COMPACT

TIJDSCHRIFT EDP-AUDITING

BEHEERSING VAN DE INFORMATIETECHNOLOGIE IN MIDDEN- EN KLEINBEDRIJF

1997/4

Compact ®
Jaargang 24, nummer 4
Een uitgave van KPMG EDP Auditors NV en Samsom Bedrijfs-Informatie, werkmaatschappij van Wolters Kluwer NV.
Het blad verschijnt 6 x per jaar.
Redactie
Prof. A.W. Neisingh RE RA (hoofdredacteur)
J.C. Boer RE RA
Ir. J.A.M. Donkers RE
Drs. R.G.A. Fijneman RE RA
J.C. van Praat RE RA
Ir.drs. J. van der Vlugt
Adviesraad
Prof.dr. J.C. Arnbak
Mr. P. van Dijken
G. van Essen RA
Prof.mr. H. Franken
Dr. K.IJ. Mollema RA
Prof. H.B. Moonen RE RA
Prof.dr.ir. R. Paans RE
Redactiesecretariaat
Mw. I. de Koning,
Samsom Bedrijfsinformatie,
Postbus 4,
2400 MA Alphen aan den Rijn
Tel.: 0172 – 466 746
Fax : 0172 – 466 569
Vormgeving
Bureau Karakter, Delft
Opmaak
Sander Pinkse Boekproduktie, Amsterdam
Abonnementen
f 165,- per jaar incl. BTW. Losse nummers f 45,- incl. BTW. Studentenabonnement f 95,- incl. BTW. Abonnementen kunnen schriftelijk tot uiterlijk één maand voor de aanvang van een nieuw abonnementsjaar worden opgezegd. Bij niet tijdige opzegging wordt het abonnement automatisch met een jaar verlengd.
Abonnementsadministratie
Samsom Bedrijfsinformatie,
Postbus 4,
2400 MA Alphen aan den Rijn
Tel.: 0172 – 466 800
Fax : 0172 – 475 933
Adreswijzigingen – ook tijdelijke – moeten minstens 8 weken voor de verschijningsdatum bekend zijn.

Uitgever
Dr. J.H. Elich

Lid van de Nederlandse organisatie van tijdschriftuitgevers NOTU

ISSN 0920 – 1645

INHOUDSOPGAVE

REDACTIONEEL

Het blad wil een bijdrage leveren aan de ontwikkeling van het vakgebied EDP-auditing door het publiceren van actuele artikelen op deelterreinen van EDP-auditing en advies, zoals: • beoordeling automatiseringsorganisaties en -systemen • risicobeheersing • telecommunicatie-adviezen • beveiligingsonderzoeken • quality assurance • opleidingen en trainingen • privacywetgeving • computercriminaliteit en nieuwe regelgeving.

Behalve voor EDP-auditors kan dit blad ook interessant zijn voor IT-deskundigen en gebruikers van informatiesystemen. De in dit tijdschrift weergegeven meningen mogen niet worden gezien als officiële zienswijze van KPMG EDP Auditors NV.

Het blad Compact is met de meeste zorg samengesteld. Niettemin is het niet geheel uitgesloten dat de geboden informatie enkel en alleen door tijdsverloop en/of andere oorzaken minder juist is. Noch KPMG, KPMG EDP Auditors, noch de redacteuren persoonlijk, noch uitgeverij Samsom BedrijfsInformatie BV, deel uitmakend van Wolters Kluwer NV, aanvaarden enige aansprakelijkheid, hoe ook genaamd, uit welken hoofde dan ook voor enig gevolg rechtstreeks of indirect voortvloeiend uit het gebruik van de informatie.

De redactie stelt gaarne ruimte in Compact beschikbaar voor reacties en/of ervaringen van lezers. Auteurs die overwegen een bijdrage te leveren, wordt verzocht kennis te nemen van de aanwijzing voor auteurs, die bij het secretariaat verkrijgbaar is.

Informatietechnologie speelt bij het besturen van ondernemingen en bij het beheersen van ondernemingsrisico's een steeds grotere rol. Uit effectiviteits- en efficiencyoverwegingen worden processen, administratieve procedures en maatregelen van interne controle in toenemende mate geautomatiseerd. Bedrijven kennen daarbij een steeds grotere afhankelijkheid van informatietechnologie. Dit geldt niet alleen voor grotere ondernemingen, maar zeker ook voor ondernemingen in het midden- en kleinbedrijf. Deze steeds grotere afhankelijkheid dwingt, ook in het midden- en kleinbedrijf, tot een adequate beheersing van de geautomatiseerde processen. Dit nummer van Compact geeft inzicht in de belangrijkste risico's in met name kleinschalige automatiseringsomgevingen en de wijze waarop beheersmaatregelen een bijdrage kunnen leveren in de beperking van deze risico's. Allereerst wordt beschreven wat kan worden verstaan onder een kleinschalige automatiseringsomgeving. De auteur geeft inzicht in verschillende kenmerken die een dergelijke omgeving typeren en meer in het bijzonder de consequenties daarvan voor beheersmaatregelen en voor taken en verantwoordelijkheden binnen de organisatie.
Niet alleen in functioneel opzicht maken geautomatiseerde systemen in het midden- en kleinbedrijf belangrijke ontwikkelingen door. Ook in technisch opzicht wordt in toenemende mate gekozen voor 'state of the art'-oplossingen. Vanwege de geboden flexibiliteit wordt niet zelden de voorkeur gegeven aan client-servertoepassingen. Dergelijke toepassingen brengen specifieke beveiligingsrisico's met zich mee die door zowel technische als organisatorische maatregelen moeten worden ondervangen. Uitgaande van een overzicht van de bedreigingen en bijbehorende beheersmaatregelen in een client-serveromgeving, gaat de auteur nader in op de beperkingen van de beheersmaatregelen en hoe de daarmee samenhangende onvolkomenheden in kleine omgevingen kunnen worden ondervangen.

Uiteraard hebben de genoemde ontwikkelingen ook consequenties voor de accountant in het kader van de controle van de jaarrekening. Bij zijn totale oordeelsvorming omtrent de wijze waarop de leiding van een onderneming belangrijke risico's beheerst, zal de accountant ook in toenemende mate belang hechten aan de wijze waarop aan de beheersing van specifieke automatiseringsrisico's inhoud wordt gegeven. Door integratie van primaire met administratieve processen reikt deze oordeelsvorming verder dan alleen een beoordeling van het administratieve systeem. Vanuit verschillend perspectief wordt daar in dit nummer van Compact aandacht aan besteed. Daarbij wordt in een algemeen kader aandacht geschonken aan de wijze waarop het management van een onderneming voldoende zekerheid heeft omtrent de beheersing van aspecten als:

1. de betrouwbaarheid van systemen;
2. de effectiviteit en efficiency van geautomatiseerde processen;
3. de naleving van wet- en regelgeving.

Onderstreept wordt dat de wijze waarop binnen de onderneming gebruik wordt gemaakt van informatietechnologie mede bepalend is voor de wijze waarop het management-controlsysteem vorm wordt gegeven. De accountant zal dat bij zijn oordeelsvorming moeten meewegen.

In het bijzonder wordt aandacht geschonken aan het proces van elektronisch bankieren, omdat daarvan, ook in het midden- en kleinbedrijf, in toenemende mate gebruik wordt gemaakt. Uitgaande van de beperkingen in omvang en functionele opzet in een kleine organisatie wordt beschreven hoe de beheersing van het elektronisch bankieren kan worden geoptimaliseerd.

Ook algemeen maatschappelijke ontwikkelingen zoals de tendens tot certificering van processen en producten, bieden het management van midden- en kleinbedrijven een handreiking om zich meer zekerheid te verschaffen omtrent de betrouwbaarheid van geautomatiseerde processen en de beveiliging van systemen en gegevens. Certificering richt zich daarbij niet alleen op een kwaliteitskeurmerk voor de functionaliteit in de vorm van softwarecertificering, maar ook op certificering van zogenaamde beveiligingssystemen: het stelsel van uniforme spelregels binnen een organisatie voor de informatiebeveiliging.

Deze Compact maakt duidelijk dat een goede samenhang tussen technische en organisatorische maatregelen het management van het midden- en kleinbedrijf voldoende zekerheid kan bieden omtrent de beheersing van geautomatiseerde processen en de beveiliging van zijn bedrijfsgegevens.

Mw. W.A. de Munck RA

Typologie van een kleinschalige automatiserings-omgeving

J.C. van Praat RE RA

Door de karakteristieken van de objecten apparatuur, systeemprogrammatuur, datacommunicatie, informatiesystemen, gegevens en mensen te analyseren en te rubriceren, wordt een overzicht gegeven van de diverse typologieën van kleinschalige automatiseringsomgevingen.

INLEIDING

Door accountants wordt een kleinschalige automatiseringsomgeving veelal gekarakteriseerd door de organisatorische aspecten centraal te stellen. Hiervan uitgaande wordt een kleinschalige automatiseringsomgeving gedefinieerd als een omgeving waar geen functiescheiding bestaat tussen de gebruikersorganisatie en de automatiseringsorganisatie, dan wel die omgeving waar binnen de automatiseringsorganisatie geen effectieve functiescheidingen bestaan. Een dergelijke definitie wordt dan uitgebreid met een aantal aanvullende karakteristieken. Voorbeelden hiervan zijn:

- beperkte automatiseringskennis bij de gebruikers;
- gebruik van standaardsoftware;
- gebruik van mini- of midrangecomputers.

Door de snelle ontwikkelingen in de informatie- en communicatietechnologie zijn dergelijke karakteristieken niet meer uitsluitend relevant. De automatiseringskennis bij gebruikers wordt groter; denk hierbij maar eens aan het gebruik van personal computers in de eigen omgeving, terwijl met name de communicatietechnologie (bijvoorbeeld Internet) het gebruik van computers sterk gestimuleerd heeft. In de moderne organisatie kan nauwelijks meer gesproken worden van computeranalfabeten. Een andere ontwikkeling is dat ook in grootschalige omgevingen steeds meer gebruik wordt gemaakt van standaardprogrammatuur. Met name wanneer het ondersteunende processen betreft is dit type programmatuur gemeengoed geworden. Ook logistieke processen worden steeds meer ondersteund door complexe en omvangrijke standaardprogrammatuur. De pakketten SAP en Baan (Triton) zijn bekende voorbeelden hiervan. Met betrekking tot de hardware zijn er eveneens ontwikkelingen waarbij naast het gebruik van minicomputers ook personal computers en servers beschikbaar komen met een vergelijkbare en soms zelfs een grotere capaciteit dan de traditionele minicomputers.

Om aan deze onduidelijkheid een einde te maken zal in dit artikel worden geprobeerd een kleinschalige automatiseringsomgeving vanuit de informatie- en communicatietechnologie (ICT) nader te definiëren. Hierbij zal worden uitgegaan van de objecten die met betrekking tot de ICT kunnen worden onderkend. Deze objecten zijn:

- mensen;
- apparatuur;
- systeemprogrammatuur;
- datacommunicatie;
- informatiesystemen;
- gegevens.

Voor al deze objecten zal hierna aangegeven worden welke componenten binnen deze objecten kunnen worden onderkend. Vervolgens zal worden aangegeven welke objecten met name in de zogenaamde kleinschalige automatiseringsomgevingen voorkomen.

DE MENSEN

Het Nederlands Genootschap voor Informatica (NGI) heeft in zijn publicatie *Taken en functies in de bestuurlijke informatica*[1] ook aandacht besteed aan de 'kleine organisatie'. Met betrekking tot de organisatie van de zogenaamde I en A-functie wordt een onderscheid gemaakt tussen de directeur die belast is met de beleidsbepaling en een medewerker van de administratie die als systeembeheerder naast zijn administratieve taak belast is met het beheer van de gegevens en de hulpmiddelen. Bovendien ondersteunt de systeembeheerder in beperkte mate de andere gebruikers.
Hoewel in de huidige situatie de hier gesuggereerde tweedeling nog steeds van toepassing is, zien we een ontwikkeling waarbij het systeembeheer zich steeds meer ontwikkelt tot een afgezonderde functie. Door het toenemende gebruik van computers in de organisatie is een afgezonderde functie al snel noodzakelijk. Ook valt op dat de directeur zelf steeds meer overlaat aan de functies die direct onder hem ressorteren. De afdelingshoofden vullen over het algemeen de formulieren van het beleid, de eisen en de wensen in. Het onderwerp informatie- en communicatietechnologie staat steeds vaker op de agenda van het periodieke overleg van het management in een organisatie.

Uit de hierboven geschetste ontwikkelingen blijkt dat het door het NGI-rapport gemaakte onderscheid tussen de directeur en de 'parttime' systeembeheerder nog steeds van toepassing is, zij het dat deze functies steeds meer ingevuld worden door het managementteam in gezamenlijk overleg, terwijl er steeds meer sprake is van een 'fulltime' systeembeheer.
Met betrekking tot de uit te voeren taken van beide functies wordt door het studierapport een goed overzicht[2] gegeven. Door de hiervoor genoemde ontwikkeling naar een fulltime systeembeheer is het echter gewenst een aantal meer operationele taken die nu aan het managementteam zijn toegewezen over te hevelen naar de systeembeheerder. Om dit te verduidelijken worden in figuur 1 de in het studierapport genoemde taken verdeeld over het managementteam en de systeembeheerder.

Met betrekking tot het systeembeheer zelf wordt een aantal taken gedefinieerd die verdeeld kunnen worden in de volgende aandachtsgebieden:
- ondersteuning gebruikers;
- beheer applicaties;
- beheer technische infrastructuur.

Op basis van deze indeling komen we tot de volgende taken:

Ondersteuning gebruikers

- Behandelen van vragen over of problemen met het exploitatieproces en de decentrale computer- en netwerkfaciliteiten. Zo nodig inschakelen van derden en coördineren van de uitvoering.

- Begeleiden van het persoonlijk computergebruik. Geven van training. Oplossen van problemen met applicaties en apparatuur.

Beheer applicaties

- Toetsen van het functioneren van het informatiesysteem aan de specificaties en verwachtingen van gebruikers, beheerder en exploitatiepersoneel. Voorstellen van wijzigingen in het informatiesysteem.

- Aanpassen van applicaties aan de door de organisatie gewenste situatie, met behulp van parameters. Installeren van parameters om de gewenste aanpassingen voor de verwerking te realiseren.

- Converteren en invoeren van bestaande gegevens en beoordelen van de resultaten.

- Programmeren van ad-hoctoepassingen voor de selectie, bewerking en presentatie van de gevraagde informatie. Uitvoeren van de ad-hoctoepassing en de resultaten ter beschikking stellen aan het managementteam.

- Zorgdragen voor de integriteit, de volledigheid en het geautoriseerd gebruik van geautomatiseerde gegevensverzamelingen en het toezien op de goede werking van de informatiesystemen.

- Controleren van de naleving van procedures voor beveiliging, autorisatie en gebruik. Hierbij behoort het voeren van een autorisatieadministratie en het toetsen van de autorisatieaanvragen aan gestelde eisen.

- Uitvoeren van het versiebeheer. Distribueren en beschikbaar stellen van de applicaties en gerelateerde documentatie.

Beheer technische infrastructuur

- Analyseren van de belasting van de technische infrastructuur en vaststellen van de wenselijke capaciteitsaanpassing aan de hand van de gebruikersprognose. Opstellen van het plan om de gewenste aanpassingen te kunnen realiseren, rekening houdend met de gewenste servicegraad.

- Zorgdragen dat de technische infrastructuur voor gegevensverwerking, gegevenspresentatie, gegevensopslag en gegevenstransport (netwerk) in functioneel, technisch en operationeel opzicht blijven voldoen aan de gestelde eisen.

- Analyseren van complexe storingen in het computersysteem. Verhelpen van de storingen, eventueel in overleg met de leveranciers van hardware en systeemsoftware. Maatregelen treffen ter voorkoming van storingen.

Gevolgen voor de kleinschalige automatiseringsomgeving

Om in een kleinschalige automatiseringsomgeving het systeembeheer adequaat te kunnen beheren is het belangrijk de nodige aandacht te besteden aan de scheiding tussen het systeembeheer en het management. Hoewel in het studierapport *Taken en functies in de bestuurlijke informatica* de nodige taken zijn weggelegd voor het management, mag van het systeembeheer meer ondersteuning worden ver-

1. Taken en functies in de bestuurlijke informatica, blz. 55 e.v.
2. Taken en functies in de bestuurlijke informatica, blz. 57.

Managementteam	Systeembeheerder
Definiëren van de taken, functies en de organisatiestructuur voor het plannen, ontwikkelen, beheren en exploiteren van de informatievoorziening. Onderhouden van het resultaat.	
Definiëren van doelstellingen, uitgangspunten en randvoorwaarden voor de informatievoorziening en automatisering, afgestemd op het bedrijfsbeleid.	Beheren van doelstellingen, uitgangspunten en randvoorwaarden voor de informatievoorziening en automatisering, afgestemd op het bedrijfsbeleid.
Op basis van de knelpunten, beleidslijnen en eisen formuleren van criteria voor de gewenste informatievoorziening.	Uitdiepen van door de gebruikersorganisatie aangegeven knelpunten, beleidslijnen en eisen.
Afleiden van organisatorische randvoorwaarden en toetsingscriteria voor de te kiezen oplossing.	Vaststellen van het veranderingsvermogen van de organisatie in relatie tot veranderingen in de informatievoorzieningen.
	Ontwikkelen van alternatieven om de gewenste situatie in de informatievoorziening te bereiken. Aanbevelingen dienen rekening te houden met beslissingscriteria.
Vaststellen van de eisen die aan de gewenste situatie worden gesteld.	Inventariseren, analyseren en afstemmen van de gewenste informatievoorziening in relatie met de gewenste bedrijfsvoering. Vaststellen van beperkingen, randvoorwaarden en uitgangspunten. Beschrijven van de eisen die aan de gewenste situatie worden gesteld.
Formuleren van de uitgangspunten die voor de invoering van de nieuwe informatievoorziening zullen worden gehanteerd.	Opstellen van een plan om in stappen te migreren van de huidige naar de toekomstige situatie van de gebruikersorganisatie. Opstellen van een plan om de nieuwe informatievoorziening te implementeren op de technische infrastructuur.
	Definiëren van projecten ten behoeve van ontwikkeling of aanpassing van gegevensverzamelingen, informatiesystemen en technische infrastructuur. Vaststellen van de samenhang tussen de projecten. Inventariseren van de eventuele conditionerende maatregelen. Inschatten van de per project benodigde tijd, mensen en middelen. Faseren van de projecten in de tijd.
Keuzen maken.	Onderzoeken van de in de markt beschikbare componenten van de technische infrastructuur. Toetsen daarvan aan de gestelde eisen en randvoorwaarden.
Kiezen van een applicatiepakket.	Onderzoeken van de in de markt beschikbare applicatiepakketten. Toetsen en zo nodig aanvullen van de eisen en wensen die worden gesteld aan de functionaliteit en de technische aspecten van de applicatiepakketten.
Periodiek uitvoeren van een evaluatie van het informatiesysteem wat betreft de technische normen en eisen, de onderhoudbaarheid, de technische betrouwbaarheid en de continuïteit.	Opstellen van een plan voor preventief en correctief onderhoud.
Controleren, verifiëren en valideren van resultaten van het ontwikkelings-, onderhouds- en exploitatieproces.	Beoordelen van de aspecten correctheid, (interne) consistentie en het voldoen aan vooraf vastgestelde normen en richtlijnen, eisen, uitgangspunten en randvoorwaarden.

Figuur 1. Taakverdeling managementteam en systeembeheerder volgens NGI.

wacht. Wanneer deze ondersteuning daadwerkelijk inhoud krijgt zal blijken dat er al snel sprake is van een afzonderlijke functie (dus een gescheiden) systeembeheer. Omdat er dan sprake is van functiescheiding tussen de gebruikersorganisatie en de automatiseringsorganisatie (systeembeheer) is een betrouwbare gegevensverwerking beter gewaarborgd. De gebruikersorganisatie (met name het management) dient echter wel aandacht te besteden aan het functioneren van het systeembeheer. Een periodieke verantwoording door het systeembeheer, die met de nodige zorgvuldigheid door het management wordt beoordeeld, is in dit verband van groot belang.

APPARATUUR

In deze paragraaf staan de computerplatformen centraal. Met betrekking tot de computerplatformen kan de indeling worden gebruikt die al vele jaren wordt gehanteerd en nog steeds van toepassing is. Het gaat hierbij om het onderscheid tussen:

- personal computers;
- mini/midrangesystemen;
- mainframecomputers;
- supercomputers.

Nadat de supercomputer in het recente verleden alleen werd gebruikt in zeer specifieke situaties (met name de wetenschappelijke wereld), wordt deze computer momenteel steeds meer gebruikt in de commerciële omgeving. Kenmerkend voor de supercomputer is dat hij gebruikmaakt van zogenaamde Massively Parallel Processors (MPPs). In de mainframewereld hebben zich echter eveneens ontwikkelingen voorgedaan die ervoor gezorgd hebben dat ook deze systemen nog steeds in de belangstelling staan. Om de capaciteit te verbeteren en ook de kosten van mainframes te verlagen, wordt gebruikgemaakt van Complementary Oxide Semiconductor (CMOS) integrated circuits. Daarnaast zien we dat ook in mainframesystemen steeds meer microprocessors worden toegepast.

Met het noemen van de microprocessors zijn we terechtgekomen in de platformen die met name in de kleinschalige automatiseringsomgeving worden gebruikt: de personal computer en de mini/midrangesystemen.

Personal Computers

Met name de ontwikkelingen met betrekking tot de microprocessors hebben gezorgd voor de grote populariteit van de personal computer. Deze computers hebben momenteel een verwerkingskracht die vergelijkbaar is met de verwerkingskracht van het mainframe van nog niet zo lang geleden. Een grotere verwerkingskracht is nodig om te kunnen voldoen aan de toenemende behoeften van de gebruikers van dergelijke systemen. De ontwikkeling van de grafische gebruikersinterface eist veel van de computer. Bovendien wordt de PC steeds meer gebruikt in netwerktoepassingen. Met name de netwerkcomputer, als laatste zeer recente ontwikkeling, staat momenteel sterk in de belangstelling. Behalve aan deze netwerkcomputer besteden we hierna ook nog aandacht aan de PC-servers en de workstations.

PC-servers
Binnen de groep van de personal computers nemen de zogenaamde PC-servers een bijzondere plaats in. In feite gaat het hier om zeer krachtige PC's, waarmee het mogelijk is de rol van de centrale computer (oorspronkelijk het mainframe) in een netwerkomgeving over te nemen. PC-servers maken vaak gebruik van meerdere processors, terwijl voorzieningen aanwezig zijn voor de zeer omvangrijke opslag van gegevens.
PC-servers beschikken over een aantal extra faciliteiten die sterk kwaliteitsverhogend zijn. Deze faciliteiten zijn[3]:

- Redundant Array of Inexpensive Disks (RAID). De RAID-technologie maakt het mogelijk de beschikbaarheid van de opgeslagen gegevens te vergroten zonder dat dit leidt tot een extra (dubbele) opslag van gegevens. Bovendien bevordert deze technologie een snellere gegevensverwerking.

- Hot-swappable disks. Dit zijn schijven die vervangen kunnen worden zonder dat de beschikbaarheid van de server in gevaar komt. Bij het vervangen van schijven is het niet nodig om het computersysteem af te zetten.

