen: de fase die aanvangt vlak na het in productie nemen van het ERP-systeem, waarin het systeem doorgaans nog niet naar behoren is ingericht en vaak nog sprake is van kinderziektes, en de daaropvolgende fase, waarin het systeem is doorontwikkeld, de inrichting is voltooid en de noodzakelijke fijnafstemming heeft plaatsgevonden.

De reden voor dit onderscheid is dat de invoering van informatiesystemen over het algemeen niet glad verloopt. Mede door de tijdsdruk die ontstaat in de slotfase van de invoering, krijgen de noodzakelijke aanpassingen van de maatregelen op het gebied van Bestuurlijke Informatieverzorging en interne controle onvoldoende of zelfs in het geheel geen aandacht. In veel gevallen wordt een nieuw ERP-systeem in productie genomen zonder dat de Bestuurlijke Informatieverzorging op het nieuwe systeem is afgestemd. Dit leidt tot tekortkomingen zoals te ruim ingerichte autorisaties, onjuiste factuurgegevens, gebruikers die geen gebruikmaken van de beheersingsmaatregelen in het systeem maar terugvallen op eigen lijstjes, verschillen tussen fysieke voorraden en voorraden in het systeem, en allerlei problemen die voortvloeien uit onvolkomenheden in de conversie van gegevens (Mancham en Brouwers, 2001). Het zal duidelijk zijn dat een ERP-systeem in deze levensfase bijzondere aandacht behoeft van de controlerend accountant.

Ook in de tweede fase, waarin het systeem naar behoren werkt en de belangrijkste maatregelen op het gebied van Bestuurlijke Informatieverzorging zouden moeten zijn ingevoerd, verdienen ERP-systemen bijzondere attentie. In de praktijk blijkt dat vooral de autorisaties in een ERP-omgeving aanleiding kunnen geven tot zorgen. Veel organisaties hebben moeite

met het inrichten en onderhouden van deze autorisaties, die onmisbaar zijn voor het realiseren van de noodzakelijke functiescheidingen. In dat geval loopt de organisatie direct risico's ten aanzien van de betrouwbaarheid van de gegevensverwerking, omdat essentiële functiescheidingen eenvoudig doorbroken kunnen worden (Vreeke en Hallemeesch, 2001).
Uit onderzoek van Vreeke en Hallemeesch (2001) blijkt dat bij het merendeel van 35 onderzochte organisaties sprake is van ernstige tekortkomingen in de beveiliging van de ERP-omgeving. De onderzoekers maken onderscheid tussen basismaatregelen en de inrichting en het beheer van de autorisaties. De geconstateerde tekortkomingen hebben betrekking op elk van deze gebieden.

De basismaatregelen omvatten onder meer het afsluiten van het systeem voor wijzigingen, het wijzigen van de standaardgebruikers, het verwijderen van 'superusers', ofwel gebruikers die in het productiesysteem alle transacties kunnen uitvoeren, het blokkeren van kritische systeemtransacties, het inrichten van relevante beveiligingsparameters als wachtwoordlengte en het afbreken van inactieve sessies, en het inrichten van wachtwoordrestricties. Dat deze basismaatregelen zulke tekortkomingen vertonen is merkwaardig, omdat het treffen van deze maatregelen volgens de auteurs een fluitje van een cent is. Een bekwaam beheerder kan zich de benodigde expertise binnen een halve dag eigen maken en ook het instellen van de bijbehorende parameters vergt hooguit enkele uren.