- Error-correcting Memory (ECC). Hoewel gebruikelijk in de mini- en mainframewereld wordt het ook in de PC-wereld mogelijk geheugenfouten automatisch te herstellen.

Uit deze ontwikkelingen blijkt naast een steeds grotere capaciteit ook de beschikbaarheid van de computersystemen van steeds groter belang te worden. Hiermee zien we dat tegen relatief lage kosten toch betrouwbare computersystemen beschikbaar komen die het gebruik van de traditionele mini/midrangesystemen sterk bedreigen. Omdat kleinschalige automatiseringsomgevingen steeds meer gebruik gaan maken van PC-servers, zien we dat de kwaliteit van de gegevensverwerking (met name de beschikbaarheid) sterk wordt verbeterd.

Workstations
Binnen de wereld van de personal computer neemt het zogenaamde workstation een bijzondere plaats in. Hoewel ze in het verleden naast de PC werden genoemd, beschikken de workstations tegenwoordig steeds meer over de faciliteiten die vergelijkbaar zijn met die van de PC.
Kenmerkend voor deze systemen is dat ze behalve een grote verwerkingskracht ook de mogelijkheid hebben gebruik te maken van het besturingssysteem Unix. Vanwege hun grote verwerkingskracht worden ze veel gebruikt in de technische wereld (CAD/CAM-toepassingen). Naast hun verwerkingskracht is ook de beschikbaarheid van netwerkfaciliteiten een sterk punt. Daarom worden de workstations steeds meer gebruikt als server in een PC-netwerk, en krijgen ze het karakter van een mini/midrangesysteem.

Netwerkcomputers
Kenmerkend voor de netwerkcomputer is dat ze gebruikmaken van het 'netwerk' waarin de gegevens en de applicaties zijn opgenomen. Men spreekt in dit verband ook wel van network computing. Op deze ontwikkeling speelt een bekende reclame-uiting[4] 'The computer is the network' handig in. Voor de netwerkcomputer betekent dit dat de vaste schijf en ook de floppy drive c.q. cd-romdrive verdwijnen. Het zal duidelijk zijn dat deze ontwikkeling vooral de betrouwbaarheid van de gegevensverwerking sterk bevordert[5]. Door gebruik te maken van netwerkcomputers is de systeembeheerder in staat de gegevensverwerking aanzienlijk beter te beheersen. Met name de risico's die voortvloeien uit het gebruik van de PC[6] worden hierdoor sterk beperkt.

Mini/midrangesystemen

De minicomputer neemt een geheel eigen plaats in. Momenteel zijn de functies van minicomputers vergelijkbaar met die van de hiervoor genoemde PC-servers. Wel is opvallend dat het over het algemeen gesloten systemen betreft. De bekendste voorbeelden van dergelijke systemen zijn de AS/400- en de VAX-systemen van Digital. Door hun geslotenheid zien we de ontwikkeling dat deze traditionele mini/midrangesystemen steeds meer worden vervangen door de hiervoor genoemde PC-servers.

3. Technology Forecast 1996, Price Waterhouse, blz. 111.
4. Sun Micro-systems gebruikt deze uiting in haar radioreclames.
5. Zie ook het artikel 'Een PC-netwerk voor beheersing van de personal computer' van Jan van Praat in de bundel Update on EDP & Accountancy, Samsom Bedrijfs-Informatie 1993.
6. Zie ook het NIVRA-studierapport Beheersing van de Micro, NIVRA 1991.

Gevolgen voor de kleinschalige automatiseringsomgeving

In deze paragraaf is aangegeven dat er meer en meer sprake is van een verschuiving van de traditionele mini/midrangesystemen naar de personal computer in al zijn verschijningsvormen. Met name de ontwikkelingen met betrekking tot de PC-servers en de netwerkcomputers zijn hierbij van belang. Gegeven het feit dat de kwaliteit van de PC-servers steeds beter wordt, is deze ontwikkeling, zeker wanneer steeds meer gebruik wordt gemaakt van netwerkcomputers, uit beheersingsoogpunt een positieve ontwikkeling. In feite zorgt de netwerkcomputer ervoor dat er weer sprake is van een toegenomen gecentraliseerd beheer van de gegevensverwerking.

SYSTEEMPROGRAMMATUUR

De hiervoor besproken apparatuur kan pas functioneren wanneer gebruik wordt gemaakt van programmatuur. Ten aanzien van de programmatuur kan een onderscheid worden gemaakt tussen toepassingsprogrammatuur en besturingsprogrammatuur. Het onderscheid tussen beide groepen heeft te maken met de functie van de programmatuur. De toepassingsprogrammatuur richt zich primair op de gebruiker. Dit betekent in de praktijk dat de gebruiker direct te maken heeft met toepassingsprogrammatuur. De besturingsprogrammatuur verzorgt vervolgens de koppeling tussen de apparatuur en de toepassingsprogrammatuur. In feite zorgt de besturingsprogrammatuur ervoor dat de toepassingsprogrammatuur goed kan functioneren.

Functies van de besturingsprogrammatuur

In de *Technology Forecast* van Price Waterhouse[7] worden met betrekking tot de besturingsprogrammatuur de volgende functies gedefinieerd:
- processorbeheer (process management);
- geheugenbeheer (memory management);
- in- en uitvoerbeheer (input/output);
- opslagbeheer (file system).

Bij het processorbeheer staat het toewijzen van uit te voeren processen (ook wel taken genoemd) aan de processor centraal. Op basis van bepaalde criteria stelt het besturingssysteem vast welke toepassing op een zeker moment gebruik mag maken van een processor. Ten aanzien van de vormen van beheer kan een onderscheid worden gemaakt tussen:
- multitasking: het beheer van meerdere processen tegelijkertijd;
- multithreading: het beheer van meerdere onderdelen (modules) van een toepassing;
- multiprocessing: het beheer van meerdere processors.

Het geheugenbeheer richt zich op het beheer van zowel het interne geheugen als het externe geheugen. Omdat het interne geheugen een beperkte capaciteit heeft, zal gekozen moeten worden welke onderdelen wel en welke onderdelen niet in het interne geheugen opgeslagen zullen worden.

De functie in- en uitvoerbeheer zorgt voor het transport van data (gegevens en programmatuur) van en naar de diverse componenten van een computersysteem (geheugens, beeldschermen, toetsenborden, etc.).

De functie opslagbeheer richt zich primair op de opslag van gegevens op de externe geheugens. Veelal wordt hierbij gebruikgemaakt van tabellen waarin aangegeven is op welke fysieke plaats bepaalde gegevens zich bevinden.

Dankzij de netwerkcomputer is er in feite weer sprake van een toegenomen gecentraliseerd beheer van de gegevensverwerking.

Naast deze basisfuncties vervullen besturingssystemen steeds meer additionele functies die voor het beheer van computersystemen van groot belang zijn. Voorbeelden van deze additionele functies zijn:
- beveiligingsbeheer;
- netwerkbeheer;
- gegevensbeheer.

Het beveiligingsbeheer maakt het mogelijk de toegang tot data adequaat te beheren. Hierbij zijn faciliteiten aanwezig met betrekking tot identificatie, authenticatie, autorisatie en verslaglegging. Het netwerkbeheer maakt het mogelijk de koppeling tussen verschillende op afstand met elkaar verbonden apparatuur te beheren. Hierdoor is het mogelijk een fysieke scheiding te realiseren tussen de plaats waar de gegevens worden ingevoerd c.q. uitgevoerd en de plaats waar de gegevens worden verwerkt. Het gegevensbeheer richt zich op het beheren van in computersystemen opgeslagen gegevens.

Om al deze functies te kunnen vervullen kan ten aanzien van de besturingsprogrammatuur een onderscheid worden gemaakt tussen:
- desktop-besturingssystemen;
- multi-user-besturingssystemen;
- netwerkbesturingssystemen.

Desktop-besturingssystemen

Zoals de naam al zegt draaien desktop-besturingssystemen op personal computers. Bekende voorbeelden hiervan zijn Ms-Dos, Windows 3.11, Windows95 en het besturingssysteem voor de Apple Macintosh. Kenmerkend voor deze besturingssystemen is dat ze gericht zijn op de individuele gebruiker (single-user). Vanwege het single-userkarakter zijn in de meeste gevallen alleen de oorspronkelijke functies van besturingssystemen aanwezig. Dit betekent dat alleen het geheugenbeheer, het in- en uitvoerbeheer en het opslagbeheer goed geregeld zijn.

7. *Technology Forecast 1996, Price Waterhouse, blz. 224 e.v.*

Dit houdt tevens in dat een aantal functies voor desktop-besturingssystemen niet of slechts zeer beperkt gebruikt wordt. Zo is de beveiliging van deze besturingssystemen zeer beperkt, terwijl ook de mogelijkheden voor gegevensbeheer niet of nauwelijks aanwezig zijn. De nieuwe besturingssystemen bieden in beperkte mate mogelijkheden voor multitasking, hoewel in de praktijk blijkt dat een dergelijke wijze van werken sterk ten koste gaat van de verwerkingssnelheid.
Een belangrijk aspect dat de moderne desktop-besturingssystemen in navolging van de Apple Macintosh wel hebben, is de grafische gebruikersinterface (Graphical User Interface, GUI).

Multi-user-besturingssystemen

Uit de naamgeving blijkt al het kenmerkende verschil met de desktop-besturingssystemen. Multi-user-besturingssystemen maken het mogelijk dat meerdere gebruikers gezamenlijk gebruikmaken van een computer. Het besturingssysteem draait hierbij volledig op de centrale computer, hetgeen betekent dat in principe volstaan kan worden met het gebruik van zogenaamde 'domme' (niet-intelligente) terminals. In de huidige praktijk zien we echter dat steeds meer gebruik wordt gemaakt van de personal computer als werkstation. In voorkomende gevallen is het dan noodzakelijk om gebruik te maken van terminalemulatie, waardoor het voor het multi-user-besturingssysteem lijkt dat er sprake is van een domme terminal die direct aangestuurd wordt door het besturingssysteem op de centrale computer.

In de kleinschalige automatiseringsomgeving is de combinatie van netwerk- en desktop-besturingssysteem populair.

De eerdergenoemde functies worden feitelijk allemaal uitgevoerd door multi-user-besturingssystemen. Het gegevensbeheer, het beveiligingsbeheer en multithreading behoren dan ook tot de standaardfaciliteiten van deze besturingssystemen. Multiprocessing is niet in alle gevallen mogelijk, doch geleidelijk wordt deze functie steeds meer gebruikt.
De bekendste voorbeelden van multi-user-besturingssystemen zijn Unix, MVS, OS/400 en OpenVMS. Hoewel deze besturingssystemen alle functies van een besturingssysteem vervullen, moet wel worden opgemerkt dat de basisversie van het besturingssysteem niet altijd de functies volledig invult. In de praktijk betekent dit dat vaak aanvullende besturingsprogrammatuur moet worden aangeschaft om een bepaalde functie beter te kunnen invullen.

Netwerkbesturingssystemen

De netwerkbesturingssystemen zijn de laatste jaren sterk in de belangstelling gekomen. Met de komst van de lokale PC-netwerken was er behoefte aan besturingssystemen die een dergelijk netwerk konden besturen. Hierbij werd in eerste instantie gebruikgemaakt van de besturingssystemen die al op de personal computer aanwezig waren, zoals Ms-Dos. Op de 'centrale' PC werd dan gebruikgemaakt van het netwerkbesturingssysteem, overigens zonder gebruik te maken van een desktop-besturingssysteem. Het bekendste voorbeeld van een dergelijk netwerkbesturingssysteem is Netware van Novell. Recent is daar WINDOWS/NT bij gekomen.

Netwerkbesturingssystemen beschikken over twee belangrijke faciliteiten:
- ze zorgen ervoor dat het netwerk adequaat functioneert. In feite betreft het de standaardfuncties van een besturingssysteem;
- ze zorgen voor mogelijkheden om het netwerk te kunnen beheren (netwerkbeheer).

Wanneer we de standaardfuncties van een netwerkbesturingssysteem vergelijken met de functies van een multi-user-besturingssysteem, dan blijken deze in belangrijke mate vergelijkbaar te zijn. Het grootste verschil betreft de functies met betrekking tot het gegevensbeheer. Juist bij netwerkbesturingssystemem zien we dat zich hier de afzonderlijke databasemanagementsystemen hebben ontwikkeld.

Ten behoeve van het beheer van netwerken kan de functie netwerkbeheer nader worden geconcretiseerd in de volgende subfuncties[8]:
- het uitwisselen van managementinformatie tussen de netwerkomgeving en de managementomgeving;
- het converteren van managementinformatie vanuit verschillende formaten waardoor een consistent formaat ontstaat;
- het transporteren van managementinformatie tussen de verschillende locaties in de managementomgeving;
- het gebruiken van managementinformatie in een zodanige vorm dat zij betekenisvol is voor de gebruikers van deze informatie;
- het presenteren van de managementinformatie aan de gebruikers ervan;
- het beveiligen van de managementinformatie waardoor alleen geautoriseerde gebruikers de informatie kunnen verkrijgen.

Op het netwerkbeheer komen we in de volgende paragraaf onder 'Local Area Networks' terug.

Gevolgen voor de kleinschalige automatiseringsomgeving

In een kleinschalige automatiseringsomgeving zien we steeds vaker de combinatie van het gebruik van netwerkbesturingssystemen en van de desktop-besturingssystemen. Hierbij bestuurt het netwerkbesturingssysteem het lokale PC-netwerk (Local Area Network). Met name de mogelijkheden met betrekking tot het beheren van de gehele technische infrastructuur dragen in sterke mate bij tot het adequaat functioneren van de technische infrastructuur in een kleinschalige automatiseringsomgeving.

8. R.S. Cohen, The Telecommunications Management Network, blz. 225.

DATACOMMUNICATIE

Met betrekking tot de datacommunicatie doen zich momenteel sterke ontwikkelingen voor binnen de wereld van zowel de Local Area Networks (LAN) als de Wide Area Networks (WAN).

Ten aanzien van de Wide Area Netwerken kan in dit kader worden gerefereerd aan een aantal moderne ontwikkelingen die het mogelijk maken dat ook kleinschalige automatiseringsomgevingen hiervan gebruik maken. Voorbeelden van deze ontwikkelingen zijn:

- Het toenemende gebruik van ISDN (Integrated Services Digital Network) waardoor een relatief snel transport ontstaat. Met de opkomst van ISDN staat ook videotelefonie c.q. video-conferencing steeds meer in de belangstelling.

- Het toenemende gebruik van mobiele communicatie, die steeds betere beveiligingsmogelijkheden biedt. Deze ontwikkeling draagt in sterke mate bij tot de flexibilisering van de arbeid (thuiswerken, overal bereikbaar zijn).

Omdat het hier gaat om ontwikkelingen die een afzonderlijke behandeling vragen, terwijl deze faciliteiten gebruikt kunnen worden in zowel een kleinschalige als een grootschalige automatiseringsomgeving, wordt er in dit artikel verder geen aandacht aan besteed.

Local Area Networks

Kenmerkend voor een Local Area Network (LAN) is dat het gebruikt wordt in een beperkte ruimte. Vaak beperkt een LAN zich tot een gebouw. Een bijzonder kenmerk van een LAN is dat meestal gebruik wordt gemaakt van personal computers als werkstations. Naast de toegenomen 'intelligentie' op de werkplek zien we dat ook in het netwerk zelf steeds meer 'intelligente' apparatuur en programmatuur wordt opgenomen. Voorbeelden hiervan zijn de bridges[9], routers[10], hubs[11] en gateways[12].
Een belangrijk aspect dat in dit artikel wat verder wordt uitgewerkt, betreft de managementfuncties die in LAN's steeds vaker voorkomen. Omdat het LAN meer en meer de kenmerken van een zenuwstelsel gaat krijgen, is een goed beheer absoluut noodzakelijk. Om dit mogelijk te maken heeft de International Standardization Organization (ISO) naast het bekende OSI-model ook het OSI Management Framework ontwikkeld. Hierbij wordt het netwerkmanagement opgesplitst in vijf onderdelen:

- Configuration management. Hierdoor is het mogelijk op afstand het gehele netwerk te beheren. Het gaat hier om het beheren van de 'netwerkvoorraad' (apparatuur, programmatuur, bekabeling en protocollen).

- Fault management. Hiermee is het mogelijk fouten te lokaliseren en oplossingen voor deze fouten te vinden.

- Performance management. In dit kader wordt voortdurend de performance van het netwerk gemeten. Het systeem geeft signalen wanneer de vooraf afgesproken performance in gevaar komt.

- Account management. Binnen deze functie worden de kosten van het netwerk doorberekend aan de gebruikers.

- Security management. Deze functie zorgt voor een adequate toegang tot de netwerkbronnen.

Om aan het netwerkmanagement inhoud te kunnen geven kan in de kleinere netwerken worden volstaan met de basisfunctionaliteiten van het netwerkbesturingssysteem zoals we dat hiervoor al besproken hebben. Wanneer het netwerk echter groter wordt, dan heeft het de voorkeur gebruik te maken van professionele op het netwerkmanagement afgestemde softwareproducten. Bekende voorbeelden hiervan zijn:
- Sun Netmanager (Sun);
- HP OpenView (Hewlett Packard);
- Netview (IBM);
- Spectrum (Cabletron);
- OmniGuard/ESM (Axent).

De netwerkbeheerder beschikt voor zijn taak over steeds meer en betere hulpmiddelen.

Een bijzondere ontwikkeling in het kader van netwerkmanagement heeft betrekking op de protocollen die worden gebruikt om de managementfuncties goed te kunnen uitvoeren. Veruit het bekendste protocol is het Simple Network Management Protocol (SNMP). Hiermee kan men alle gegevens die nodig zijn om inhoud te kunnen geven aan het OSI Management Framework beschikbaar krijgen op een centraal werkstation, het zogenaamde Network Management Station. Alle intelligente componenten beschikken over aanvullende software om de benodigde gegevens te verzamelen. SNMP noemt dit de SNMP agents. Deze gegevens worden door de SNMP agents vastgelegd in de Management Information Base (MIB). Het SNMP-protocol zorgt ervoor dat de gegevens uitgewisseld kunnen worden tussen de netwerkcomponenten. Ten slotte zorgt de managementsoftware ervoor dat de resultaten gepresenteerd kunnen worden aan de gebruiker, doorgaans de netwerkbeheerder. Hiertoe beschikt de software meestal over een grafische gebruikersinterface.

In de toekomst zullen de mogelijkheden om het netwerk te kunnen beheren alleen maar beter worden. Zo zijn recentelijk de beveiligingsmogelijkheden van SNMP aanzienlijk verbeterd. Verder neemt ook de snelheid van de netwerken flink toe. In dit verband kan worden gewezen op het toenemende gebruik van glasvezelbekabeling, terwijl ATM (Asynchronous Transfer Mode) ervoor zorgt dat ook video steeds beter mogelijk wordt.

9. Bridges maken het mogelijk twee verschillende netwerken (bijvoorbeeld ethernet en token ring) aan elkaar te koppelen, waarmee voor de gebruiker één netwerk ontstaat.
10. Routers kennen de netwerktopologie en kunnen vervolgens het beste pad kiezen in dat netwerk.
11. Een hub (geen afkorting) beschikt naast de routerfaciliteiten ook over zogenaamde managementfuncties waardoor de netwerk- (of systeem-) beheerder het netwerkverkeer beter kan bekijken.
12. Een gateway zorgt ervoor dat netwerken met verschillende protocollen met elkaar kunnen communiceren.

Gevolgen voor de kleinschalige automatiseringsomgeving

Uit het voorgaande blijkt dat het beheer van netwerken steeds beter inhoud kan worden gegeven. De netwerkbeheerder beschikt daartoe over steeds meer en betere hulpmiddelen. Een goed netwerkmanagement is dan ook een absolute vereiste. Hierbij zijn duidelijke afspraken nodig tussen de gebruikersorganisatie en het netwerkbeheer (automatiseringsorganisatie). Dit alles betekent dat ook in een kleinschalige automatiseringsomgeving steeds meer mogelijkheden aanwezig zijn om het netwerk te kunnen beheersen.

INFORMATIESYSTEMEN

Met betrekking tot de informatiesystemen kan een onderscheid worden gemaakt tussen:
- bedrijfsbrede toepassingen;
- transactieverwerkende toepassingen;
- informatieverstrekkende toepassingen;
- kantoortoepassingen;
- persoonlijke toepassingen.

Kenmerkend voor de bedrijfsbrede toepassingen[13] is dat ze de mogelijkheid hebben om vrijwel het gehele bedrijfsgebeuren met een enkele toepassing te ondersteunen. Bekende voorbeelden hiervan zijn de pakketten SAP en Triton (Baan). Hoewel deze pakketten begonnen zijn met de ondersteuning van de financiële functie richten ze zich steeds meer op de logistieke processen in een organisatie. Richtten deze systemen zich primair op grootschalige omgevingen[14], momenteel is een tendens waarneembaar dat men zich meer en meer op de kleinschalige automatiseringsomgevingen gaat richten. Een zeer recent voorbeeld is SAP. Deze organisatie heeft voor de R/3-versie (client-serverversie) de Accelarated SAP (ASAP[15]) methode ontwikkeld. Hierdoor kan het configureren van de processen met een factor 10 worden versneld, waardoor het ook voor kleinschalige omgevingen efficiënt kan zijn gebruik te gaan maken van dergelijke pakketten. Ook Baan heeft een soortgelijk hulpmiddel beschikbaar: Dynamic Enterprise Modeller (DEM). Het parametriseren van dergelijke pakketten blijft echter een belangrijk aandachtspunt voor de systeembeheerder. In de hiervoor genoemde beschrijving van de taken wordt dit aspect ook uitdrukkelijk genoemd.

Een transactieverwerkende toepassing zorgt ervoor dat een transactie (een reeks van handelingen die als een geheel worden gezien) in een onderlinge verwevenheid wordt uitgevoerd[16]. In feite wordt een gestructureerd minibesluitvormingsproces doorlopen. Zo kan het voorkomen dat de verkoop van een pakje sigaretten aan de kassa van een supermarkt leidt tot het doen van een bestelling bij de leverancier van het betreffende merk om een nieuwe levering te doen. Transactieverwerkende toepassingen richten zich, in tegenstelling tot de bedrijfsbrede toepassingen, meestal op een beperkt deel van het bedrijfsproces. Meestal wordt een enkel bedrijfsproces ondersteund, en vallen andere bedrijfsprocessen buiten die ondersteuning. In het hiervoor genoemde voorbeeld zal de desbetreffende toepassing geen mogelijkheden hebben om bijvoorbeeld salarissen te verwerken.

Informatieverstrekkende toepassingen (men spreekt in dit verband ook wel van beslissingsondersteunende systemen ofwel Decision Support Systems) behoeven slechts in zeer beperkte mate ontworpen te worden. Met deze systemen is het mogelijk zowel de gestructureerde als de ongestructureerde problemen aan te pakken. Met name als in de organisatie aan de voorwaarde van een goede gegevensarchitectuur is voldaan, kan een gebruiker op relatief eenvoudige wijze informatie verkrijgen ter ondersteuning van de besluitvorming. Hierbij kan een informatieverstrekkende toepassing in alle fasen van de besluitvorming een rol spelen. Het gaat hierbij zowel om de opsporingsfase, de ontwerpfase als de keuzefase[17]. Ook in kleinschalige automatiseringsomgevingen worden dergelijke hulpmiddelen steeds meer gebruikt. Om zulke toepassingen goed te kunnen gebruiken moeten de gebruikers op de hoogte zijn van de mogelijkheden en onmogelijkheden. Belangrijk is in ieder geval om te weten dat alleen die informatie te verkrijgen is waarvoor de basisgegevens ook daadwerkelijk in het systeem vastgelegd zijn.

Kantoortoepassingen missen over het algemeen de complexiteit van de bedrijfsbrede toepassingen en de transactieverwerkende toepassingen. Deze toepassingen bestaan uit een heterogene verzameling van standaardpakketten, maatwerkprogrammatuur en geautomatiseerde en niet-geautomatiseerde activiteiten. Goede voorbeelden van dergelijke toepassingen zijn:
- tekstverwerkers;
- spreadsheets;
- agendasystemen;
- electronic mail.

Met name de verdere verspreiding van de personal computer (al of niet opgenomen in een netwerk) heeft ervoor gezorgd dat vrijwel iedere gebruiker in een organisatie (van hoog tot laag) dagelijks van deze hulpmiddelen gebruikmaakt, ook in de kleinschalige omgevingen.
In het verlengde van de kantoortoepassingen liggen de persoonlijke toepassingen. Deze toepassingen worden meestal afgedekt door gebruik te maken van een standaardpakket of door eindgebruikersontwikkeling (end user computing), waarbij de gebruiker meestal weinig aandacht schenkt aan de vaak relatief hoge exploitatiekosten, de flexibiliteit en de kwaliteit.

Gevolgen voor de kleinschalige automatiseringsomgeving

Uit de hiervoor genoemde ontwikkelingen met betrekking tot de informatiesystemen blijkt dat in kleinschalige omgevingen steeds meer gebruik wordt gemaakt van standaardprogrammatuur. Dit laatste geldt niet alleen voor de ondersteunende processen; ook de primaire en logistieke processen worden steeds meer ondersteund door standaardprogrammatuur.
Kenmerkend voor deze standaardprogrammatuur

13. Men spreekt ook wel van Enterprise Resource Planning (ERP)-systemen.
14. Een goed voorbeeld is SAP R/2 dat functioneert op mainframesystemen.
15. Dit hulpmiddel configureert de toepassing door de klant relatief eenvoudige keuzen te laten maken. Hierbij is een zogenaamde Engineer beschikbaar die de duizend bedrijfsprocessen van R/3 overzichtelijk indeelt. Door deze aanpak wordt tachtig procent van het systeem opgezet.
16. Bestuurlijke Informatiekunde van Bots, Van Heck, Van Swede en Simons, Cap Gemini Publishing, 1990, blz. 130 e.v.
17. Deze fasen zijn genoemd in het boek Bestuurlijke Informatiekunde van Bots, Van Heck, Van Swede en Simons, Cap Gemini Publishing, 1990, blz. 132.

is dat vanwege hun grote flexibiliteit er veel aandacht besteed moet worden aan de juiste inrichting van dergelijke pakketten. Hiervoor is een diepgaande kennis van dergelijke pakketten bij de beheerder van groot belang. Dit is een reden temeer om veel aandacht te schenken aan de organisatie van het systeembeheer. Vanwege de relatief grote afhankelijkheid van het systeembeheer dient het management veel zorg te besteden aan de bewaking van de activiteiten van het systeembeheer. Een tweede kenmerk van standaardprogrammatuur is dat deze programmatuur steeds betrouwbaarder functioneert. Er wordt veel aandacht besteed aan de geprogrammeerde controles en dat geldt evenzeer voor de blijvende integriteit.
Concluderend kunnen we dan ook stellen dat een eenmaal goed ingericht standaardpakket kan zorgen voor een integere gegevensverwerking. Belangrijk is wel dat veel aandacht wordt geschonken aan de organisatie van het systeembeheer, waarbij de activiteiten van de systeembeheerder bewaakt zullen moeten worden door het management.

GEGEVENS

Hoewel de gegevens zelf geen onderwerp zijn van dit artikel, zijn de hulpmiddelen die zich richten op het beheer van de gegevens wel van belang. Het betreft hier de databasemanagementsystemen die ook in kleinschalige automatiseringsomgevingen steeds meer gebruikt worden. Met name het fenomeen Client/Server heeft hiervoor gezorgd.

Traditioneel worden drie groepen databasemanagementsystemen onderscheiden[18]:
- hiërarchische DBMS'n;
- netwerk-DBMS'n;
- relationele DBMS'n.

Omdat in kleinschalige omgevingen vrijwel uitsluitend gebruik wordt gemaakt van relationele databasemanagementsystemen wordt hierna alleen stilgestaan bij deze DBMS'n. Voor een nadere toelichting op de twee andere soorten wordt verwezen naar het boek van de auteur[19].

Kenmerkend voor relationele DBMS'n is dat gegevens worden opgeslagen in zogenaamde tabellen, die weer bestaan uit kolommen waarin records worden opgeslagen. Belangrijke kenmerken van deze DBMS'n zijn[20]:
- eenvoud in opzetten van de database;
- eenvoud in aanpassingen en onderhoud;
- relaties zijn eenvoudig te leggen;
- eenvoudige querytaal (SQL);
- snelheid;
- ondersteuning van een groot aantal hardwareplatformen;
- sluit aan bij moderne technieken.

Naast de basisfuncties[21] die een DBMS per definitie heeft, is er ook een aantal bijzondere aspecten bij gekomen die het ook voor kleinschalige organisaties aantrekkelijk maken om gebruik te maken van relationele databasemanagementsystemen. Deze aspecten zijn:
- het gebruik maken van stored procedures;
- two phase commit;
- replicatie;
- transactie processing.

Een eenmaal goed ingericht standaardpakket kan zorgen voor een integere gegevensverwerking.

Het gebruik van stored procedures (varianten hierop zijn de begrippen triggers en rules) maakt het mogelijk direct aan de gegevensdefinitie controlemogelijkheden te koppelen. Dit betekent dat bij bijvoorbeeld het muteren van een gegeven een stored procedure wordt opgestart die automatisch controleert of de mutatie juist is. In feite spreken we hier van een geprogrammeerde controle. Het voordeel van een dergelijke aanpak is dat bij het benaderen van een gegeven de geprogrammeerde controle altijd wordt uitgevoerd. Een tweede voordeel is dat deze controles niet meer opgenomen hoeven te worden in de toepassingsprogrammatuur zelf, hetgeen het onderhoud aanzienlijk vereenvoudigt. Zantinge en Adriaans[22] stellen in dit verband dat er sprake is van intelligente databases. Dit zijn gewone databases, waarbij men door middel van stored procedures een extra dimensie toevoegt aan de mogelijkheden van de database.

Het two phase commit protocol zorgt ervoor dat de gegevensverwerking gericht op gegevens die op meerdere servers zijn opgeslagen, op een integere wijze plaatsvindt. Pas wanneer op beide servers de gegevens goed zijn verwerkt, worden de transacties definitief gemaakt. Gaat het op één van beide systemen fout dan wordt de foutieve transactie op beide servers door middel van een zogenaamde roll back teruggedraaid. De gebruiker moet er vervolgens voor zorgen dat de transactie nog een keer wordt verwerkt.

Via replicatie is het mogelijk dat gegevens op meerdere plaatsen worden opgeslagen. Het DBMS zorgt er vervolgens voor dat periodiek de gegevens op elkaar worden afgestemd. De beheerder van de database (de hiervoor genoemde systeembeheerder) kan zelf bepalen welke gegevens gerepliceerd worden en wanneer de gegevens gesynchroniseerd worden. Het grote voordeel van deze benadering is dat de gegevensverwerking relatief snel kan geschieden zonder dat de integriteit van de database direct in gevaar komt. Een bijkomend voordeel is dat de gegevens meerdere keren opgeslagen worden hetgeen ook de beschikbaarheid van de opgeslagen gegevens verbetert.

Transaction processing is een ontwikkeling die afkomstig is uit de mainframewereld. Met name het product Customer Information Control System (CICS) van IBM is een zeer bekend voorbeeld. Een dergelijke TP-monitor maakt het mogelijk een grote hoeveelheid transacties tegelijkertijd te verwerken. Om dit te kunnen doen moet aan een aantal voorwaarden worden voldaan[23]:

18. Zie Inleiding EDP Auditing van Jan van Praat en Hans Suerink, Kluwer Bedrijfswetenschappen, 1995, blz. 132 e.v.
19. Inleiding EDP Auditing van Jan van Praat en Hans Suerink, Kluwer Bedrijfswetenschappen, 1995.
20. Zie Client/Server en gedistribueerde databases van D. Zantinge en dr. P.W. Adriaans, Lansa Publishing, 1994, blz. 68 e.v.
21. De belangrijkste zijn: Concurrency control, referentiële integriteit, back up en recovery.
22. Client/Server en gedistribueerde databases van D. Zantinge en dr. P.W. Adriaans, Lansa Publishing, 1994, blz. 83.
23. Client/Server en gedistribueerde databases van D. Zantinge en dr. P.W. Adriaans, Lansa Publishing, 1994, blz. 130.

J.C. van Praat RE RA
Is sinds 1977 werkzaam in de openbare accountantspraktijk, waarvan sinds 1984 fulltime als EDP-auditor. Momenteel is de heer Van Praat werkzaam als Senior EDP Audit Manager en leider van de Haagse vestiging van KPMG EDP Auditors. Daarnaast is hij universitair hoofddocent aan de postdoctorale opleiding EDP Auditing aan de Erasmus Universiteit Rotterdam. Hij publiceert regelmatig over typologie en beveiliging van IT-systemen.

– Atomicity: de verandering die een transactie in het systeem teweegbrengt, is atomair. Dat betekent dat de hele transactie al of niet is verwerkt.

– Consistentie: als de transactie wordt uitgevoerd op een consistent systeem dan is het resultaat ook altijd een consistent systeem.

– Isolatie: een transactie kan pas invloed hebben op een andere transactie als zij volledig is afgehandeld.

– Duurzaamheid: als een transactie is afgehandeld dan is de wijziging van het systeem duurzaam.

Ook in kleinschalige automatiseringsorganisaties wordt steeds meer gebruikgemaakt van transactieprocessors. CICS is bijvoorbeeld ook beschikbaar voor de AS/400 en Unix-systemen.

Gevolgen voor de kleinschalige automatiseringsomgeving

Omdat ook in kleinschalige organisaties de informatievoorziening steeds belangrijker wordt, is het noodzakelijk dat ook daar het beheer van gegevens de nodige aandacht krijgt. Het gebruik van databasemanagementsystemen levert hierbij een belangrijke bijdrage. Het grote voordeel hiervan is de sterk verbeterde toegankelijkheid van de in de systemen opgeslagen gegevens. Het gebruik van deze systemen in combinatie met de hiervoor genoemde informatiesystemen (die zelf ook gebruikmaken van een DBMS) geeft grote mogelijkheden voor een op de organisatie afgestemde informatievoorziening. Door dergelijke systemen in te zetten is het ook voor kleinschalige omgevingen steeds beter mogelijk een sneller inzicht te verkrijgen in de gang van zaken in de onderneming. Een aanvullende voorwaarde hiervoor is wel dat het management goed op de hoogte is van de mogelijkheden die deze systemen bieden.

SAMENVATTING

In het begin van dit artikel is aangegeven dat de organisatie van de gegevensverwerking een aanzienlijk probleem was in een kleinschalige automatiseringsomgeving. Voor accountants was dit probleem vaak zo groot dat men dan maar om de computer heen controleerde. Uit dit artikel blijkt echter dat met name de ontwikkelingen in de informatie- en communicatietechnologie steeds meer mogelijkheden bieden om een oordeel over de betrouwbare gegevensverwerking te onderbouwen. Een aantal aansprekende voorbeelden hiervan is:

- het gebruik van standaardprogrammatuur, niet alleen in de ondersteunende, maar ook in de primaire processen;
- de beschikbaarheid van tools om de technische infrastructuur te kunnen beheersen;
- de mogelijkheid van een gecentraliseerd beheer van de technische infrastructuur met behulp van deze tools;
- de mogelijkheid om gebruik te maken van PC-servers en netwerkcomputers;
- de uitstekende mogelijkheden van databasemanagementsystemen om gegevens te beheren en beschikbaar te stellen aan de gebruikers.

Maar de organisatie van de gegevensverwerking blijft een punt van aandacht. Gezien de hiervoor genoemde ontwikkelingen blijft het noodzakelijk om te streven naar een adequaat ingevuld systeembeheer (of netwerkbeheer). Om de technische infrastructuur (apparatuur, besturingsprogrammatuur, datacommunicatie en toepassingen) te kunnen beheren is het zonder meer nodig een deskundig beheer in te richten. Verder is het belangrijk dat het management de nodige aandacht besteedt aan het functioneren van het systeembeheer. Hierbij behoort een goed ingevuld verantwoordingsmechanisme.

Beheer en beveiliging van Client/Servers

Ir.drs. J. van der Vlugt

Client-serversystemen bieden flink wat flexibiliteit tegen de prijs van flexibiliteit voor ongenode gasten. Om tot een adequate beveiliging te komen, zullen de bedreigingen moeten worden onderkend en met technische en organisatorische maatregelen bestreden.

INLEIDING

In steeds meer systemen wordt gebruikgemaakt van het client-serverconcept. Vaak is dat vanwege het gevoel mee te moeten met de tijd. Ook zijn vele standaardapplicaties zoals databasemanagement-systemen opgezet volgens client-serverprincipes (hoewel vaak minder consequent dan voorgespiegeld) omdat daarmee de gewenste mate van 'open'heid van de systemen is te bereiken. Doordat aan zo'n open applicatie eenvoudig andere standaardapplicaties en maatwerk kunnen worden gekoppeld, kan de afnemer relatief eenvoudig vervangende of nieuwe applicaties toevoegen.
Deze zaken betekenen dat het client-serverconcept bij uitstek geschikt is voor kleinere IT-omgevingen, omdat juist die geen eigen (huis)standaard kunnen afdwingen en zij maatwerk en dergelijke vaak niet zelf en veelal met relatief hoge kosten door anderen kunnen laten ontwikkelen.

Nu lijkt het vanuit beveiligingsoogpunt wel eens alsof met het client-serverconcept van beide zijden alleen de negatieve aspecten worden overgenomen: de centrale controlemogelijkheden gaan verloren en de lokale beveiliging verbetert niet. Nu client-serversystemen volwassen worden, komen er steeds meer en steeds betere beheerhulpmiddelen op de markt om vanuit centrale beheerorganen decentrale systemen te kunnen beheren. Op beveiligingsgebied lijkt de markt nog niet geheel uitgekristalliseerd, al gaan de ontwikkelingen snel en worden de producten steeds beter.

Behalve met technische hulpmiddelen staat of valt een effectief IT-(beveiligings)beheer met een goede (administratieve) organisatie. Echter juist in kleinere organisaties, waar client-serversystemen een groot deel van de IT-infrastructuur uitmaken, is er nog wel eens wat aan te merken op de beheerorganisatie. Vaak niet uit onwil – gezien de omvang van dergelijke organisaties is het gewoonweg niet effectief of efficiënt om meer mensen en middelen in te schakelen voor het IT-beheer. Met een kanon op een mug schieten doet het wellicht aardig onder vakgenoten als men eens een keer raak blijkt te hebben geschoten, bij het management zal een goede balans tussen bedreigingen en tegenmaatregelen een betere (blijvende) indruk maken.

Wil men de balans goed in evenwicht brengen, dan zullen de bedreigingen en tegenmaatregelen in redelijk detail moeten worden onderzocht. In dit artikel wordt hierop ingegaan. Allereerst zal een overzicht worden gegeven van de technische componenten van client-serversystemen voorzover die uit beheer- en beveiligingsoogpunt relevant zijn. Daarna zal worden ingegaan op de bedreigingen voor de vertrouwelijkheid, integriteit en beschikbaarheid van de gegevens. Die gegevens zullen immers het uiteindelijke doel van systeemgebruik of inbraakpogingen zijn, de programmatuur eromheen is alleen een middel.
Vervolgens zullen de maatregelen tegen die bedreigingen worden besproken. Tot slot zullen de controlemogelijkheden worden gerecapituleerd.

CLIENT-SERVERSYSTEMEN

Client-serveromgevingen kennen geen beveiligingsrisico's die fundamenteel verschillend zijn van die van andere omgevingen. Waar in die andere omgevingen de systeemcomponenten veelal in een computer of systeem zijn geïntegreerd, zijn bij een client-serveromgeving de componenten vaak verdeeld over diverse systemen of anderszins vrij zelfstandig te herkennen.

Figuur 1 geeft een sterk vereenvoudigd overzicht van de technische componenten van een client-serverarchitectuur. Daarin is aangegeven dat normaliter een gebruiker met een keuze in een menu of met een muisklik op een button een vraag om informatie stelt aan de applicatie. De gebruiker hoeft daarvoor niet te weten dat het slechts de clientapplicatie is die hij bevraagt. De informatieaanvraag komt bij de applicatie aan met eraan gekoppeld de naam of andere identificatie van de gebruiker. De applicatie bepaalt vervolgens of aan het verzoek ter plekke kan worden voldaan. Bij een client-serverapplicatie is dit hoogst onwaarschijnlijk.

De applicatie zal dan ook bezien welke andere (deel)applicatie de gestelde vraag wél kan beantwoorden, en verpakt de gebruikersvraag in een eigen (remote procedure) call, inclusief wederom enige identificerende gegevens. Deze call wordt doorgegeven aan het operatingsysteem; eventueel via middleware, als die als apart element kan worden onderscheiden.

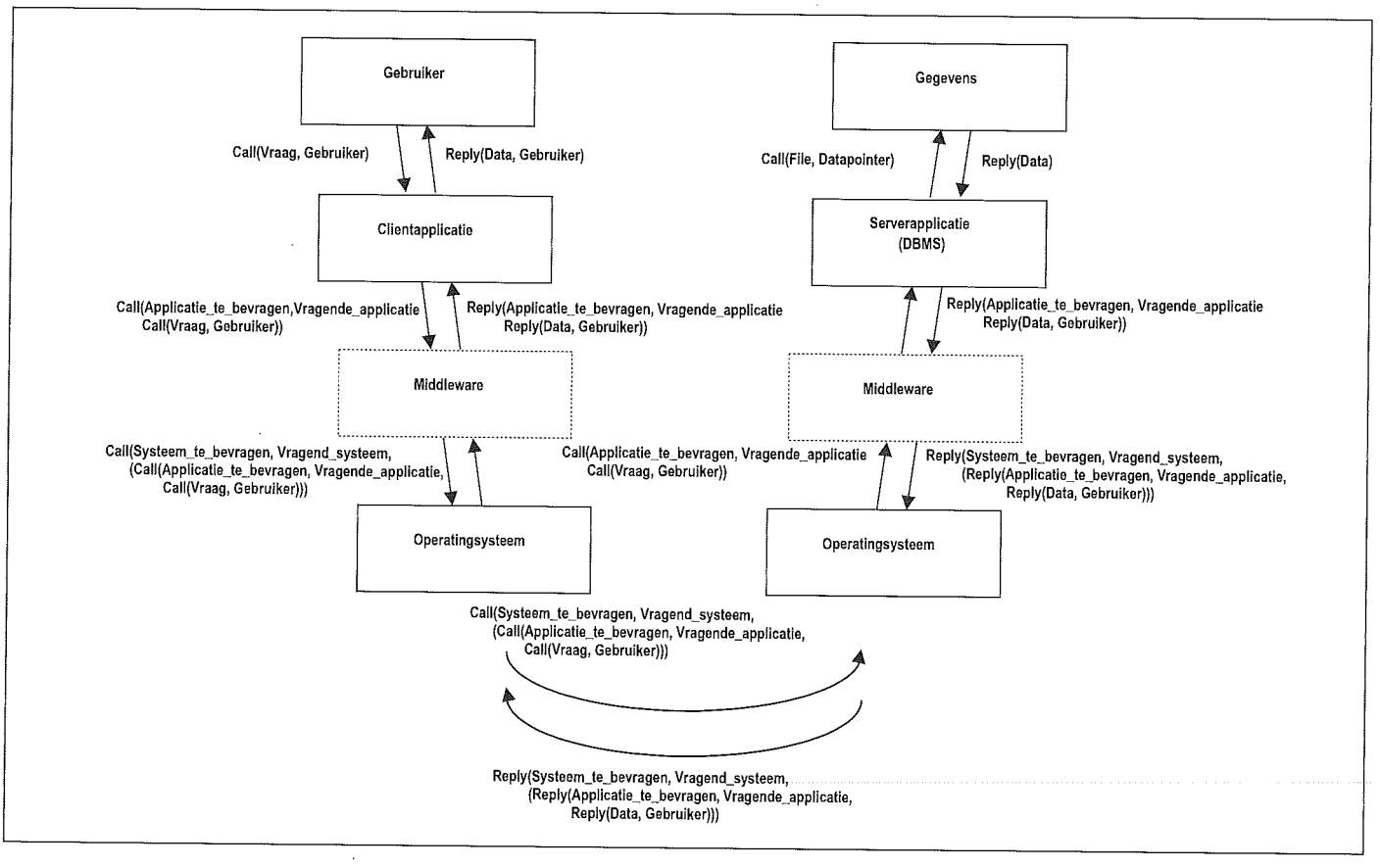
Het operatingsysteem kan op zichzelf niets doen aan het beantwoorden van de oorspronkelijke vraag en fungeert alleen als intermediair tussen clientapplicatie en serverapplicatie. Zodra het operatingsysteem de locatie van de serverapplicatie kent, geeft hij de call van de clientapplicatie daaraan of daarheen door. De middleware verzorgt vaak dat opzoeken van de locatie van de serverapplicatie of het systeem waar desgewenst zo'n serverapplicatie kan worden gestart.

Het operatingsysteem aan de ontvangende kant ontvangt de call en 'pakt die uit'. Het resultaat, de call aan de serverapplicatie, wordt aan de serverapplicatie – in figuur 1 is deze omwille van de eenvoud aangeduid als DBMS – doorgegeven. De serverapplicatie bepaalt de gegevensbehoefte door een vertaling van de call met oorspronkelijke vraag naar een vraag om specifieke gegevens uit file(s), en geeft die call door aan de gegevens (in casu het filesysteem).

Vervolgens wordt het hele traject terugwaarts doorlopen. Daarbij worden de identificaties van de aanvragers (operatingsysteem, clientapplicatie en gebruiker) als adres gebruikt.

BEDREIGINGEN

Uitgangspunt is dat ieder element en iedere gegevensoverdracht kwetsbaar is voor inbreukpogin-



Figuur 1. Client-servercomponenten vanuit technische optiek.

gen op de vertrouwelijkheid, integriteit of beschikbaarheid.

Vertrouwelijkheid en integriteit

Te onderscheiden zijn:
- de valse gebruiker;
- de ongeautoriseerde gebruiker;
- een Man in the Middle;
- fouten in de serverapplicatie;
- fouten in de input.

Valse gebruiker
Ten eerste kan het zijn dat de gebruiker niet is wie hij zegt te zijn. Dit gebeurt met name door het bij anderen dan de rechtmatige gebruiker bekend raken van de user-id-passwordcombinatie. Dit kan eenvoudig doordat gebruikers elkaars user-ids en passwords kennen om bij vakantie of andere afwezigheid bepaalde taken van elkaar te kunnen overnemen. Dit mag dan een aanzienlijke inbreuk zijn op de regels van administratieve organisatie, in de praktijk komt dit zeer regelmatig voor. Een andere manier van het bekend raken van passwords is dat gebruikers te eenvoudige passwords kiezen. Andere gebruikers of hackers zullen die dan kunnen achterhalen. Daar user-ids meestal in enige vorm de naam van de gebruiker of de organisatiestructuur bevatten, zijn die eenvoudig te raden: een andere gebruiker kan uit zijn eigen user-id afleiden hoe die van een collega eruit zal zien. Een hacker kan het dataverkeer over een netwerk afluisteren en kan daarin de identificaties van gebruikers voorbij zien flitsen.