De maatregelen op het gebied van inrichting en beheer van autorisaties hebben betrekking op het 'op maat snijden' en onderhouden van autorisatieprofielen, rollen en activiteitgroepen op de verschillende functies binnen de organisatie. Zeker in grotere ERP-omgevingen is dit een complexe en daardoor foutgevoelige aangelegenheid. Wij citeren Vreeke en Hallemeesch (2001) over het inrichten van autorisaties in SAP: 'Men kan binnen SAP als eerste autoriseren op de transacties die een functie of gebruiker kan opstarten, en daarna op welke activiteiten en veldwaarden hij binnen die transactie kan en mag invoeren. Bijvoorbeeld: het wel of niet kunnen invoeren van een inkooporder is een 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 800 veldautorisaties mogelijk voor duizenden transacties en rapportages. De transacties die een functie in de organisatie (of een gebruiker) mag opstarten, plus de daartoe behorende veldautorisaties, legt men vast in een autorisatieprofiel. De hoeveelheid veldkeuzen en transacties maakt het direct complex. … 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.' Daarbij komt dat autorisaties zelden worden getest op te ruime bevoegdheden. Ook het beheer van autorisaties kent vaak tekortkomingen. Het gaat hierbij om het uitgeven van nieuwe autorisaties, het intrekken van gebruikers die van functie veranderen of uit dienst treden, of het deactiveren van 'slapende' accounts. Het gevolg van deze tekortkomingen is dat de autorisaties in ERP-systemen vaak veel 'ruimer' zijn ingericht dan op grond van de bestaande, in de organisatie vastgelegde functiescheidingen de bedoeling kan zijn.

Deze problematiek houdt overigens niet op bij de inrichting van autorisaties in het ERP-systeem zelf. Ook de beveiliging van de technische infrastructuur, waarop het ERP-systeem draait, is van belang. Is die beveiliging niet in orde, dan kunnen onbevoegden via het netwerk toegang krijgen tot de ERP-omgeving, waarna zij de autorisaties in deze omgeving ongemerkt kunnen aanpassen. Zie Roos Lindgreen, Overbeek en De Wolf (2004) voor meer informatie.

Wij zien dat autorisaties in ERP-omgevingen van fundamenteel belang zijn voor het inrichten van de benodigde functiescheiding, en dat deze autorisaties in de praktijk tal van tekortkomingen vertonen. Concreet betekent dit dat de accountant er zeer verstandig aan doet om in de jaarrekeningcontrole bijzondere aandacht te besteden aan de inrichting van het ERP-systeem en daarbij een IT-auditor in te schakelen die goed is ingevoerd in de complexe wereld van autorisaties en andere beheersingsmaatregelen. Vaassen (2003) stelt dat accountantskantoren heldere richtlijnen dienen te implementeren voor het inzetten van IT-auditors in de jaarrekeningcontrole, met inbegrip van het consequent bewaken van de naleving ervan.

5 Conclusie

Als conclusie van dit artikel mag ten slotte gelden, dat Limperg het belang van arbeidsdeling, van functiescheiding voor de controle heeft onderkend, hoewel hij dit niet heeft uitgewerkt. In de woorden van Limperg: '…. waarbij individuen en de door hen verstrekte gegevens elkaar controleren'. ■

Literatuur

Leenaars, J.J.A., (1993), *Funktiescheidingen in hooggeautomatiseerde omgevingen*, Samsom.

Limperg, Th., *Leer der organisatie*, delen I, II, III, IV en V, bewerkt door Drs. G.D. Ribbius.

Mancham, P.J. en P.P.B. Brouwers, (2000), ERP en AO/IC-alignment, in: *De Accountant*, november 2000.

Roos Lindgreen, E., P.L. Overbeek en R. de Wolf, (2004), De accountant en de kruipruimte, in: *Maandblad voor Accountancy en Bedrijfseconomie*, jg. 78, nr. 1/2, pp. 16-22.

Vaassen, E., (2003), Risico-inschattingen door accountants in het kader van Enterprise Resource Planning-systemen, in: *Maandblad voor Accountancy en Bedrijfseconomie*, jg. 77, nr. 11, pp. 509-520.

Vreeke, A. en D. Hallemeesch, (2001), Richt jij de autorisaties even in?, in: *Compact*, 2001/6, pp. 27-33.

De Vries, Joh., (1994), Limperg [jr.], Théodore (1879-1961), in: *Biografisch Woordenboek van Nederland*.

Noten

1 In dit artikel wordt gesproken over functiescheiding à la Starreveld. Uiteraard is (traditionele) functiescheiding niet een exclusieve vondst van Starreveld; het is een belangrijk leerstuk van de klassieke inrichtingsleer.

2 In tegenstelling tot in veel literatuur wordt hier alleen dan van controletechnische functiescheiding gesproken indien deze scheiding primair ten behoeve van de interne controle plaatsvindt.