Ongeautoriseerde gebruiker
Daarnaast kan het zijn dat de gebruiker in kwestie niet bevoegd zou mogen zijn om de vraag die hij stelt, te stellen. Dit kan het geval zijn als een applicatie een reeks van functies bevat die omwille van de controletechnische functiescheiding over diverse functionarissen dient te worden verdeeld. Als dat onvoldoende gebeurt – doordat de (client- of server)applicatie dat niet kan, of doordat de instellingen wel mogelijk zijn maar niet zijn geïmplementeerd – biedt dit een enkele gebruiker de mogelijkheid met zichzelf samen te spannen.

Aan de andere kant zal een gebruiker al of niet met boze opzet kunnen proberen buiten de client-serverapplicatie om bij de gegevens te komen. De hulpmiddelen (tools) om direct files op harde schijven te onderzoeken zijn nog steeds wijd en zijd voorhanden. Of de verkregen data eenvoudig leesbaar is, zal de meeste kwaadwillende inbrekers niet veel uitmaken – een bestand met hexadecimale karakters is met enige nabewerking meestal snel inzichtelijk te maken.

Man in the Middle
Het is niet op voorhand zeker te stellen dat de vraag van de gebruiker wel direct bij de clientapplicatie terechtkomt. Het is voor een ontwikkelde programmeur een koud kunstje om een programma te schrijven dat zich tussen de gebruiker en de clientapplicatie plaatst ('Man in the Middle'[1]).

Bij een Man in the Middle wordt normaliter alleen gedacht aan het afluisteren van het opstarten van berichtensessies, dat wordt onderbroken zodra de Man in the Middle voldoende informatie heeft om één van beide partijen te impersonificeren, die partij vervolgens buiten werking te stellen en dan zelf als ware hij de werkelijke tegenpartij toegang te krijgen tot de berichten van de andere partij.
Het is echter ook mogelijk dat het optreden van de Man in the Middle voor beide partijen onzichtbaar blijft. En wel als alle gebruikersverzoeken en de respons daarop zullen worden gekopieerd, waarna ze conform verwachting worden afgehandeld. Als de Man in the Middle later de gekopieerde gegevens analyseert, zal hij allicht allerlei gegevens over inlogpogingen terugvinden, inclusief user-ids en passwords, en kan hij kopieën krijgen van gegevens die uit organisatie- of privacy-perspectief vertrouwelijk zouden kunnen zijn. Hij kan daarna ook zelf allerlei acties uitvoeren als ware hij een legitieme gebruiker.

Het optreden van een Man in the Middle kan voor beide partijen onzichtbaar blijven

Dit Man-in-the-Middlescenario is van toepassing op alle communicatie zoals aangegeven in figuur 1. Zo kan een hacker de gegevens in een call van een clientapplicatie aan de middleware lezen en/of wijzigen, of een eigen variant van de call in de communicatiestroom tussenvoegen. Hij kan bijvoorbeeld ook de call in of komende vanaf de middleware zodanig laten wijzigen dat de call vanuit het operatingsysteem eerst bij een 'verkeerd' systeem terechtkomt, daar wordt gekopieerd en/of gewijzigd en vervolgens naar het oorspronkelijk bedoelde systeem wordt verzonden.
In figuur 1 staat met steekwoorden een aantal parameters aangegeven die in de client-servercommunicatie worden uitgewisseld. Een inbreker met voldoende kennis (en juist kwaadwillende hackers hebben die kennis) kan, indien geen tegenmaatregelen zijn genomen, elk van die parameters wijzigen.

In bovenstaande Man-in-the-Middlebedreigingen is er telkens sprake van het ogenschijnlijk ongestoord doorzenden van de gegevens na kopiëren, modificeren en/of herstellen. Dit dient om te voorkomen dat de Man-in-the-Middle te veel in de gaten loopt. Zodra immers allerlei berichten die afgetapt worden, niet aankomen, zullen de bijbehorende clientapplicaties en hun gebruikers al snel gaan klagen. De kundige hacker zal er dan ook voor zorgen tussen de responsberichten (ontvangstbevestigingen) die tussen allerlei communicatieschakels worden uitgewisseld, juist het responsbericht dat van doen heeft met de gemodificeerde call, terugwaarts aan te passen alsof er niets aan de hand is.

Fouten in de serverapplicatie
De integriteit van het systeem wordt ook bedreigd doordat in de serverapplicatie een aantal zaken mis kan gaan. De risico's bestaan uit:

1. Of Trojan horse, hoewel daarbij eerder gedacht wordt aan het door de gebruiker bewust binnenhalen van een ogenschijnlijk nuttige applicatie met onvermoede malicieuze neveneffecten.

– Het ongeautoriseerd toegang verschaffen aan gebruikers. Veelal zal de serverapplicatie de in menubeveiliging doorgevoerde autorisatiestructuur dienen te controleren. Maar al te vaak is die structuur onvoldoende nauwkeurig in te stellen en als dat wel kan, blijkt dat in de praktijk vaak onvoldoende te zijn gebeurd.

– Trojan horses. Dit zijn programmaatjes die, zonder dat de gebruiker er iets van merkt, worden meegebracht met allerlei 'handige' uitbreidingen van de serversoftware. Met sommige screensavers worden bijvoorbeeld stukjes programma meegeïmporteerd die de door de gebruiker ingetypte passwords apart opslaan zodat ze later door een hacker kunnen worden opgehaald.

– Verwerkingsfouten. Software is mensenwerk, en foutvrije programmatuur is uiterst zeldzaam. Programmeurs voelen zich echter vrijwel altijd voldoende zeker van hun zaak om controletotalen achterwege te kunnen laten. Daardoor kan bijvoorbeeld een database wel degelijk vervuild raken ondanks dat allerlei referentiële integriteiten schijnbaar worden gecontroleerd.

Fouten in de input
Ten slotte vormen ook (soms triviale) invoerfouten een bedreiging voor de integriteit. De invoerfouten zijn onder te verdelen in het op de juiste plaats invoeren van verkeerde gegevens en het op de verkeerde plaats invoeren van de juiste gegevens.

In het eerste geval is er sprake van gewone typefouten. Niets menselijks is de gebruiker vreemd. Het risico is echter dat een applicatie dit soort invoerfouten niet signaleert of niet kan signaleren; een verkeerd ingevoerd jaartal zal allicht als zodanig best geldig kunnen zijn.
Het verkeerd invoeren van de juiste gegevens is net wat subtieler. Daarbij gaat het erom dat gegevens in de verkeerde velden of in de verkeerde schermen worden ingevoerd. Als de gegevens dan ook nog door allerlei losstaande invoercontroles komen, is achteraf zeer moeilijk te achterhalen waar de gegevens zijn gebleven.

Beschikbaarheid: DoS

Het netjes doorgeven van berichten door een Man in the Middle doet een hacker natuurlijk niet als hij destructieve doelen nastreeft. Als hij kan zorgen anoniem te blijven, zal hij door het muteren of weghalen van berichten in de communicatiestromen aanzienlijke schade kunnen aanrichten. Vele systemen zullen immers maar zeer beperkte hoeveelheden misinformatie kunnen verwerken (afwijzen) voordat ze vastlopen door overlopende buffers of ingeprogrammeerde 'paniek'-standen.

Deze zogenaamde Denial-of-Service (DoS-)aanvallen zullen normaliter met name gericht zijn op de elementen die van buitenaf bereikbaar zijn. Hierbij valt met name te denken aan de operatingsystemen die vanaf externe netwerkverbindingen worden aangevallen. Soms richt de aanval zich alleen op het voor systemen van buitenaf onbereikbaar maken van het operatingsysteem, soms ook gaat de aanval verder en wordt ervoor gezorgd dat het systeem in zijn geheel wordt overbelast waardoor het ook voor de middleware en client- of serverapplicaties onbruikbaar wordt – en daarmee voor de gebruikers.

Twee afwijkende vormen van DoS-aanvallen mogen echter niet ongenoemd blijven. Ten eerste kan een kwaadwillende hacker door het willekeurig raden van passwords een account blokkeren. Om password raden tegen te gaan zal een account immers normaliter na drie of vier onjuiste passwords blokkeren. Als een hacker maar genoeg user-id-passwordcombinaties laat proberen – dat kan zeer eenvoudig geautomatiseerd en dus zeer snel –, zal hij ongetwijfeld een groot deel van de accounts kunnen uitschakelen. Als hij op deze manier ook de accounts van de systeembeheerders blokkeert (of van anderen die accounts kunnen deblokkeren), zal in principe niemand met voldoende rechten meer in het systeem kunnen komen om herstelacties uit te voeren.
Ten tweede kan een DoS-aanval worden uitgevoerd op de gegevens. Door een commando binnen te smokkelen dat gegevens wist, zullen die gegevens onbereikbaar worden voor de eigenlijke gebruikers. In de praktijk blijkt deze mogelijkheid veel simpeler toegankelijk dan wel eens wordt gedacht. Een commando als 'format C:' of vergelijkbare strekking valt in kleinere systemen juist vaak gemakkelijk als parameter mee te geven bij het opstarten van overigens zeer gangbare programma's, of is te verpakken in een willekeurige zoekopdracht.

TECHNISCHE TEGENMAATREGELEN

In tabel 1 zijn de hiervoor genoemde bedreigingen per client-serverelement weergegeven, alsmede de te nemen tegenmaatregelen. Deze paragraaf bespreekt vooral de technische maatregelen tegen de bedreigingen, de maatregelen van organisatorische aard worden in de volgende paragraaf besproken.

Passwords
Een terrein waar de laatste tijd behoorlijke vooruitgang is geboekt, is het met technische middelen (software) afdwingen van het gebruik en de tijdige vernieuwing van sterke passwords. Hiermee kan een aanzienlijk deel van de zwakten van de gangbare praktijken van eigennamen en automerken worden weggenomen. Nodeloos te zeggen dat het met ingewikkelder passwords des te belangrijker wordt om met organisatorische richtlijnen zeker te stellen dat niemand zijn password opschrijft.

Menu- en bestandsbeveiliging
Hiervoor was er steeds sprake van beveiliging van de uitgewisselde berichten c.q. het uitsluiten van ongeautoriseerde berichten of gebufferde gegevens. Een andere manier van beveiligen bestaat uit het beveiligen van toegang tot de client-servercomponenten zelf. Twee belangrijke elementen daarin zijn het begin en eind van het verwerkingstraject: menubeveiliging en bestandsbeveiliging. Hiermee kan een aantal vertrouwelijkheids- en integriteitsrisico's worden verminderd.

Bedreigingen	Tegenmaatregelen
Valse gebruiker	Organisatorisch: richtlijnen inzake geheimhouding, passwords, uitloggen en controle daarop. Technisch: implementatie en automatische controle sterke passwords en passwordleeftijden.
Ongeautoriseerde gebruiker	Organisatorisch: menubeveiliging gebruiken en controleren, indien niet aanwezig of aanvullend: rapportage ter decharge, richtlijnen inzake fysieke toegangsbeveiliging en controle daarop. Technisch: menubeveiliging, bestandsbeveiliging (filesysteem-niveau en/of versleutelen).
Man in the Middle: afluisteren	Technisch: versleutelen berichtinhoud (ongebruikelijk voor intern berichtenverkeer)*, gescheiden processen.
Man in the Middle: modificeren of toevoegen	Organisatorisch: richtlijnen inzake fysieke toegangsbeveiliging en controle daarop. Technisch: elektronische volgnummers waarin verwerkt de zender- en ontvangerauthenticatie, tijdstempel en berichtkenmerken, versleutelen (ongebruikelijk voor intern berichtenverkeer)*, gescheiden processen.
Trojan horse	Organisatorisch: richtlijnen inzake change management en fysieke beveiliging en controle daarop.
Verwerkingsfouten (bewust of onbewust)	Technisch: indien aanwezig controletotalen, invoercontroles en andere application controls.
Denial-of-Service: accounts blokkeren	Organisatorisch: richtlijnen inzake logische en fysieke beveiliging en controle daarop. Technisch: filteren van berichtenverkeer.
Denial-of-Service: gegevens deleten	Organisatorisch: richtlijnen inzake fysieke toegangsbeveiliging en controle daarop. Technisch: filteren van berichtenverkeer en bestandsbeveiliging (filesysteem-niveau en/of versleutelen).
Denial-of-Service: systeem blokkeren	Technisch: filteren van berichtenverkeer.

* Ongebruikelijk, want de gebruiker, applicaties, middleware en operatingsysteem behoren normaliter tot de vertrouwde systeemomgeving; *mits* met voldoende organisatorische beveiliging en general IT controls is het risico op inbreuk inderdaad niet zeer groot.

Tabel 1. Bedreigingen bij elementen van client-server-omgevingen en tegenmaatregelen.

Menubeveiliging richt zich op de subjectkant van systeemgebruik: Mag de gebruiker die zich aandient wel de systeemfunctie gebruiken die hij wil? Voorzover de applicatie al voldoende functiescheidingen toestaat in de menubeveiliging (de granulariteit ofwel fijnkorreligheid is vaak te grof), is er zeker in kleinere omgevingen vaak een probleem met het goed inrichten en handhaven van de autorisatietabellen, zoals hieronder nader zal worden uitgewerkt. Bovendien is identificatie van de gebruikers steeds problematischer geworden. De mogelijkheid om zich voor te doen als een ander (zie Man in the Middle hierboven) en softwarefouten (waaronder ook het vergeten van het uitschakelen van de mogelijkheid om uit de menuprogrammatuur te breken) verminderen de garanties die aan menubeveiliging kunnen worden ontleend. Voorzover de juiste beheermaatregelen worden getroffen en controles op de loggings en dergelijke plaatsvinden, zal menubeveiliging normaliter echter een nuttig preventief element in het totaal van beveiligingsmaatregelen zijn.

Bestandsbeveiliging richt zich daarentegen op de objectkant van systeemgebruik: Gegeven het feit dat de gebruiker de systeemfunctie kennelijk mag gebruiken, mag dat dan wel voor de gevraagde gegevens? In wezen is er dan sprake van een menubeveiliging op bestandsniveau. Veelal wordt er hierbij (soms ook expliciet door de serversoftware) vertrouwd op het operatingsysteem waar het filesysteem onderdeel van uitmaakt. Ook hier spelen de problemen van de granulariteit, de discipline in het beheer van al of niet toegekende rechten en de technische kwaliteit van de software (het operatingsysteem en het filesysteem) een rol. Alle drie laten ze nogal eens te wensen over, ook bij operatingsystemen die leidend zijn in de markt voor server-operatingsystemen.
Dit neemt niet weg dat adequate bestandsbeveiliging een zeer aanzienlijke bijdrage levert aan het totaal van beveiligingsmaatregelen.

Mocht dan toch ongeautoriseerde toegang zijn verkregen, dan kan de bruikbaarheid van ongeautoriseerde toegang tot bestanden worden verminderd door versleuteling van de opgeslagen gegevens. Door de voortschrijdende techniek zijn hiervoor inmiddels zeer bruikbare hulpmiddelen beschikbaar gekomen. De voorheen hoge overhead door het telkens moeten ver- en ontsleutelen van gegevens is in de laatste jaren aanzienlijk teruggebracht. Tegenwoordig kan versleuteling zonder meer een wezenlijke bijdrage leveren aan effectieve en efficiënte gegevensbeveiliging – binnen zekere grenzen. Het risico blijft natuurlijk dat de gegevens met harde

schijf en al worden gestolen en de kapitaalkrachtige dief de versleuteling kraakt. De techniek schrijdt op dit punt snel voort; kraaktechnieken die tot voor kort onmogelijk veel tijd zouden vragen, kunnen heden ten dage binnen afzienbare tijd worden uitgevoerd.

Berichtennummering, versleutelen
In de praktijk lijkt het vaak niet nodig om alle berichtenverkeer tussen gebruiker en operatingsysteem en tussen operatingsysteem en gegevens te versleutelen of te voorzien van elektronische volgnummers met allerlei integriteitsinformatie erin verwerkt. Er is immers vaak sprake van een vertrouwde omgeving, ofwel alle elementen staan onder redelijke controle, en met voldoende algemene computercontroles kan worden voorkomen dat er, om maar iets te noemen, geen virussen of Trojaanse paarden worden binnengehaald.

De neiging bestaat derhalve om voor het berichtenverkeer tussen operatingsystemen (het netwerkverkeer) de risico's wat laag in te schatten. Hier lijkt een rol te spelen dat voor niet-ingewijden zoals sommige managers, dergelijke aanvallen technisch nogal moeilijk uitvoerbaar lijken. Door het achterwege laten van een voldoende diepgaande risicoinschatting wordt het moeilijke onderwerp van berichtversleuteling eenvoudig vermeden. Een Denial-of-Service is immers eenvoudig op te lossen door de netwerkstekkers eruit te trekken?

Maar de risico's op een Man in the Middle en op Denial-of-Serviceaanvallen zijn heel wat groter dan ze op het eerste gezicht lijken. De technische moeilijkheidsgraad valt mee, en in de praktijk blijken kwaadwillenden vaak veel tijd óf geld te hebben om eenvoudig hanteerbare technische hulpmiddelen te ontwikkelen. Misschien lijken de gevolgen van een Denial-of-Serviceaanval dan niet zo groot, maar de werkelijke schade bestaat mede uit imagoverlies en verloren werkuren van soms vele medewerkers. Opgeteld kan het dan gaan om een aanzienlijke verliespost.

De risico's op een Man in the Middle en op Denial-of-Serviceaanvallers zijn heel wat groter dan ze op het eerste gezicht lijken.

Een Man in the Middle zal minder vaak voorkomen en is ook minder eenvoudig te realiseren, de schade echter is navenant groter. Een geoefende tegenstander (en dat is hij al als hij zich aan zo'n aanval waagt) kan in principe bij alle gegevens komen die hij wil. Van vertrouwelijkheid of waarborgen voor de integriteit is dan weinig sprake meer. De auteur kent een praktijksituatie waarin bij een systeem met een zeer gecompliceerde versleuteling van berichtinhoud, berichtvolgnummers, verzendtijd en -datum, zender- en ontvangeridentificaties en kenmerken van alle berichtelementen en een zeer beperkte kring van insiders, toch een poging werd gedaan om financiële transacties die de inbreker zouden bevoordelen, binnen te smokkelen gedurende specifieke berichtensessies. Voorwaar een bijzondere technische prestatie die op voorhand bijna uit te sluiten zou zijn, maar de genoemde beveiliging bleek maar net omvattend genoeg om de inbraak te verijdelen en de inbreker te grijpen. Als het even kan is dergelijke versleuteling dus zonder meer aan te raden.

Versleuteling als techniek heeft natuurlijk ook zijn eigen mitsen en maren. Zo zijn zelfs de meest veilig geachte algoritmen kraakbaar gebleken. Wat men daar echter bij vergeet te vermelden, is dat het om zeer gecoördineerde kraakpogingen ging. In de praktijk zal de economische waarde van een gekraakt bericht vrijwel altijd al nihil zijn tegen de tijd dat de code gekraakt is, en naast vooruitgang in de kraaktechnieken (hardware en algoritmen) is er ook vooruitgang in de versleutelingsalgoritmen.

Gescheiden processen
Een onderwerp dat verwant is aan wat men normaliter onder logische toegangsbeveiliging verstaat, is het in de systemen gescheiden houden van de processen (draaiende programma's). Dit houdt in dat het ene programma niet in het geheugen van de andere kan lezen of schrijven; eventuele gegevensoverdracht tussen programma's vindt dan plaats op een door het operatingsysteem streng gecontroleerde wijze. Systeemontwikkelaars die applicaties voor grote mainframes maken, zijn daarmee geheel vertrouwd.

Bij kleinere systemen ontbraken echter tot voor kort de technische mogelijkheden tot dergelijke afscherming in de operatingsystemen. Daardoor zijn er nog vele applicaties in omloop – en daaronder zeer bekende – die gebruikmaken van allerlei gaten in de scheidingen tussen de draaiende programma's, of die dergelijke gaten bieden. Er kan dan niet meer worden vertrouwd op de vertrouwelijkheid van gegevens die in het geheugen van een bepaalde applicatie staan. Is er sprake van gegevens die alleen door die applicatie of alleen door de desbetreffende gebruiker met alleen die applicatie mogen worden bewerkt, dan zal het lezen door een andere applicatie namens dezelfde of een andere gebruiker van die gegevens een doorbreking zijn van de logische toegangsbeveiliging die overigens prima in orde lijkt te zijn.

Hieraan is ook het probleem gerelateerd dat na het afsluiten van een applicatie of alleen al het vrijgeven van een stuk intern geheugen of schijfruimte, daarop vaak nog de gegevens zijn te achterhalen. In grote systemen zijn faciliteiten aangebracht om die gegevens tijdig weg te poetsen, maar wederom zijn dergelijke middelen in kleinere systemen moeilijk te krijgen en zijn ze (omdat ze vaak ook performanceverlies met zich meebrengen) onhandig in gebruik.

Filteren van berichtenverkeer
Een effectief instrument tegen Denial-of-Serviceaanvallen maar ook tegen inbraakpogingen in het algemeen is het gebruik van firewalls, zowel voor de communicatie tussen eigen netwerken als tussen segmenten van de eigen netwerken. Door het filteren van berichten van typen die bij voorbaat

niet zijn toegestaan en door het op enige wijze op de firewall controleren van toegangsrechten kunnen 'aan de poort' reeds een hoop moeilijkheden worden voorkomen.

Firewalls vormen een belangrijk beheer(s)object. Het is zeker niet zo dat het eenmaal installeren van een firewall, als dat al goed gebeurt, de organisatie van alle zorg verlost. Organisaties die een of meer firewalls introduceren, vertrouwen er vaak op dat de firewall het overgrote deel van alle informatiebeveiliging zal overnemen. Men vergeet dan vaak dat alle beveiligingszaken dan wel alsnog in en rond de firewall moeten worden geregeld, en dat de firewall tevens een soort single point of failure wordt. Als er dan iets mis is met de firewall waardoor een indringer bijvoorbeeld weet binnen te komen, dan blijken vaak de verdedigingen erachter zwak te zijn.

Controletotalen
Een laatste technische tegenmaatregel is het in de software opnemen van controletotalen. Dit is een punt dat op zeer veel onbegrip stuit bij softwareontwikkelaars. Vanuit hun professionele trots begrijpelijk; controletotalen suggereren immers dat ze hun werk niet goed zouden doen en ze vragen kostbare verwerkingscapaciteit.

Anderzijds wordt niet (alleen) het werk van de softwareontwikkelaars gecontroleerd. Controletotalen zijn er juist om afwijkingen van de blijvende integriteit van de gegevens te signaleren. Dergelijke afwijkingen worden beslist niet alleen veroorzaakt door fouten in de software.

Invoercontroles en andere application controls
Een tweede trap van beveiliging is gelegen in de application controls. Jenkins, Cooke en Quest ([Jenk92]) delen die in in de volgende categorieën:
- file continuity;
- asset protection;
- completeness of input, hiervoor bestaan de volgende controles:
  - computer matching;
  - computer sequence check;
  - batch totals;
  - checking of print-outs;
- accuracy of input.

File continuity (dat de gegevens correct blijven) en asset protection zijn hierboven reeds besproken bij bestandsbeveiliging.

Op de punten completeness of input en accuracy of input bieden client-serveromgevingen een gemiddelde tussen wat op een PC-systeem mogelijk zou zijn en wat voor centrale systemen mogelijk zou zijn. De controles vinden noch in het geheel niet plaats zoals bij veel PC-georiënteerde systemen, noch worden ze pas veel later in batches doorgevoerd. De controles vinden in principe plaats op het meest natuurlijke moment, als verbetering nog mogelijk is: bij invoer.
Mits de controles zijn ingebouwd, natuurlijk. De computer matching, sequence checks, batch totals en geautomatiseerde accuracy checks zullen vrijwel altijd handmatig moeten worden ingeschakeld en in kleinere omgevingen wordt er omwille van de vereiste snelheid van ontwikkelen gemakkelijk één vergeten. Op zich is dat nog geen ernstige kwestie, er volgt normaliter immers nog een testfase en in het gebruik zullen verkeerde gegevens op een zeker moment ook wel gaan opvallen. Maar zeker in dat laatste geval is de schade dan al een feit. Niet alleen is er dan een speurtocht nodig naar de oorzaak van de afwijking, ook zullen de bestaande gegevens gedetailleerd moeten worden geschoond. Dus is het zaak daar alert op te zijn, zowel bij de ontwikkeling en implementatie van een systeem als achteraf bij het onderhoud.

De tendens naar meer client-serversystemen betekent een toename van het aantal onveilige clients in een netwerk.

Voor client-serveromgevingen speelt echter de marktmacht van softwareleveranciers (van pakketten of maatwerk) een negatieve rol. Ze leveren de software vaak zonder ingebouwde controletotalen of zonder goede signalering van afwijkingen. Controletotalen kunnen dan nog wel worden toegevoegd, maar soms tegen aanzienlijke meerkosten. Hierdoor komt het gebruik van controletotalen helaas vaak in de verdrukking. Terwijl toepassing ervan nu juist zo'n nuttige extra waarborg kan zijn voor de integriteit van de gegevens(verwerking).

ORGANISATORISCHE TEGENMAATREGELEN

De organisatorische tegenmaatregelen zijn vaak op een redelijk niveau geïmplementeerd zonder dat bewust gekozen is voor juist dát niveau. Om een wat meer consistent geheel van maatregelen te krijgen, is het belangrijk ze te inventariseren en hun bijdrage aan de totale beveiliging in te schatten. Daarvoor is een inzicht in de beperkingen van de organisatorische maatregelen nodig; hieronder zullen daarvan enkele worden besproken.

Fysieke toegangsbeveiliging

Inzake de maatregelen rond fysieke toegangsbeveiliging valt op dat ondanks dat de communicatiewereld toegroeit naar een mondiaal (Inter)netwerk, de vaak nogal rechttoe-rechtaan fysieke beveiliging weer in belang toeneemt. De snel toenemende afhankelijkheid van geautomatiseerde systemen en derhalve de potentiële schade door calamiteiten aan geautomatiseerde systemen is daar waarschijnlijk de voornaamste oorzaak van.

Tegelijkertijd betekent de tendens naar meer client-serversystemen dat het aantal onveilige clients in een netwerk toeneemt. Voorheen viel het op als een medewerker, of erger nog, een onbekende met een terminal rondliep, op zoek naar een aansluitpunt.

Met het voorheen beperkte aantal aansluitpunten was er nog relatief eenvoudig een overzicht te krijgen van de erop aangesloten clienthardware – die vaak ook nog persoonsgebonden was of waarvan het gebruik specifiek kon worden gecontroleerd (aparte afdelingsruimte).

Tegenwoordig past elke laptop-client in zowat elke dossierkoffer. Daarmee is het binnenbrengen van clienthardware met allerlei illegale software zeer eenvoudig geworden. Daaraan toegevoegd brengt het toenemend gebruik van netwerken (onder andere voor client-serversystemen) met zich mee dat er op steeds meer plaatsen binnen organisaties aansluitpunten voor de netwerken zijn. En al die aansluitpunten dienen ook nog zoveel mogelijk open te staan om hinderlijk lange wachttijden wegens het heropenen voor gebruikers te vermijden.

Als de onveilige client zich niet binnen het eigen kantoor bevindt maar bijvoorbeeld via een inbel- of Internetaansluiting 'binnenkomt', zijn de risico's natuurlijk nog groter. Als er al wordt gewerkt met authenticatie op basis van bezitskenmerken (PIN-codes of codegenererende pasjes) dan worden die immers bij voorkeur in de buurt van de PC bewaard. Diefstal van een koffer met laptop betekent dan al snel ook diefstal van de extra authenticatiemiddelen.

Logische toegangsbeveiliging

Een ander beveiligingsaspect dat aanzienlijk door de nieuwe client-serverstructuur is beïnvloed, is de logische toegangsbeveiliging. De aandacht gaat vooral uit naar de verdergaande ontwikkeling van authenticatie- en integriteitscontroles. De reeds bestaande lacunes in logische toegangsbeveiliging blijven echter bestaan.

Het in orde zijn van de opzet én het bestaan van beveiligingsmaatregelen blijkt nog steeds een uitzondering.

Zoals hiervoor aangegeven zijn de clients steeds minder te vertrouwen. Bovendien zijn client-serverstructuren nadrukkelijk gericht op het versturen en ontvangen van losse berichten. Daarmee worden de mogelijkheden voor het onderhouden van een elektronische vertrouwensband sterk verminderd. In toenemende mate zal het nodig zijn elk bericht, de afzender ervan en de betekenis binnen het eigen systeem te controleren op authenticiteit en integriteit, daar in de inhoud van een bericht malicieuze parameters, macrovirussen en dergelijke kunnen worden binnengesmokkeld. Een inhoudelijke beoordeling van de data zal nodig zijn.
Daarnaast zal vaak versleuteling van de berichtinhoud plaatsvinden. Hieraan zijn voordelen verbonden zoals de toegenomen waarborg van vertrouwelijkheid en integriteit (onontsleutelbare berichten worden weggegooid), maar ook nadelen zoals bemoeilijking van de authenticatiecontrole van elk binnengekomen bericht door de toegenomen vereiste capaciteit.

Zeker omdat met het toegenomen belang van individuele berichten en de toegenomen afhankelijkheid van de systemen de authenticiteit en integriteit van de berichten van groter belang zijn dan voorheen, zal met het oog op de aanslag op de verwerkingscapaciteit door het versleutelen en het berekenen van volgnummers bij systeemontwerpen, met het bepalen van de technische specificaties en de capaciteitsplanningen meer rekening moeten worden gehouden dan voorheen.

Almachtige beheerders
Eén van de belangrijkste lacunes in de logische toegangsbeveiliging is dat juist de operatingsystemen die vaak in client-serveromgevingen worden gebruikt, zogenaamde superuser accounts kennen voor de systeembeheerder(s). Dergelijke accounts zijn, door het operatingsysteem afgedwongen, zodanig opgezet dat bijvoorbeeld een systeembeheerder alle rechten nodig heeft voor het uitvoeren van zijn dagelijks werk. Of ten minste zal hij regelmatig de instelling van gebruikersrechten moeten kunnen wijzigen. En daarmee die van hemzelf, hetgeen betekent dat hij zichzelf eventueel ontnomen rechten weer terug kan geven.
Dit betekent een verzwaring van de controlerende taak. Serveroperatingsystemen hebben echter nogal eens de opzet dat de logging files ook voor de systeembeheerders (de gecontroleerden) toegankelijk zijn. De integriteit ervan kan dan niet worden gewaarborgd. Integendeel, juist de gecontroleerde systeembeheerders zullen vaak over de meeste kennis beschikken hoe onreglementaire (ongeautoriseerde) acties in de loggings te maskeren.
De enige oplossing die dan nog rest is de systeembeheerders belang te geven bij de juistheid van de loggings en andere verantwoordingen.
Indien een interne of externe auditor periodiek of onregelmatig vaststelt dat de systemen feitelijk precies zo blijken te zijn ingericht als uit de rapportages van de systeembeheerders blijkt, bevestigt dit de betrouwbaarheid van de systeembeheerders en hun rapportages.
Overigens zijn er ook serveroperatingsystemen die de logging inherent buiten beïnvloeding van de systeembeheerders kunnen houden, of die zelfs het superuserrecht voor de systeembeheerders niet nodig hebben. In voorkomende gevallen kunnen de zeer speciale gebruikersrechten met behulp van enveloppenprocedures, vierogenprincipe en dergelijke voldoende veilig worden gebruikt.

Onveilige clients
Dat de server wordt afgeschermd is des te meer nodig omdat de clients niet te vertrouwen zijn. Hiervoor werden al enkele fysieke beveiligingsaspecten van clients besproken. In logische zin zijn de typische clients echter ook slecht te beschermen. Zo is het beschermend vermogen van clients met alleen de bescherming van Windows '95 nihil. Ook andere 'beveiligingen' zoals screensaver-passwordbeveiliging zijn volstrekt onbetrouwbaar, enkele uitzonderingen daargelaten. En apart gebruikte authenticatiesoftware met PIN-pasjes en dergelijke is software als alle andere; exploiteerbare program-

meerfouten of ondeugdelijke versleutelingsalgoritmen komen daarin evengoed voor.

Opzet versus praktijk
Mocht dan een in opzet redelijk of goed stelsel van beveiligingsmaatregelen zijn gekozen, dan wil dat in de praktijk nogal eens in het slop raken. Helaas blijkt het nog steeds een uitzondering als de opzet én het bestaan van de beveiligingsmaatregelen in orde is. Met name een gebrek aan aandacht voor het bijhouden van allerlei wijzigingen in de techniek en, nog sneller wisselend, in de autorisatietabel die in de user accounts en rights wordt uitgedrukt, betekent vaak een beperking in de werking van het stelsel van beveiligingsmaatregelen.

Alerting
Een mogelijkheid die wel steeds meer opgeld doet, is de inschakeling van software die aparte signalen geeft indien er vooraf gedefinieerde gevaarlijke activiteiten worden uitgevoerd, of juist andersom, indien activiteiten worden uitgevoerd die niet expliciet vooraf veilig zijn verklaard. Dergelijke alertingsystemen leveren een behoorlijke bijdrage aan het in de greep houden van allerlei ongewenste activiteiten op clients en servers, al blijft er sprake van een potentieel gebrekkige of te omzeilen softwareoplossing.

Change management

Een zeer belangrijk onderdeel van de beveiliging, en al helemaal als het gaat om client-serveromgevingen die gebruikmaken van software die iedere programmeur kan aanpassen, is het voorkomen van onbeheerste aanpassingen in een in oorsprong veilige omgeving. De maatregelen daartoe zijn samen te vatten in de term change management.

Gescheiden omgevingen
Bij change management denkt men al snel aan het hanteren van gescheiden omgevingen voor ontwikkeling of installatie, test en acceptatie respectievelijk productie van systemen. Gescheiden omgevingen zijn vaak gerealiseerd met behulp van aparte subdirectories en daarmee zou het change management zijn geregeld.

In kleine systemen is het gebruik van aparte subdirectories ook inderdaad de oplossing om gescheiden systemen te krijgen (als men niet uit continuïteitsoverwegingen kiest voor het ontwikkelen en testen op een aparte computer), maar dat biedt geen bescherming tegen het buiten beeld van de ontwikkelaar of installateur wijzigen van allerlei parameterbestanden die voor de hele server gelden. Om nog maar te zwijgen van programmatuur die – zo bedoeld door een kwaadwillende programmeur of per ongeluk door per definitie voorkomende softwarefouten – direct tijdens of na de installatie door de grenzen van de subdirectories heenbreekt en bewust of onbewust in andere directories programmatuur of gegevensbestanden wijzigt. Vaak zal de installatiesoftware de programmatuur in vooraf bepaalde directories neerzetten; directories waar nu juist reeds de programmatuur in productie staat.

Bovendien is de installatie van programmatuur vanaf cd-rom's of zelfs vanaf het Internet hedentendage zo eenvoudig dat een gebruiker nauwelijks meer controle heeft op het installatieproces. Dat betekent dat de controle op de aanwezigheid van niet-toegestane software een steeds moeizamere aangelegenheid is.

Procedures
Behalve dit soort softwareproblemen bestaat change management ook uit een breed scala van administratieve beheersmaatregelen en -procedures. Die zijn van preventieve aard, zoals bijvoorbeeld test-, acceptatie- en overdrachtprocedures en het hanteren van richtlijnen inzake een verbod op installatie van illegale of van het Internet gekopieerde programmatuur, dan wel van repressieve aard, zoals controles op de programmatuur die op PC's aanwezig is. Deze laatste zijn overigens tegenwoordig met betrekkelijk eenvoudige hulpmiddelen ook op afstand uit te voeren; systeembeheerders kunnen met 'remote administration'-hulpmiddelen vanaf hun eigen werkplek een inventarisatie maken van de hardware en software die op een willekeurige PC aanwezig is. Mocht de zogenaamde agent-software op de PC zijn uitgeschakeld, dan is dat al een signaal op zich dat er op die PC iets onoorbaars aan de hand is.

In kleinere omgevingen is het verschil tussen onbelangrijke ingrepen en wezenlijke ingrepen (die qua schaal meestal ook vrij klein zullen zijn) vaak moeilijk te onderkennen. Het nut van het registreren van allerlei kleinere activiteiten lijkt dan te ontbreken, met als gevolg dat op enig moment geen overzicht van de uitgevoerde activiteiten voorhanden is.

Problem management
In wat grotere omgevingen bestaat er naast het change management ook het problem management. In kleinere omgevingen bestaan de bijbehorende taken ook wel degelijk, maar ze zijn dan niet zo expliciet onderscheiden als in grote omgevingen. En daar problem management uit de aard van de zaak vaak te maken heeft met snelle ingrepen in de systemen om acute problemen te kunnen oplossen, zullen de beheersbaarheid en controleerbaarheid van problem-managementgestuurde ingrepen in de systemen vaak slecht zijn.

Mocht het change management al helemaal beheerst worden met schriftelijk goed te keuren wijzigingsaanvragen en dergelijke, dan zullen ingrepen uit hoofde van problem management de effectiviteit van het change management vaak doorbreken. En het oplossen van acute gebruikersproblemen wordt door het management vaak – terecht – belangrijker gevonden dan het handhaven van de nogal eens wat bureaucratische wijzigingsformulierenstromen. Rapportage achteraf kan dan de consistentie en de volledigheid van registratie van de getroffen maatregelen en ingrepen waarborgen.

Testfouten
Als er al sprake is van gescheiden omgevingen, dient er natuurlijk voor fouten in de testprocedures te worden gewaakt. Daarbij valt te denken aan de volledigheid van de tests en aan testspecifieke modificaties aan de software.

De volledigheid van de tests is een moeilijk vast te stellen criterium. In de praktijk komt het nogal eens voor dat kleinere softwaresystemen weliswaar door gebruikers worden getest (bijvoorbeeld voor acceptatie), maar dat daarbij maar een beperkte verzameling testgevallen wordt doorlopen. Het is immers schier onmogelijk om alle denkbare in- en uitvoerscenario's op een gestructureerde wijze te testen en er wordt dan al snel teruggevallen op het doorlopen op een beperkt aantal 'gewone' testgevallen, een handvol vaak voorkomende afwijkingen en een paar speciale gevallen.
Bij gebrek aan gedetailleerde ontwikkelspecificaties waartegen de verzameling testgevallen kan worden gecontroleerd – het systeem was immers interactief ontwikkeld in overleg met de gebruiker? – zal men pas in het dagelijks gebruik allerlei fouten tegen komen. Dit overkomt overigens de besten; ook marktleidende softwareproducten zijn deels op deze wijze ontwikkeld en bevatten fouten doordat uitputtend testen niet mogelijk was. In kleinere organisaties is het echter zoveel moeilijker de tests goed uit te voeren dan bij de grote softwareleveranciers omdat eenvoudigweg de kennis en capaciteit ontbreekt.

De volledigheid van de tests is een moeilijk vast te stellen criterium.

Een tweede probleempunt bij testen is dat nogal eens modificaties worden gedaan aan de software in de testomgeving, omdat de testomgeving nu net op een aantal punten afwijkt van de productieomgeving waar de software voor bedoeld is. Bovendien is het helaas niet geheel ongebruikelijk dat allerlei verbandscontroles en controletotalen in de software voor het gemak van testen worden uitgeschakeld. In de testomgeving zijn die controles niet nuttig, de tester controleert de uitkomsten immers handmatig? Maar op die wijze controleert hij niet de controles, en het voorafgaand aan inproductiename weer inschakelen van de controles wordt wellicht vergeten.

De beheeractiviteiten rond informatietechnologie lijden aan hetzelfde euvel als de inrichting van de logische toegangsbeveiliging: doordat de organisatie altijd vertrouwde op onderlinge, vaak zeer informele, controles, is er vaak geen papieren vastlegging van de opzet van de beheeractiviteiten (procedures en richtlijnen). En als er al een opzet is, dan ontbreekt het vaak aan discipline om de audit trail van bijvoorbeeld change management adequaat bij te houden.

Aldus biedt het onderwerp change management voor de beveiliging van kleinere omgevingen een gemengd beeld. Enerzijds zijn er technische en praktische beheerproblemen, anderzijds zijn er technische hulpmiddelen die het beheer van alle deelsystemen terug kunnen brengen bij een centraal rekencentrumachtig organisatieonderdeel. De praktijk leert dat deze laatste mogelijkheid een aanzienlijke bijdrage kan leveren aan de informatiebeveiliging in brede zin.

CONTROLES ACHTERAF

Voor controles achteraf zijn twee stappen te onderscheiden: de registratie van het IT-bedrijfsgebeuren en de rapportage die daarover plaatsvindt.

Registratie

Voor wat betreft de registratie van het IT-bedrijfsgebeuren valt een onderscheid te maken naar de registraties in traditionele zin (de feitelijke vastlegging van het bedrijfsgebeuren) en de registraties inzake de geautomatiseerde activiteiten en de beheeractiviteiten daaromheen.
De feitelijke vastlegging van het bedrijfsgebeuren verschilt niet wezenlijk van die in grote omgevingen, zij het dat de verwerking in een client-serveromgeving vrijwel on line geschiedt. Hierdoor zullen voorraad(reserverings)standen en dergelijke veel actueler kunnen zijn. Anderzijds zijn de registraties eenvoudiger toegankelijk dan in grote omgevingen, met de risico's voor de integriteit van dien.

Autorisaties
Voor de registraties inzake de geautomatiseerde activiteiten geldt in principe hetzelfde. Van belang is hierbij met name dat de vastlegging van de autorisaties in de logische toegangsbeveiliging en het gebruik dat ervan wordt gemaakt, zijn terug te vinden in de loggings. De vastlegging van de autorisaties dient overigens op schrift te geschieden, opdat de feitelijke instellingen controleerbaar zijn tegenover een separate en vooraf geautoriseerde soll-positie.

In nogal wat kleinere omgevingen ontbreekt de discipline om dergelijke schriftelijke vastleggingen apart bij te houden. Als er al een beleid is te onderkennen, is dat vaak slechts na analyse van de feitelijke user rights in de systemen te achterhalen. Controle op de juistheid van dergelijke instellingen is dan meestal een globale beoordeling van de redelijkheid van de instellingen. Daarbij worden allerlei kennelijke dubbelfuncties voor lief genomen omdat het zo efficiënt is als de ene medewerker zonder meer het werk van de ander kan overnemen. Dat daarvoor aparte accounts kunnen worden gecreëerd, blijft meestal buiten beschouwing.

Loggings
In kleinere omgevingen ontbreekt het ook nogal eens aan kwalitatief voldoende loggings. Er worden bijvoorbeeld niet de juiste activiteiten gelogd of de loggings worden onvoldoende geïnspecteerd. Tezamen met het vaak onvoldoende beveiligen van de loggings (waardoor de juistheid en de volledigheid in het geding komen), mede bepaald door de soms onontkoombare toegang die systeembeheerders ertoe hebben, vermindert dit de waarde van de loggings als vastlegging van de geautomatiseerde activiteiten aanzienlijk. Dat terwijl met name client-serveromgevingen zodanig verspreid staan

opgesteld dat oogtoezicht op de activiteiten moeilijker is dan in bijvoorbeeld centrale omgevingen. Maar dat laat onverlet dat de loggings een waardevolle aanvulling zijn om de vele activiteiten die niet door een systeembeheerder worden uitgevoerd, in de gaten te houden.

De vraag om rapportage wordt vaak gezien als een gebrek aan vertrouwen. Hierdoor en door de inspanning die ervoor nodig is, bestaat een tegenzin tegen het afleggen van verantwoording over de uitgevoerde activiteiten. De verantwoording is echter ook een middel ter verkrijging van decharge. Mocht er iets misgaan in de systemen, dan kan aan de hand van rapportages worden aangetoond dat dat in ieder geval niet aan de systeembeheerders heeft gelegen. En zoals hierboven is uiteengezet, is het juist in client-serveromgevingen zeer wel mogelijk dat beschikbaarheids- en andere beveiligingsproblemen niet door de systeembeheerders worden veroorzaakt maar door derden, binnen of buiten de eigen organisatie.
In kleinere omgevingen blijft echter het nadeel bestaan dat de rapportages door systeembeheerders zelf worden opgesteld. De organisatie is vaak niet groot genoeg om (deeltijds) interne EDP-auditors in dienst te hebben en zal moeten terugvallen op externe EDP-auditors, gezien het belang van onafhankelijke controle.

AFSLUITEND

Het zal zaak zijn de risico's in voorkomende gevallen te inventariseren en alleen de maatregelen te nemen die gezien de risico's nodig zijn. Technische maatregelen als het volledig versleutelen van 'alle' berichtenverkeer zijn weliswaar effectief maar brengen aanzienlijke kosten met zich mee voor de aanschaf van de benodigde software en hardware door de vaak veel omvangrijkere en tragere datacommunicatie. De systemen in grote omgevingen zijn al hoogstzelden met alleen technische maatregelen af te dichten, en in client-serveromgevingen is dat vrijwel onmogelijk. Daarom zullen organisatorische maatregelen aanvulling moeten bieden.

Daarbij moet dan wel de onderlinge samenhang van de systemen, risico's en tegenmaatregelen in het oog worden gehouden. Het afschermen van zeer gevoelige applicaties heeft immers zo weinig zin als de data ertussen onveilig wordt getransporteerd over een openbaar netwerk als bijvoorbeeld het Internet.
Bovendien: alle beveiligingsmaatregelen worden aanzienlijk minder effectief als gebruikers slordig met informatie omgaan. Client-serveromgevingen met hun wijd verspreide, lees moeilijk in het oog te houden, gebruikers bieden al te veel mogelijkheden voor het bij printers laten slingeren van hoogst vertrouwelijke gegevens, het opslaan van gegevens die onder geen beding zouden mogen worden gestolen op floppies en dergelijke.

Kortom, er bestaan geen eenduidige, rechttoerechtaan oplossingen voor de beveiliging van client-serveromgevingen. Desondanks kan met een afgewogen verzameling organisatorische en technische maatregelen in het algemeen een redelijk niveau van beveiliging worden bereikt.

LITERATUUR

[Bron96] R.H.H.M. Bronzwaer, *Systeemsoftware onder controle*, Compact 96/3.

[Gast92] S.J. Gaston, *Managing and Controlling Small Computer Systems Including LANs*, The Canadian Institute of Chartered Accountants, 1992.

[Jenk92] B. Jenkins, P. Cooke en P. Quest, *An audit approach to computers*, The Institute of Chartered Accountants in England and Wales, London 1992.

[Koed96] M.J.A. Koedijk en W.A. de Munck, *System Review Services*, Compact 96/3.

Ir.drs. J. van der Vlugt
Is als EDP-auditor werkzaam bij KPMG EDP Auditors. Zijn aandachtsgebied ligt bij advies voor en audit van informatiebeveiligingsbeleid en de planning en beheersing van automatiseringsprojecten. Daarnaast heeft hij zich binnen de business unit Technical Auditing gespecialiseerd in de beveiliging en audit van Windows NT-systemen.

Informatietechnologie en management control in het algemeen en voor het MKB in het bijzonder

E.F. Heck RA,
mw. drs. M.J.A. Koedijk RA en
mw. W.A. de Munck RA

In het MKB is de management control van informatietechnologie nog niet zo ingeburgerd als bij grote organisaties. Ten onrechte, de voordelen van een management-controlraamwerk voor de beheerste inzet van informatietechnologie kunnen ook in het MKB worden behaald.

INLEIDING

Overal in het bedrijfsleven is de afgelopen jaren duidelijk geworden dat de informatietechnologie (IT) een onmisbare factor is geworden bij het realiseren van de bedrijfsdoelstellingen. Ook in het midden- en kleinbedrijf (MKB) raken de bedrijfsprocessen meer en meer verweven met informatietechnologie. Dat geldt niet langer alleen voor de informatieverzorgende (ondersteunende) processen, maar ook in toenemende mate voor de primaire processen, gericht op het leveren van producten of diensten. Dit impliceert dat het management van dergelijke organisaties een steeds groter belang heeft bij zekerheid omtrent het goed functioneren van informatietechnologie. Net als bij grote organisaties zal het management van MKB-bedrijven dus antwoord willen hebben op de vraag of de informatietechnologie:

- effectief is; in de zin dat zij voldoet aan de gebruikerseisen en -wensen en in voldoende mate de bedrijfsprocessen ondersteunt;
- efficiënt is; dat wil zeggen dat informatietechnologie bijdraagt aan het verkorten van doorlooptijden van processen, maar ook dat aan informatietechnologie zelf niet onnodig veel geld wordt uitgegeven;
- betrouwbaar is; als een belangrijke randvoorwaarde om bedrijfsprocessen effectief te kunnen ondersteunen. Geeft betrouwbaarheid het management de zekerheid dat de juiste beslissingen worden genomen?;
- zodanig is ingericht dat de continuïteit in voldoende mate is gewaarborgd, teneinde de zekerheid te hebben dat op korte en lange termijn de geautomatiseerde ondersteuning van processen beschikbaar blijft;
- zodanig is opgezet dat het systeem voldoet aan de verplichtingen welke voortvloeien uit de Wet persoonsregistraties (WPR) en de Wet computercriminaliteit (WCC).

Dit artikel geeft in algemene termen inzicht in de belangrijkste aspecten waaraan het management van MKB-organisaties bij het beantwoorden van deze vijf vragen aandacht moet schenken.
In dit artikel zal eerst in zijn algemeenheid worden ingegaan op de verschijningsvormen van informatietechnologie en management control. Vervolgens zal worden nagegaan wat de invloed van informatietechnologie in haar verschillende verschijningsvormen op het proces van management control is. In het bijzonder gaan wij daarna in op de specifieke MKB-aspecten in het geschetste kader. Tot slot schenken wij kort aandacht aan de rol van de accountant bij de jaarrekeningcontrole in de MKB-sector.

VERSCHIJNINGSVORMEN VAN IT

De afhankelijkheid van IT bij de ondersteuning van de bedrijfsprocessen varieert naargelang de wijze van inzet van IT. Analoog aan de verschijningsvormen van IT-projecten ([Donk95]) kunnen de volgende vier verschillende verschijningsvormen worden onderscheiden waarin IT de bedrijfsprocessen ondersteunt:
- IT als hulpmiddel;
- IT als beheersinstrument;
- IT als verbeteringsinstrument;
- IT als strategisch wapen.

IT als hulpmiddel
Bij deze vorm is er sprake van inzet van IT puur als hulpmiddel om bestaande simpele bedrijfsprocessen efficiënter te laten verlopen. Hierbij kan worden gedacht aan standaardsoftware zoals een losstaand financieel pakket, tekstverwerker en spreadsheets. In deze fase is veelal sprake van end-user-computing. Naarmate een onderneming groeit waarbij IT slechts als hulpmiddel wordt ingezet, wordt al snel duidelijk dat de mate waarin IT de bedrijfsprocessen ondersteunt niet meer effectief en efficiënt is en dat door het gebruik van end-user-computing de kans op fouten wordt vergroot.

IT als beheersinstrument
Door de groei van de onderneming en toenemende mate van flexibilisering worden bedrijfsprocessen complexer. Binnen de onderneming bestaat de behoefte om de informatievoorziening te verbeteren. In deze fase worden losse toepassingen op afdelingsniveau en soms ook al geïntegreerde systemen ontworpen en gerealiseerd.

IT als verbeteringsinstrument
Doelstelling van deze vorm is om met de mogelijkheden van IT de bestaande bedrijfsprocessen te verbeteren, te stroomlijnen of gedeeltelijk te herontwerpen. De behoefte om IT als verbeteringsinstrument in te zetten ontstaat als IT slechts was ingezet als beheersinstrument waarbij alleen is gefocust op verbetering van de informatievoorziening en niet zozeer op de verbetering van de bedrijfsprocessen.

IT als strategisch wapen
IT wordt ingezet als strategisch wapen wanneer bedrijven IT aangrijpen om de totale organisatie structureel te verbeteren en belangrijke concurrentievoordelen te behalen. Deze vorm ontstaat doordat de onderneming zich op strategisch niveau aan het heroriënteren is op de marktvraag, marktkansen en bedreigingen. Dit leidt vaak tot Business Process Redesign-projecten waarbij sterk rekening wordt gehouden met de mogelijkheid die het gebruik van IT biedt.

Zoals blijkt uit de bovenstaande verschijningsvormen zal een onderneming die IT als hulpmiddel gebruikt minder afhankelijk zijn van IT bij de sturing en beheersing van de bedrijfsuitoefening dan een onderneming die IT als strategisch wapen gebruikt. Een hoge mate van afhankelijkheid impliceert dat bij het beheersen van het bedrijfsproces een hoge mate van betrouwbaarheid, beschikbaarheid en effectiviteit van het geautomatiseerde systeem is vereist.

MANAGEMENT CONTROL

Om inzicht te krijgen in de wijze waarop het management bedrijfsprocessen beheerst en hoe IT hierop ingrijpt, wordt in deze paragraaf nader ingegaan op het begrip management control (de beheersingssystematiek). Allereerst is het van belang dat een organisatie in de tijd wordt beheerst. Deze beheersing vindt plaats op basis van de management-controlcyclus. Daarnaast is het van belang inzicht te hebben in de vraag welke processen in een organisatie beheerst moeten worden en wat daarbij de aandachtsgebieden zijn. Tot slot zal worden nagegaan welke mechanismen, componenten of hulpmiddelen nodig zijn om management control te kunnen uitvoeren.

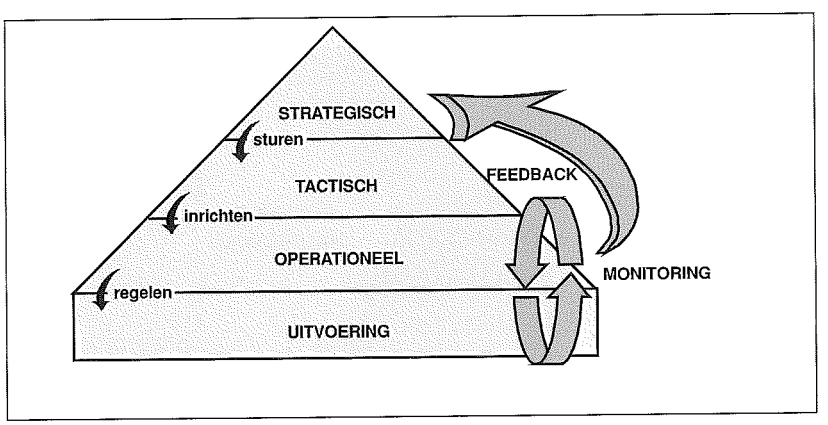
Management-controlcyclus

Om een proces in de tijd te kunnen beheersen moet een aantal fasen worden doorlopen. In de procestechnologie wordt hiervoor een vaste cyclus gebruikt. Deze cyclus komt neer op het formuleren van een norm, sturen van het proces naar die norm, waarnemen en zo nodig bijsturen of corrigeren. Deze cyclus is iteratief aangezien het continue proces door de omgeving kan veranderen. Tijdens het proces zal continu getoetst moeten worden of de norm moet worden aangepast of dat het proces moet worden bijgestuurd.

Deze cyclus wordt wel aangeduid als management-controlcyclus (figuur 1). De belangrijkste instrumenten van de management-controlcyclus zijn beleid, sturing, uitvoering, monitoring en feedback. Het beleid geeft hier de kaders aan. De instrumenten sturing, monitoring en feedback zorgen ervoor dat de uitvoering van de bedrijfsprocessen binnen deze kaders plaatsvindt.

Gebieden van management control

Zoals uit voorgaande paragraaf blijkt vindt beheersing van de bedrijfsprocessen in de tijd plaats op basis van het doorlopen van de management-controlcyclus. Deze cyclus wordt voor alle bedrijfs-



Figuur 1. Management-controlcyclus.

processen doorlopen. Dus zowel voor de primaire bedrijfsprocessen zoals bijvoorbeeld inkoop, productie en verkoop als voor de ondersteunende bedrijfsprocessen zoals administratie. Binnen deze bedrijfsprocessen zijn er enkele aandachtsgebieden die beheerst moeten worden. In het COSO-onderzoek ([COSO92]) zijn deze management-controlgebieden vastgesteld aan de hand van discussies, brainstormsessies en dergelijke met onder meer managers van vooraanstaande ondernemingen en andere externe belanghebbenden.

In het COSO-rapport worden de volgende management-controlgebieden onderscheiden:
- de effectiviteit en efficiëntie van de bedrijfsprocessen;
- de betrouwbaarheid van de financiële gegevens;
- de naleving van de wetten en regelgeving.

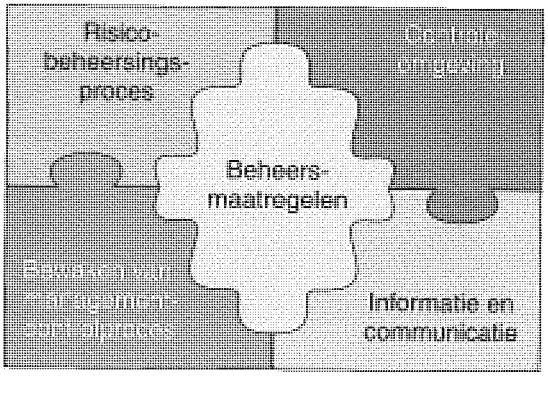
Hiervan afgeleid kan de beheersing over deze gebieden worden omschreven als:
- operational control;
- financial control;
- compliance control.

In dit kader is management control dan te omschrijven als het totaal van operational, financial en compliance control over *alle* bedrijfsprocessen.

Componenten van management control

Het management beschikt over een vijftal onderling gerelateerde componenten voor het beheersen van de bedrijfsprocessen, welke met behulp van de zojuist beschreven instrumenten in de management-controlcyclus zijn geïntegreerd. Afhankelijk van allerlei factoren zoals de grootte, het type en de cultuur van het bedrijf en de stijl van leidinggeven worden deze componenten door het management ingezet. De componenten van management control zijn:
- controleomgeving;
- risicobeheersingsproces;
- informatie en communicatie;
- bewaken van het management-controlproces;
- beheersmaatregelen.

De componenten van management control zijn onderling nauw verweven en vormen samen een geïntegreerd systeem. De componenten kunnen elkaar aanvullen, versterken, compenseren of verzwakken. Voor de beoordeling van de kwaliteit van de management control zullen de componenten dan ook in relatie tot elkaar moeten worden beoordeeld.
De componenten worden hieronder kort toegelicht.



Figuur 2. De componenten van management control ([KPMG1]).

Controleomgeving
De controleomgeving omvat het geheel van factoren die de werksfeer en cultuur binnen een organisatie bepalen en daarmee de controlebewustheid van de mensen binnen de organisatie. Het gaat hier om integriteit en ethische waarden, de mentaliteit en wijze van optreden van de ondernemingsleiding, bekwaamheden van het personeel, wijze van delegatie van verantwoordelijkheden en bevoegdheden, het personeelsbeleid en dergelijke. De controleomgeving vormt de grondslag voor de andere componenten van management control, omdat deze component bepaalt of personeel en management hun verantwoordelijkheden ten aanzien van de beheersmaatregelen nakomen.

Risicobeheersingsproces
Onder risicobeheersingsproces wordt verstaan de wijze waarop het management zijn ondernemingsdoelstellingen bepaalt en daarnaast vaststelt welke risico's het behalen van deze doelstellingen bedreigen, teneinde adequate maatregelen te kunnen treffen om deze risico's te beheersen (indien gewenst). Het risicobeheersingsproces moet ervoor zorgen dat noodzakelijke beheersmaatregelen op het gebied van betrouwbaarheid, effectiviteit, efficiëntie en wet- en regelgeving worden getroffen.

Informatie en communicatie
Van belang is dat de informatie- en communicatiesystemen leiden tot adequate operationele en financiële informatievoorziening. De informatievoorziening moet toereikend, tijdig en dusdanig gedetailleerd zijn dat de mensen binnen een organisatie in staat zijn hun verantwoordelijkheden te dragen. De effectiviteit van sturing, monitoring en feedback van de management-controlcyclus is in belangrijke mate afhankelijk van de kwaliteit van deze component.

Bewaken van het management-controlproces
Bewaking van het management-controlproces is erop gericht de werking van de beheersmaatregelen in de tijd vast te stellen. De bewaking kan geschieden in de vorm van permanente activiteiten als onderdeel van de bedrijfsprocessen, afzonderlijke activiteiten of een combinatie van beide.

Beheersmaatregelen (de specifieke beheersmaatregelen)
Bij de specifieke beheersmaatregelen gaat het om de uitvoering van voorschriften en maatregelen die zekerheid verschaffen dat de richtlijnen van de leiding worden opgevolgd en dat de nodige acties worden ondernomen ter beheersing van de risico's die het bereiken van de doelstellingen van de organisatie in gevaar brengen. Specifieke beheersmaatregelen worden op alle niveaus en in alle functies binnen de organisatie verricht.

De componenten controleomgeving, risicobeheersingsproces, informatie en communicatie en het bewaken van het management-controlproces scheppen het kader waarbinnen de specifieke be-

heersmaatregelen (de vijfde component) adequaat kunnen functioneren. Zie figuur 2, waarin de onderlinge relatie in de vorm van een puzzel is weergegeven. Dit kader wordt ook wel omschreven als de algemene beheersmaatregelen, omdat deze maatregelen niet gerelateerd zijn aan één transactiesoort en/of ondernemingsdoelstelling.

MANAGEMENT CONTROL EN IT

In deze paragraaf wordt aangegeven hoe de IT ingrijpt op de eerder geschetste invalshoek van management control.

De invloed van IT op de gebieden van management control

Om de IT te kunnen gebruiken bij de beheersing van de bedrijfsprocessen (management control) is het een voorwaarde dat het management van IT adequaat is geregeld. In deze paragaaf wordt besproken welke invloed IT heeft op de beheersing van de drie gebieden van management control. Vervolgens wordt nagegaan hoe de IT in deze deelgebieden kan worden beheerst.

Operational control
Bij operational control gaat het om het beheersen van de effectiviteit en efficiëntie van de bedrijfsprocessen. IT zal hierbij een belangrijke rol spelen. Wanneer we naar een willekeurige levenscyclus van een onderneming kijken, zullen de bedrijfsprocessen bij de 'geboorte' eerst handmatig dan wel door middel van het inzetten van IT 'als hulpmiddel' worden bewaakt. Voorlopig zijn de processen op die wijze te beheersen zolang de onderneming niet te onstuimig groeit. Na enige tijd blijken de processen niet meer efficiënt en effectief te werken. IT wordt nu gebruikt om naast de ondersteunende processen ook alle of delen van de primaire processen te ondersteunen. IT wordt in deze situatie ingezet als beheersinstrument, en IT en processen raken steeds meer verweven. Gevolg van deze inzet is dat ook de aan IT te stellen eisen zwaarder zullen worden. De onderneming groeit vervolgens door, waarbij IT en andere processen langzaam worden uitgebouwd en aan elkaar gekoppeld. Er ontstaat in een snel veranderende omgeving een situatie waarbij verschillende hard- en softwarecomponenten met verschillende leeftijden en uiteenlopende kwaliteiten in verschillende bedrijfsprocessen aan elkaar zijn gekoppeld. De processen blijken niet meer efficiënt en effectief te worden ondersteund door IT. In deze situatie zal het management de IT aangrijpen om de bedrijfsprocessen te verbeteren. Tot slot zal de onderneming in de fase die gericht is op schaalvergroting of conglomeraatvorming IT strategisch inzetten om de beoogde synergievoordelen te kunnen behalen.
Vanzelfsprekend zullen de algemene eisen die aan IT gesteld kunnen worden zwaarder zijn in een volgende levensfase.

Financial control
Bij financial control gaat het om de beheersing van de betrouwbaarheid van de financiële verslaggeving. Ook hier zullen de verschijningsvorm van IT en de aan IT te stellen algemene en specifieke eisen afhankelijk zijn van de levensfase van de onderneming. Overigens hoeft de verschijningsvorm niet parallel te lopen met die van operational of compliance control.

Bij compliance control speelt IT slechts een beperkte ondersteunende rol.

De betrouwbaarheid van de financiële verslaggeving zal in het algemeen worden beheerst door het samenspel van algemene computercontroles en toepassingscontroles, welke in de volgende subparagraaf nader worden toegelicht.

Compliance control
Hieronder wordt verstaan de beheersing van de bedrijfsprocessen gericht op de naleving van de geldende wet- en regelgeving. IT speelt, zoals in de voorgaande paragrafen uiteen is gezet, een belangrijke rol bij de operational en financial control. Computercontroles kunnen echter niet zorgen voor het goed functioneren van compliance control. Zo zal bijvoorbeeld de toets of een jaarrekening is opgesteld conform Titel 9 BW2 niet door geprogrammeerde controles kunnen worden uitgevoerd. Hiervoor is het zogenaamde professional judgement vereist van een bekwaam persoon. IT speelt wel een beperkte ondersteunende rol bij compliance control. Zo zijn er bijvoorbeeld in de accountantscontrole geautomatiseerde checklists voor toetsing van jaarrekeningen aan de wettelijke bepalingen. Daarnaast is de wet- en regelgeving veelal beschikbaar via cd-roms of een intranet. Overigens heeft IT wel een aantal raakvlakken die van belang zijn voor compliance. Hierbij kan gedacht worden aan regelgeving op het gebied van Electronic Data Interchange (EDI), juridische aspecten rondom het digitaliseren van ondernemingsarchieven, de Wet persoonsregistraties (WPR) en de Wet computercriminaliteit (WCC).

De invloed van IT op de componenten van management control

De inzet van IT, in welke verschijningsvorm dan ook, heeft invloed op de beheersing van een onderneming. IT wordt ingezet om ondernemingsdoelstellingen te realiseren en zal het beheersingsproces ondersteunen, maar moet zelf ook beheerst worden. De trend dat Administratieve Organisatie (AO) en IT worden geïntegreerd, versterkt dit aspect in belangrijke mate. In deze subparagraaf wordt per component van management control kort gekenschetst wat de invloed van IT daarop is.

Controleomgeving
Zoals is gebleken uit de omschrijving van deze component in de vorige paragraaf zal IT geen invloed hebben op de controleomgeving, omdat deze component voortkomt uit de normen en waarden die binnen het bedrijf aanwezig zijn. De controleomgeving heeft duidelijk wel invloed op de uitvoe-

Figuur 3. Afhankelijkheids-analyse.

Bedrijfsproces	Informatiesysteem	Betrouwbaarheid	Beschikbaarheid	Effectiviteit
Verkopen	Sales	Hoog	Hoog	Hoog
Salarissen	Pers	Hoog	Laag	Laag
Inkopen	Purch	Hoog	Gemiddeld	Gemiddeld

ring van de op IT-gebied getroffen beheersmaatregelen. Op IT-gebied zijn in dit kader bekende voorbeelden de omgang met wachtwoorden, de backupdiscipline van de gebruikers, verbod op gebruik van illegale software en viruspreventie. In de accountantscontrolepraktijk worden deze voorbeelden vaak gebruikt als indicatoren voor de controleomgeving binnen een onderneming.

Informatie en communicatie
De invloed van IT op deze component is natuurlijk groot. IT richt zich immers bij uitstek op de informatieverwerking en communicatie. De inzet van IT zal in belangrijke mate bepalen in hoeverre het management succesvol zal zijn in het realiseren van de beheersing van de drie management-controlgebieden.

Risicobeheersingsproces
Bij het risicobeheersingsproces dient aandacht te worden geschonken aan de bedreigingen ten aanzien van de ondernemingsdoelstellingen die voortkomen uit het gebruik van IT, zodat beheersmaatregelen kunnen worden getroffen om deze risico's te ondervangen. Het is immers zo dat uitval van de systemen, het in ongerede raken van gegevensbestanden of het door onbevoegden kennis nemen dan wel manipuleren van bepaalde gegevens ernstige gevolgen kan hebben voor de bedrijfsvoering.

De te onderkennen risico's zijn, zoals gesteld, afhankelijk van de wijze van inzet (verschijningsvorm) van IT. Van belang is dat het management een afhankelijkheidsanalyse (figuur 3) uitvoert gericht op de betrouwbaarheid, de beschikbaarheid (continuïteit) en effectiviteit ([Munc95]). Aspecten die daarbij een rol spelen zijn:
- het belang van IT voor de bedrijfsvoering;
- de omvang van de organisatie;
- de complexiteit van IT;
- de aard van de aanwezige processen.

Als de geanalyseerde gebieden sterk van de IT afhankelijk zijn, zullen de te treffen beheersmaatregelen in en rondom IT (de zogenaamde computercontroles) ook van een hoog niveau moeten zijn. Het is niet zo dat als de afhankelijkheid laag is, geen beheersmaatregelen getroffen hoeven te worden. De afhankelijkheidsanalyse zegt iets over het niveau van de te treffen maatregelen. Dezelfde bedreigingen blijven immers bestaan, maar de omvang van de gevolgen voor de onderneming is kleiner.

Bewaken van het management-controlproces
Het gebruik van IT verandert het principe van het bewakingsproces niet. Het is wel mogelijk dat IT als hulpmiddel wordt ingezet. Van belang is dat het management bij het inrichten van het bewakingsproces rekening houdt met IT-aspecten. Dit impliceert dat het topmanagement adequaat moet worden geïnformeerd.

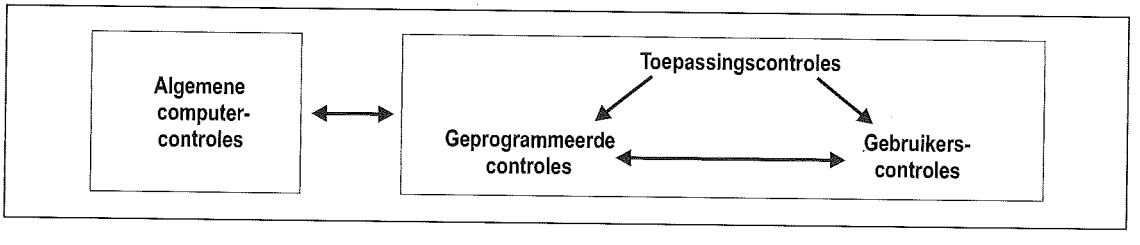
Beheersmaatregelen
Zoals reeds gesteld zal het management beheersmaatregelen invoeren die gerelateerd zijn aan operational, financial en compliance control. In verband hiermee is het management ook genoodzaakt beheersmaatregelen in te voeren die gebaseerd zijn op de specifieke risico's van IT, welke zijn onderkend bij de risicoanalyse.

De risico's op het gebied van de informatie- en communicatiesystemen worden beheerst door computercontroles met een algemeen karakter (algemene computercontroles) en computercontroles die zich richten op een specifieke applicatie, de zogenaamde toepassingscontroles. Deze toepassingscontroles bestaan uit zowel geprogrammeerde als gebruikerscontroles (figuur 4) ([Munc95]).

De algemene computercontroles zijn onder te verdelen in de volgende onderwerpen:
- beleid en management;
- functiescheidingen;
- logische toegangsbeveiliging;
- fysieke toegangsbeveiliging;
- systeemontwikkeling, onderhoud- en/of pakketselectieprocedures;
- continuïteit;
- systeembeheer- en productieprocedures;
- gebruikerssatisfactie.

De algemene computercontroles scheppen het kader dat moet zorgen dat de toepassingscontroles effectief worden opgezet en dat de werking in de tijd

Figuur 4. Computercontroles.



van de geprogrammeerde toepassingscontroles wordt gerealiseerd. De goede werking van de geprogrammeerde controles in een applicatie is bijvoorbeeld afhankelijk van de kwaliteit van de test-, acceptatie- en overdrachtsprocedures, die onderdeel zijn van de algemene computercontroles.

Gerelateerd aan de uitkomsten van de afhankelijkheidsanalyse (en daarmee de inzet van IT) en de mogelijkheden binnen de organisatie zal het management de algemene computercontroles opzetten.

MKB EN IT

De inzet van IT in het MKB kent zijn eigen karakteristieken.

Kenmerken management control in MKB

Als het management-controlproces van het MKB wordt vergeleken met dat van grotere ondernemingen worden vaak de volgende verschillen genoemd:

- In het MKB zal in het algemeen sprake zijn van minder geformaliseerde procedures (niet vastgelegd bijvoorbeeld in een handboek, geen vastlegging van uitvoering).

- Het contact van het management met het personeel is veel directer en informeler (oogtoezicht, snellere communicatie).

Wij willen benadrukken (net zoals in het COSO-rapport is gedaan [Maij97]) dat ondanks de minder geformaliseerde organisatie in het MKB, het management-controlproces niet minder effectief hoeft te zijn! Het gaat tenslotte om de aanwezigheid van de management-controlcyclus en het daadwerkelijk uitvoeren van algemene en specifieke beheersmaatregelen, niet om de formele vastlegging daarvan.

IT-kenmerken en risico's MKB

Het artikel van Van Praat in deze Compact gaat in op de typologie van de kleinschalige automatiseringsomgeving. Hij richt zich daarbij op de technische ontwikkelingen en de daaraan gerelateerde mogelijkheden op het gebied van beheersing. In het kader van dit artikel wordt onder een kleinschalige automatiseringsomgeving verstaan die omgeving waar geen functiescheiding bestaat tussen de gebruikersorganisatie en de automatiseringsorganisatie, dan wel die omgeving waar binnen de automatiseringsorganisatie geen effectieve functiescheidingen bestaan ([KPMG2]). In dit kader wordt gesproken over geen verbijzonderde automatiseringsorganisatie, respectievelijk verbijzonderde automatiseringsorganisatie. Hieronder wordt nader op deze situaties ingegaan.

Verbijzonderde automatiseringsorganisatie
In deze situatie is een beperkt aantal functionarissen vrijgemaakt om te zorgen dat de gebruikte computerapparatuur, systeemsoftware en de toepassingsprogramma's voor de gebruikers beschikbaar zijn en blijven. De nadruk van de werkzaamheden zal liggen op de bediening van de apparatuur, het maken van overzichten en bestandsselecties, het maken van incasso- of betaaltapes en het maken van back-ups. In uitzonderingsgevallen zal ook sprake zijn van het ontwikkelen en onderhouden van toepassingsprogramma's.

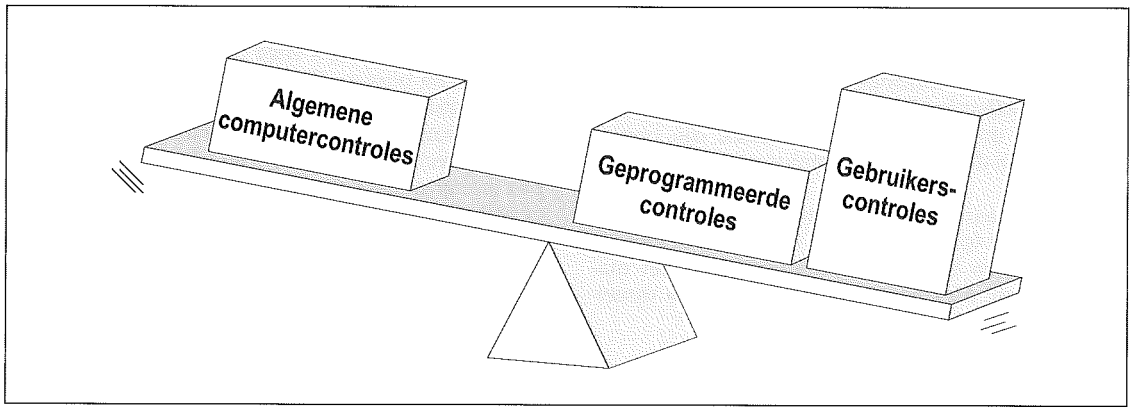
De organisatie kent een specifiek continuïteitsrisico als gedetailleerde kennis van de automatiseringsomgeving slechts bij een enkele functionaris bekend is.

Binnen deze automatiseringsorganisatie bestaat veelal geen functiescheiding, zelfs niet wanneer sprake is van meerdere functionarissen. Deze functionarissen zijn meestal in staat elkaars werk over te nemen, kennen elkaars password en vervangen elkaar bij afwezigheid. Er bestaat in deze situatie wel functiescheiding tussen de gebruikersorganisatie en de automatiseringsorganisatie.

Het ontbreken van functiescheiding binnen de automatiseringsorganisatie vergroot de volgende risico's:
- het risico op ongeautoriseerde wijzigingen in de programma's, hetgeen wordt versterkt indien sprake is van zelf ontwikkelde software;
- het risico op ongeautoriseerde wijzigingen in de gegevens.

Om deze risico's te beheersen of in ieder geval tot een minimum te beperken zal het management van de organisatie aanvullende maatregelen moeten nemen. Extra maatregelen moeten zeker worden getroffen rondom fraudegevoelige processen, zoals bijvoorbeeld betalingen.
Naast bovenstaande risico's bestaat ook een specifiek continuïteitsrisico voor de organisatie als gedetailleerde kennis van de automatiseringsomgeving slechts bij een enkele functionaris bekend is. Tot slot zal het management zich moeten realiseren dat de automatiseringsfunctionaris toegang heeft tot alle gegevens, waaronder waarschijnlijk ook vertrouwelijke gegevens.

Geen verbijzonderde automatiseringsorganisatie
Indien de werkzaamheden zodanig beperkt zijn dat verbijzondering niet zinvol is, wordt de automatiseringsfunctie ondergebracht bij gebruikers, vaak als een nevenfunctie. Veelal wordt in deze situatie gebruikgemaakt van (eenvoudige) standaardsoftware en computerapparatuur.
Doordat in deze situatie behalve de functiescheiding binnen de automatiseringsorganisatie ook de functiescheiding tussen de gebruikersorganisatie en de automatiseringsorganisatie ontbreekt, worden de in de vorige subparagraaf onderkende risico's versterkt.



Figuur 5. Computercontroles bij het MKB.

Karakteristieken kleinschalige automatiseringsomgeving
Uit bovenstaande blijkt dat in dit artikel het onderwerp derhalve wordt benaderd vanuit de organisatorische en daarmee de beheersmatige kant; de gebruikte computerapparatuur wordt in dit kader minder relevant gevonden. Aanvullend op bovenstaande definitie kent een kleinschalige automatiseringsomgeving vaak de volgende karakteristieken ([KPMG3]):
- beperkte automatiseringskennis;
- gebruik van standaardsoftware;
- gebruik van eenvoudige hardware zoals PC's, mini- of midrangecomputer.

Beperkte automatiseringskennis
In kleinschalige automatiseringsomgevingen kan sprake zijn van een beperkte kennis van automatisering bij de gebruikers en/of automatiseringsfunctionarissen. Dit kan een risico betekenen bij de aanschaf of het ontwikkelen van nieuwe programmatuur. Door onvoldoende kennis en ervaring bestaat het risico dat deze programmatuur niet voldoet aan de doelstellingen en eisen van het management en de gebruikers. Ook bestaat het risico dat nieuwe programmatuur of versies van programmatuur niet goed worden getest, zodat problemen pas worden gesignaleerd als de programmatuur al in productie is (met alle gevolgen van dien).

De beperkte kennis van de gebruikers en/of automatiseringsfunctionarissen kan het risico op ongeautoriseerde wijzigingen verkleinen.

De beperkte kennis van gebruikers kan tot gevolg hebben dat sommige handmatige gebruikerscontroles niet adequaat blijken te zijn. Hierbij kan gedacht worden aan de beoordeling van loggings en dergelijke verslagen. Overigens kan de beperkte kennis van de gebruikers en/of automatiseringsfunctionarissen het risico op ongeautoriseerde wijzigingen verkleinen!

Gebrek aan kennis kan ook betrekking hebben op de gebruikte (standaard)software, bijvoorbeeld ten aanzien van de rapporteringsmogelijkheden. Dit kan in de gebruikersorganisatie leiden tot het zelf ontwikkelen van toepassingen, bijvoorbeeld met beschikbare spreadsheet- en databaseprogramma's: end-user-computing. De in dit kader onderkende risico's van end-user-computing zijn:
- de gehanteerde gegevens zijn verouderd of niet juist;
- de zelf ontwikkelde applicatie bevat fouten, waardoor de uitkomst niet juist is;
- gebrek aan documentatie van de zelf ontwikkelde applicatie;
- gebrek aan back-upmaatregelen.

Het management dient zich bewust te zijn van de risico's en indien noodzakelijk passende maatregelen te nemen. Denk hierbij aan scholing, aanwenden externe kennis en formele procedures ten aanzien van end-user-computing.

Gebruik van standaardsoftware
Het gebruik van standaardsoftware zorgt dat het risico op ongeautoriseerde wijzigingen in de applicatie wordt beperkt. Veelal is de sourcecode niet of althans niet op de productiemachine aanwezig. Het risico op ongeautoriseerde wijzigingen in de gegevens blijft daarentegen bestaan.

Doordat ontwikkeling niet plaatsvindt binnen de automatiseringsorganisatie maar door derden, ontstaat functiescheiding tussen ontwikkeling en productie. Van belang blijft evenwel dat goede acceptatie-, test- en overdrachtprocedures plaatsvinden, niet alleen bij de aanschaf en ingebruikneming van de standaardsoftware maar bij iedere nieuwe versie.

Een bijzonder punt van aandacht bij het gebruik van standaardsoftware is de continuïteit van de softwareleverancier, omdat de onderneming in zekere mate afhankelijk zal zijn van deze leverancier.

Gebruik van mini- of midrangecomputer
In zijn algemeenheid kan gesteld worden dat de kwaliteit van de computerapparatuur en systeemsoftware zodanig is dat een voldoende beveiligingsniveau is te realiseren, zelfs als gebruik wordt gemaakt van een PC/serveromgeving. Van belang is wel dat de benodigde kennis om zorg te dragen voor een adequate beveiliging aanwezig is binnen de onderneming en als dit niet het geval is dat deze kennis via externen wordt verkregen.

In een kleinschalige automatiseringsorganisatie be-

staat de mogelijkheid dat de locatie van de computerapparatuur zich in de gebruikersorganisatie bevindt. Dit betekent een verhoogd risico ten aanzien van de continuïteit van de werking van de apparatuur.

Kenmerken computercontroles in MKB

Het is niet altijd rendabel voor een bedrijf om de algemene computercontroles maximaal in te richten, bijvoorbeeld vanwege beperkte omvang, beperkte afhankelijkheid of uit efficiëntieoverwegingen. Om dit te compenseren zal het management aanvullende (andere) maatregelen moeten treffen en dus de toepassingscontroles zwaarder moeten inrichten. In het MKB is dat veelal van toepassing doordat de inrichting van de automatiseringsorganisatie is beperkt.

De toepassingscontroles zijn, zoals reeds beschreven, te splitsen in geprogrammeerde controles en gebruikerscontroles. Voor de werking van de geprogrammeerde controles in de tijd is een minimumniveau van inrichting van de algemene computercontroles een voorwaarde (denk bijvoorbeeld aan test-, acceptatie- en overdrachtsprocedures). Hoe beter de algemene computercontroles, hoe meer het management impliciet kan steunen op de werking van de programmatuur en daarmee op de geprogrammeerde controles, waardoor de omvang van de gebruikerscontroles kan afnemen.

Daar de inrichting van de automatiseringsorganisatie binnen het MKB meestal minimaal is, zal het accent liggen op de gebruikerscontroles als de meest effectieve beheersmaatregel. Zij moeten zodanig zijn ingericht dat zij in samenspel met de geprogrammeerde controles voldoende zekerheid geven over de betrouwbare werking van de programmatuur en de integriteit van de gegevens. De verhouding tussen de computercontroles binnen het MKB is in figuur 5 weergegeven.

SAMENVATTING EN IMPLICATIE VOOR DE JAARREKENINGCONTROLE

Dit artikel betoogt dat de beheersing van IT in het MKB bevredigend kan worden geregeld. Het management zal zich rekenschap moeten geven van de invloed van IT op alle vijf management-controlcomponenten en de inrichting van het management-controlsysteem moeten laten aansluiten op de wijze waarop IT is ingezet in de organisatie.

De beoordeling van de wijze waarop het management van een onderneming de risico's met betrekking tot IT beheerst, is van toenemend belang. Door die beoordeling kan de accountant zich een indruk vormen over de kwaliteit van de IT en op grond daarvan een betere invulling geven aan de controle van de jaarrekening en de klankbordfunctie voor het management ([Munc95]). De accountant zal ook bij het MKB aan het proces van management control, de componenten en de getroffen beheersmaatregelen controlezekerheid kunnen ontlenen.

De verwachting is dat de accountant in de toekomst verplicht wordt, in navolging van een aantal andere landen, te rapporteren over de kwaliteit van het management-controlsysteem.

LITERATUUR

[Donk95] J.A.M. Donkers, M. Groesz RE, ir. J.A. Verstelle, *Informatietechnologie, Management control van de geautomatiseerde omgeving*, Controlling in de praktijk nr. 11, Kluwer, Deventer 1995.

[Munc95] W.A. de Munck RA, *Informatietechnologie als beoordelingsobject in de hedendaagse controlebenadering*, Compact 1995/3.

[COSO92] COSO, Committee of Sponsoring of the Treadway Commission, *Internal Control Integrated Framework*, AIPCA, Jersey City, 1992.

[Maij97] S.J. Maijoor, *Corporate governance, internal control en het midden- en kleinbedrijf*, Accountant-Adviseur, nr. 1/2, p. 11-15, januari/februari 1997.

[KPMG1] KPMG Cursus Module 5/6.

[KPMG2] KPMG AKSO; Cursus Automatisering Kleinschalige Ondernemingen.

[KPMG3] KPMG Peat Marwick and the Royal Hong Kong Police Crime Prevention Bureau, *Computer Security for users of small computer systems.*

[KPMG4] KPMG Handboek KAS.

E.F. Heck RA, mw. drs. M.J.A. Koedijk RA en mw. W.A. de Munck RA zijn allen werkzaam op (senior) managersniveau in de business unit Informatie Technologie en Accountantscontrole (ITAC) van KPMG EDP Auditors. Hun werkveld beslaat met name EDP-auditwerkzaamheden in het kader van de jaarrekeningcontrole zoals systeembeoordelingen, afhankelijkheidsanalyses, benchmarking IT controls en ondersteunende werkzaamheden ten behoeve van de automatiseringsparagraaf van de adviesbrief. Zij zijn mede actief in de ontwikkeling van methoden, producten en trainingen op het gebied van EDP-audit die gebruikt kunnen worden in het kader van de jaarrekeningcontrole. De heer Heck werkt daarnaast nog deeltijds in de controlepraktijk.

Elektronisch bankieren in het MKB

Drs. R. Oudega RE en mw. M. Pieper

Om bij het toepassen van elektronisch bankieren het betalingsproces in de hand te kunnen houden is een aantal beheersmaatregelen te implementeren. Het proces wordt stap voor stap doorlopen en de attentiepunten worden aangegeven. Hierbij wordt rekening gehouden met de beperkingen die een kleine organisatie met zich meebrengt.

INLEIDING

Nagenoeg alle organisaties beschikken over één of meer vormen van elektronische betaalsystemen. Met name de efficiency en de effectiviteit van het betalingsproces zijn belangrijke argumenten om tot deze meer moderne vormen van betalen over te gaan. Er zijn verschillende verschijningsvormen van elektronische betaalsystemen die momenteel naast elkaar worden aangetroffen. Voor grote aantallen betalingen wordt veel gebruikgemaakt van diskette, tape of cartridge. De betalingen worden in elektronische vorm op het gekozen medium geplaatst en met begeleidingsformulier verzonden aan de juiste instelling. Het begeleidingsformulier bevat informatie over onder meer het aantal betalingen en de bijbehorende bedragen en is voorzien van de benodigde handtekeningen en controletotalen. Hiermee dient dit formulier als autorisatie door de opdrachtgever van de betalingsopdrachten op het desbetreffende medium.

Steeds vaker worden de betalingsopdrachten niet meer op diskette, tape of cartridge geplaatst maar door middel van datacommunicatie verzonden naar de juiste instelling. Hierbij is nog steeds sprake van het fysiek verzenden van een begeleidingsformulier. Het gebruik van een elektronisch bankiersysteem is een derde verschijningsvorm die bij zeer veel organisaties wordt aangetroffen. Met behulp van een door de bank aangeboden systeem worden betalingsopdrachten via datacommunicatie verzonden, waarbij ook de procuratie (het begeleidingsformulier) op elektronische wijze wordt uitgevoerd. Daarnaast worden met deze systemen ook andere functies uitgevoerd, zoals het opvragen van rekeninginformatie en cash-managementactiviteiten.

Het betalingsproces is gevoelig voor fouten en malversaties. Organisaties zullen vooral preventieve maatregelen treffen om te voorkomen dat betalingen ten onrechte worden uitgevoerd. De introductie van elektronische betaalsystemen vraagt om passende maatregelen ter beheersing van de risico's. In dit artikel wordt aan de hand van een uitwerking van de toepassing van elektronische bankiersystemen allereerst het proces nader uitgewerkt. Vervolgens wordt een algemeen normenkader gepresenteerd voor het realiseren van een betrouwbaar betalingsverkeer met behulp van een elektronisch bankiersysteem. Aan de hand van dit normenkader wordt nader geanalyseerd op welke wijze een kleinere organisatie betrouwbaar betalingsverkeer kan realiseren.

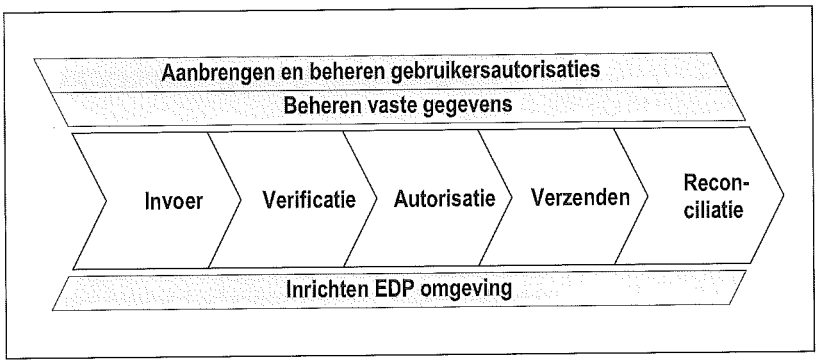
HET ELEKTRONISCH BANKIERPROCES

In deze paragraaf wordt het betalingsproces met behulp van een elektronisch bankiersysteem nader uitgewerkt. Deze uitwerking is de basis voor de analyse die in dit artikel verder wordt uitgevoerd. Het elektronisch bankierproces is in figuur 1 schematisch weergegeven. Dit schema geeft inzicht in de primaire en secundaire activiteiten die de organisatie dient uit te voeren.

Aanbrengen en beheren gebruikersautorisaties
Functiescheiding speelt een zeer belangrijke rol bij de beheersing van de risico's die samenhangen met het betalingsverkeer. De functies die het elektronisch bankiersysteem biedt, zoals invoeren van betaalopdrachten, opvragen van gegevens en verzenden van betalingsopdrachten, worden zodanig toegekend aan de verschillende gebruikers dat de beoogde controletechnische functiescheiding wordt gerealiseerd. Bij de meeste elektronische bankiersystemen kunnen de organisaties deze functies zelfstandig toekennen, en is er een functionaris aanwezig die deze toekenningstaak vervult. Bij een enkel elektronisch bankiersysteem is het noodzakelijk dat binnen de computer van de bank deze autorisaties zijn aangebracht. De bank draagt in dat geval zorg voor het aanbrengen van de autorisaties op aangeven van de organisatie.
Extra aandacht dient te worden geschonken aan de functionaris die de bevoegdheden toekent en beheert. Voorkomen dient te worden dat deze functionaris zichzelf zodanige bevoegdheden kan toekennen dat hij/zij het hele betaaltraject zelfstandig kan uitvoeren.

Beheren vaste gegevens
Bij de meeste elektronische bankiersystemen is het mogelijk vaste klantgegevens op te slaan. Deze gegevens kunnen vervolgens worden gebruikt bij het aanmaken van betalingen. Andere voorbeelden van vaste gegevens zijn debetrekeningen, muntsoorten en omschrijving van de aard van de betaling.

Invoeren van betalingen
Het betaalproces start met het invoeren van individuele betaalopdrachten. Deze invoer kan zowel handmatig als automatisch geschieden. Handmatige invoer zal in veel gevallen volstaan indien er weinig betalingen worden verricht. Bij automatische invoer worden de betalingsopdrachten vanuit de geautomatiseerde financiële administratie geïmporteerd in het elektronisch bankiersysteem, via een diskette of via een netwerk. Bij automatische invoer van betalingen wordt gebruikgemaakt van de mogelijkheden die de toepassing van een elektronisch bankiersysteem biedt voor het verbeteren van de efficiency en effectiviteit van de betalingsorganisatie. Dubbel werk wordt hiermee vermeden en de accuratesse van automatische invoer is veelal hoger dan die van handmatige invoer. Uiteraard speelt bij een automatische invoer de betrouwbaarheid van de geautomatiseerde financiële administratie een belangrijke rol waar het gaat om de juistheid en volledigheid van de betaalopdrachten.



Figuur 1. Het elektronisch bankierproces in stappen.

Verificatie, autorisatie en verzenden van betaalopdrachten
Nadat de invoer van de betaalopdrachten is afgerond, dient procuratie te worden verleend voor de betalingen. Deze procuratie wordt verleend met behulp van het elektronisch bankiersysteem en een hulpmiddel voor procuratie. Een voorbeeld van een dergelijk hulpmiddel is een calculator. Deze calculator genereert een code die aan de betaalbatch wordt toegevoegd bij verzending. Doordat de calculator uniek is voor de opdrachtgever, kan de bank aan de hand van deze code vaststellen dat de ontvangen betaalopdrachten authentiek zijn. Tevens is het aan de hand van de toegevoegde code mogelijk voor de bank om vast te stellen dat de betalingsopdrachten na het verlenen van de procuratie niet meer zijn gewijzigd. Iedere wijziging die zou zijn aangebracht, heeft tot gevolg dat de code onjuist is. In dat geval zullen de opdrachten niet worden verwerkt door de bank. Een ander voorbeeld van een hulpmiddel voor procuratie is een lijst met codes die achtereenvolgens dienen te worden gebruikt door de opdrachtgever.

Reconciliatie van betaalopdrachten
Het sluitstuk op het betaalproces is de controle op de juiste verwerking van de betalingsopdrachten. Op basis van de elektronische dagafschriften kan de verwerking van de betalingsopdrachten worden gecontroleerd. Dit kan handmatig en automatisch plaatsvinden. Met name bij organisaties die veel uitgaand betalingsverkeer hebben is automatische reconciliatie een functionaliteit die de efficiency sterk verbetert.
De automatische reconciliatie is eveneens toepasbaar op de inkomende betalingen. Door de geautomatiseerde check van de ontvangen betalingen met de debiteurenadministratie kunnen aanmerkelijke efficiencywinsten worden bereikt.

Inrichten EDP-omgeving
De PC die vaak wordt gebruikt voor het elektronisch bankieren dient op adequate wijze te zijn ingericht, zodat deze voortdurend beschikbaar zal zijn en voldoende is beveiligd. Hierbij kan worden gedacht aan het versiebeheer van de gebruikte programmatuur, het onderhoud van de PC en andere meer algemene beheersmaatregelen. Onderscheid kan worden gemaakt tussen een stand-alone-PC en een PC die in een netwerk geschakeld is. De laatste zal extra maatregelen voor het beperken van de toegang tot de functies voor elektronisch bankieren noodzakelijk maken.

NORMENKADER VOOR HET ELEKTRONISCH BANKIERPROCES

Het uitgaand betalingsverkeer heeft vaak de bijzondere aandacht van de organisaties. Hele stelsels van maatregelen zijn opgezet om te waarborgen dat slechts juiste betalingen worden verricht aan rechthebbenden. De maatregelen die zijn getroffen met betrekking tot elektronische bankiersystemen kunnen organisatorisch, softwarematig, hardwarematig of fysiek van aard zijn. Van groot belang is dat deze maatregelen goed op elkaar zijn afgestemd. Een elektronisch bankiersysteem kan prima mogelijkheden bieden voor het aanbrengen van een functiescheiding, maar als de organisatie hier niet goed mee omgaat is van de vereiste functiescheiding geen sprake.

In deze paragraaf wordt een normenkader gegeven voor de maatregelen die dienen te zijn getroffen om een betrouwbaar en continu elektronisch bankierproces te realiseren.
Met behulp van een procesketen is inzicht verkregen in de primaire en ondersteunende activiteiten in het elektronisch bankierproces. Deze procesketen vormt tevens de basis voor het normenkader. De primaire activiteiten behoren tot het eigenlijke elektronisch bankierproces en zijn globaal onder te verdelen in vijf stappen: invoer, verificatie, autorisatie, verzenden en reconciliatie. De ondersteunende activiteiten bestaan uit het inrichten EDP-omgeving, het aanbrengen en beheren gebruikersautorisaties en het beheer van vaste gegevens. Aan de hand van bedreigingen zijn per activiteit normen opgesteld. Het geheel is weergegeven in tabel 1.

NORMENKADER TOEGEPAST IN HET MKB

Juist in een kleinschalige omgeving kan het gebruik van een elektronisch bankiersysteem nieuwe risico's met zich meebrengen. Een kleinschalige onderneming is genoodzaakt met beperkte middelen en beperkte capaciteit de risico's tot een acceptabel minimum te beperken.
In de vorige paragraaf is het algemene model beschreven, gericht op de inrichting van de beheersorganisatie bij het gebruik van een elektronisch bankiersysteem. In deze paragraaf wordt per activiteit bekeken in hoeverre het MKB aan de geformuleerde norm tegemoet kan komen. Bij het inrichten van de beheersorganisatie zullen de gewenste normen worden afgezet tegen de praktische werkbaarheid en de haalbaarheid van de normen. Daarbij wordt getracht een effectieve balans te vinden tussen de maatregelen geboden door het 'standaard' elektronisch bankiersysteem en de eventuele aanvullende maatregelen in de organisatie.

Tabel 1. Activiteiten van en normen voor het elektronisch bankierproces.

Activiteiten	Normen
Aanbrengen en beheren gebruikersautorisaties	• De procedures rond het invoeren en onderhouden van de gebruikersbevoegdheden dienen de blijvende juistheid van de aangebrachte functiescheidingen te waarborgen en controle hierop mogelijk te maken. • De betrokkenheid van ten minste twee functionarissen dient noodzakelijk te zijn voor het uitvoeren van betalingen. • Het systeem dient alleen toegankelijk te zijn voor bevoegde gebruikers.
Beheer bestanden met vaste gegevens	• De procedures en bevoegdheden voor het onderhouden van vaste gegevens dienen de juistheid en volledigheid van deze gegevens te waarborgen en controle hierop mogelijk te maken.
Invoeren betaalopdrachten	• De procedures voor het invoeren van betaalopdrachten dienen de juistheid en volledigheid van de betaalopdrachten te garanderen.
Verificatie, autorisatie en verzending van betaalopdrachten	• De betaalopdrachten dienen slechts te worden geautoriseerd door hiertoe bevoegde functionarissen. • Voor het verlenen van de autorisatie (procuratie) van betaalopdrachten dient de juistheid en volledigheid te worden vastgesteld. • Hulpmiddelen voor het verlenen van de procuratie dienen slechts ter beschikking van de procuratiehouder te worden gesteld.
Reconciliatie van betaalopdrachten	• De (elektronische) dagafschriften dienen te worden afgestemd met de oorspronkelijke facturen of de uitstaande verplichtingen in de crediteurenadministratie.
Inrichten EDP-omgeving	• De apparatuur waarop het elektronisch bankiersysteem is geïnstalleerd, dient slechts toegankelijk te zijn voor rechthebbenden. • De continuïteit van het elektronisch bankiersysteem dient te worden gewaarborgd. Onder meer kan hierbij worden gedacht aan back-upapparatuur en het maken van back-ups van gegevensbestanden.

Aanbrengen en beheren gebruikersautorisaties

Het aanbrengen van functiescheidingen en het beheren van gebruikersautorisaties vormen twee belangrijke componenten van beheersing van het elektronisch bankierproces.

Functiescheiding
De basiseis die is gesteld aan de functiescheiding binnen het betalingsproces is dat de betrokkenheid van minimaal twee functionarissen noodzakelijk is voor het uitvoeren van betalingen. In de praktijk wordt dit vaak op de volgende wijze opgelost. Eén medewerker houdt zich bezig met het invoeren, verifiëren en verzenden van de betaalopdracht. De tweede medewerker controleert de betaalopdracht op volledigheid en juistheid en autoriseert de betaling voor verzending (deze medewerker heeft de procuratiebevoegdheid).

Bij kleinere organisaties kan het niettemin moeilijk zijn deze functiescheiding te realiseren. In dat geval kan het noodzakelijk zijn alle voor betaling benodigde functies te laten uitvoeren door de procuratiehouder. Hier is sprake van een in de praktijk geaccepteerd risico. De procuratiehouder is sowieso gerechtigd tot het verrichten van betalingen en zal in een dergelijke kleinere omgeving over ruimere bevoegdheden beschikken. Zaak is het wel de autorisatiebevoegdheid in ieder geval slechts te verlenen aan procuratiehouders. Overigens is het in deze situatie van belang dat het crediteurenbeheer (het registreren en betaalbaar stellen van de verplichtingen) door een andere functionaris dan de procuratiehouder wordt uitgevoerd.

Beheer gebruikersautorisaties
In de meest wenselijke situatie worden de bevoegdheden ingevoerd door minimaal twee functionarissen die niet operationeel bij het verrichten van betalingen zijn betrokken. Minimaal twee functionarissen zijn vereist opdat controle kan worden uitgeoefend op het toekennen van bevoegdheden. Hiermee wordt voorkomen dat een functionaris zichzelf ruime bevoegdheden kan toekennen.
In de praktijk is deze norm moeilijk te realiseren. Slechts één functionaris (een systeembeheerder) is noodzakelijk om de bevoegdheden in te voeren en te onderhouden. In dat verband wordt vaak gewezen op de vertrouwenspositie van een systeembeheerder. Oogtoezicht en controle op de blijvende juistheid van de bevoegdheden binnen het elektronisch bankiersysteem zijn mogelijk aanvullende maatregelen.
Een extra mogelijkheid is de bevoegdheden te laten onderhouden door de procuratiehouder. Enige affiniteit bij en gevoel voor automatisering is hiervoor echter noodzakelijk.

Beheer bestanden met vaste gegevens

De waarde van de bestanden met vaste gegevens is enigszins beperkt. Vaste klantgegevens kunnen worden gebruikt bij het snel aanmaken van betalingsopdrachten. De gegevens kunnen daarbij echter worden overschreven, zodat er geen betrouwbaarheidswaarborgen aan kunnen worden toegekend. In een kleinere omgeving is het nut van de toepassing van de vaste gegevens binnen het elektronisch bankiersysteem dan ook meer gelegen in de efficiencyvoordelen.

Invoer betaalopdrachten

Procedures dienen de juistheid en volledigheid bij de invoer van (betaal)opdrachten te garanderen. De functionaris die zich bezighoudt met het invoeren van een betaalopdracht dient niet in staat te zijn de betaalopdracht voor verzending te procureren, tenzij deze functionaris beschikt over procuratiebevoegdheid.

Verificatie, autorisatie en verzending van betaalopdrachten

Het verrichten van procuratie voor de betaalopdrachten is de belangrijkste stap in het betalingsproces. Betaalopdrachten kunnen alleen worden geautoriseerd door de procuratiehouder met gebruik van een procuratiemiddel. Het beheer van het hulpmiddel voor procuratie is de belangrijkste waarborg voor de inrichting van een betrouwbare betalingsorganisatie. Een reële bedreiging is dat de procuratiehouder dit hulpmiddel overdraagt aan een medewerker. Argumenten die hiervoor worden gehanteerd hebben vaak betrekking op werkdruk. In de praktijk is het vaak zo dat de procuratiehouder zich niet geroepen voelt om deze taak te verrichten. De consequentie is dat de uitvoerende functionarissen in dit geval feitelijk zelfstandig betalingsopdrachten kunnen uitvoeren. Behalve het adequaat beheer van de hulpmiddelen voor procuratie dient tevens de controle op de betaalopdrachten op het scherm aan de hand van brondocumenten te worden uitgevoerd. Eventueel kan daarbij worden geopteerd voor een steekproefsgewijze controle.

Het beheer van het hulpmiddel voor procuratie is de belangrijkste waarborg voor de inrichting van een betrouwbare betalingsorganisatie.

Een belangrijk voordeel van het gebruik van een elektronisch bankiersysteem is dat de procuratiehouder een adequate controle van de betalingsopdrachten kan uitvoeren. Er is absolute zekerheid dat de betalingsopdrachten op het scherm ook daadwerkelijk worden verzonden. Bij het gebruik van bijvoorbeeld tape als medium voor het verzenden van betalingsopdrachten wordt deze controle uitgevoerd aan de hand van een detailoverzicht van de inhoud van de tape. Aanvullende maatregelen dienen dan te zijn getroffen om te waarborgen dat het detailoverzicht daadwerkelijk de inhoud van de tape weergeeft.

Reconciliatie van betaalopdrachten

Het sluitstuk op het hele betaaltraject is de controle van de juiste verwerking van de betaalopdrachten. Dit kan worden uitgevoerd aan de hand van de in-

Drs. R. Oudega RE
Is als EDP Audit Manager werkzaam bij KPMG EDP Auditors. Hij richt zich daarbij met name op audits en advisering inzake de beheersing en besturing van informatietechnologie.

Mw. M. Pieper
Is als EDP-auditor werkzaam bij KPMG EDP Auditors, business unit Financiële Dienstverlening. Haar aandachtsgebied ligt bij advies voor en audit van de implementatie van geautomatiseerde betaalsystemen en de administratieve organisatie en interne controle betreffende betaaltoepassingen.

formatie die met het elektronisch bankiersysteem kan worden opgevraagd. Snelle detectie van fouten draagt in het algemeen bij aan een snellere oplossing van het probleem.

Algemeen systeembeheer

Het algemeen systeembeheer zal in een kleinere werkomgeving geen aandacht vragen die afwijkt van het systeembeheer van de overige computers en netwerken. In de artikelen van Van der Vlugt en Van Praat, elders in deze Compact, wordt hierop uitgebreid ingegaan.

TOT SLOT

In dit artikel hebben wij aan de hand van een schematisch model van de toepassing van een elektronisch bankiersysteem voor het verrichten van betalingen de verschillende activiteiten inzichtelijk gemaakt. Met dit model als basis is er een normenkader opgesteld aan de hand waarvan de implementatie kan worden beoordeeld. Deze beoordeling is vervolgens uitgevoerd voor 'kleinere' bedrijven. Hoewel de beoordeling niet specifiek is gemaakt voor een werkelijke organisatie kunnen bij dergelijke kleinere organisaties enkele algemeen geldende belemmeringen worden onderkend voor het realiseren van een betrouwbaar betalingsverkeer. Een belangrijke steunpilaar voor het inrichten van een betrouwbare betalingsorganisatie, een adequate functiescheiding, is bij dergelijke organisaties niet of slechts moeizaam te bereiken. Niettemin is de conclusie dat het met behulp van een elektronisch bankiersysteem ook in een kleine organisatie mogelijk is een betrouwbaar betalingsverkeer te realiseren. Een belangrijke rol is dan weggelegd voor de procuratiehouder. Deze zal zijn verantwoordelijkheid ten aanzien van de controle van de opdrachten en het verrichten van de procuratie met het procuratiehulpmiddel moeten onderkennen en dragen.

Ook voor andere geautomatiseerde betaalsystemen kan een dergelijke analyse worden uitgevoerd. Indien gebruik wordt gemaakt van elektronische media zoals diskette en tape is de controlefunctie van de procuratiehouder minder eenvoudig. Extra maatregelen moeten zijn getroffen om te waarborgen dat de procuratiehouder de daadwerkelijk verzonden betalingsopdrachten op tape, diskette of via datacommunicatie kan controleren. Door nauwgezet het betaalproces te analyseren en te beoordelen is echter ook bij andere geautomatiseerde betaalsystemen een haalbare norm voor het midden- en kleinbedrijf op te stellen.

Certificering van software

Drs. H.G.Th. van Gils RE RA en drs. A.R.J. Basten

Een kwaliteitskeurmerk heeft vaak een specifieke betekenis die niet altijd wordt doorzien. Proces- en productgerichte certificering en beoordeling van software hebben elk hun eigen waarde voor leveranciers en afnemers.

INLEIDING

Het keuren van diensten en producten is al lange tijd een gebruikelijk fenomeen. Iedereen kent de keurmerken van de KEMA op elektrische producten en de slogan 'goedgekeurd door de Nederlandse Vereniging van Huisvrouwen' is bij veel mensen een begrip. Velen zullen daarbij zelfs het groene *keurmerkcirkeltje* voor ogen hebben staan.

Zo'n keurmerk biedt de (potentiële) gebruiker snel inzicht in een kwaliteitsaspect van een product of dienst. Van veel zaken weet je dat het een keurmerk moet bevatten, ook al weten we niet eens precies waar het voor staat (wanneer is iets 'goedgekeurd door de Nederlandse Vereniging van Huisvrouwen'?). Bij elektrische apparaten heeft het meestal wel iets met veiligheid te maken. De meesten reageren daarop dan ook met zoiets als 'met keurmerk, dan zal het wel goed (veilig) zijn'. Er zijn maar weinig mensen die aan de koelkastverkoper het volledige keuringsrapport van de KEMA zullen opvragen om vast te stellen wat dat KEMA-keurmerk precies voor die koelkast betekent.

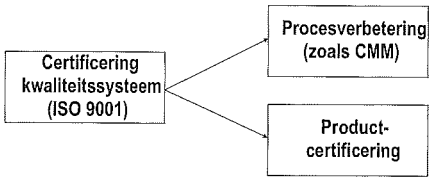
Inmiddels zijn er de nodige initiatieven geweest om tot een kwaliteitskeurmerk voor softwareproducten te komen. Daar in het midden- en kleinbedrijf (MKB) veel gebruik wordt gemaakt van standaardsoftware, is het zinvol om de betekenis van softwarecertificering te beschrijven. Dit artikel geeft de huidige stand van zaken met betrekking tot de certificering van software. Om kwalitatief goede software te kunnen ontwikkelen, is normaal gesproken een deugdelijk kwaliteitssysteem bij de ontwikkelaar van betekenis. Bij ISO 9000-certificeringstrajecten zie je vaak dat een kwaliteitsverbeteringstraject aan de certificering voorafgaat. In dit artikel wordt daarom eerst ingegaan op de ontwikkelingen rond procesverbetering en productcertificering. De productcertificering wordt vervolgens beschreven naar ontwikkelingen vanuit de certificeringsbranche (zoals ISO) en vanuit de accountants/EDP-auditorganisaties. Het artikel wordt afgesloten met de mogelijkheden van softwarecertificering versus systeembeoordelingen en de consequenties daarvan voor de accountant bij zijn totale oordeelsvorming omtrent kwaliteit van risicobeheersing in het kader van de jaarrekeningcontrole.

CERTIFICERING: PRODUCT EN/OF PROCES

Kwaliteit van software

Zoals reeds gesteld zijn er inmiddels de nodige initiatieven geweest om tot een kwaliteitskeurmerk voor softwareproducten te komen. Echter, in de praktijk is er nog geen organisatie in Nederland die algemeen erkende kwaliteitskeurmerken à la ISO afgeeft. Wel wordt veel onderzoek gedaan naar het beschrijven van wat eigenlijk verstaan moet worden onder kwaliteit van software.

Kwaliteit van software wordt in eerste instantie bepaald door de kwaliteit van het ontwikkelingsproces, zowel organisatorisch als inhoudelijk. Een groot aantal softwareproducenten is inmiddels ISO 9001-gecertificeerd. Deze standaard beschrijft de internationale normen voor kwaliteit van processen in het algemeen ('ISO 9001: Quality Systems – model for the quality assurance in design/development, production, installation and servicing'). Aangezien deze standaard voor allerlei branches van toepassing was, is er een aanvullende standaard gekomen in de vorm van ISO 9000-3 ('Guidelines for the application of ISO 9001 to the development, supply and maintenance of software'). Mede door de aanhoudende kritiek op ISO-certificering stellende dat een certificaat op zich niets zegt over het niveau van de kwaliteit van het product ('ook de fabrikant van betonnen zwemvesten is gecertificeerd'), is er in het kader van evaluatie van softwarekwaliteit een positieve ontwikkeling. Software-certificering beoordeelt niet het ontwikkelingsproces, maar juist ook het softwareproduct zelf (zie figuur 1).



Figuur 1. Evaluatie in softwarekwaliteit.

De bekendste ontwikkeling in het streven naar absolute kwaliteitsverbetering is het Capability Maturity Model (CMM) van het Software Engineering Institute (SEI), ingesteld door (wederom) het Amerikaanse Ministerie van Defensie (zie onder andere [Paul93]). Daarbij worden vijf niveaus onderkend die een steeds hoger kwaliteitsniveau weergeven. In Nederland pogen steeds meer organisaties volgens CMM de kwaliteit van het ontwikkelingproces op een hoger niveau te tillen. De vijf niveaus zijn in tabel 1 kort samengevat.

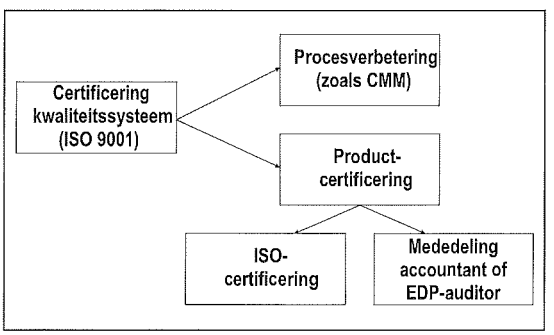
Tabel 1. De niveaus en key process areas van CMM.

Level	Key Process Areas
5. Optimaal Voortdurende procesverbetering is mogelijk door een kwantitatieve feedback van het proces en van het uitproberen van innovatieve ideeën en technologieën.	Defect prevention Technology change management Process change management
4. Beheerst Gedetailleerde meetgegevens uit het ontwikkelingsproces en van de productkwaliteit worden verzameld. Kritische procesindicatoren en productindicatoren zijn bekend en beheerst.	Quantitative process management Software quality management
3. Gedefinieerd Het ontwikkelingsproces (voor uitvoering als sturing) is gedocumenteerd, gestandaardiseerd, en in de organisatie geïmplementeerd. Alle projecten maken daarvan gebruik.	Organization process focus and definition Training program Integrated software management Software product engineering Intergroup coordination, Peer reviews
2. Herhaalbaarheid Basis-projectmanagementprocessen zijn geïmplementeerd voor de beheersing van de kosten, planning en functionaliteit. Projectbewaking vindt plaats, zodat in projecten ervaringen van vorige projecten kunnen worden meegenomen.	Requirements management Software project planning Software project tracking and oversight Software subcontract management Software quality assurance Software configuration management
1. Initieel Het ontwikkelingsproces is ad hoc, soms zelfs chaotisch. Weinig procedureel geregeld; succes hangt vooral af van individuele activiteiten.	

Uit SEI-onderzoeken (o.a. [Gold95]) blijkt overigens dat nog veel verbeteringen in de softwarebranche bereikt kunnen worden. Er bevinden zich nog veel organisaties op niveau 1, terwijl er vrijwel geen organisaties (wereldwijd) op niveau 4 of 5 zijn te vinden.

Overigens is een soortgelijke beweging binnen de accountancy te onderkennen. Vrijwel alle nieuwe controleaanpakken van de grote kantoren bevatten de vraag in hoeverre het management control van de bedrijfsprocessen van zodanig niveau is, dat de kwaliteit van die processen meetbaar wordt. Dat betekent veelal dat accountants zullen gaan stimuleren dat 'key process areas' worden onderkend en dat meetbare key performance indicators (KPI's) voor de kwaliteit van bedrijfsprocessen worden gedefinieerd, gemeten en de resultaten daarvan voor de beheersing worden geanalyseerd.

Een andere manier om aan de kritiek van de ISO-(proces)certificatie tegemoet te komen is het laten keuren van het eindproduct, ofwel certificering van het softwareproduct. Ook op dit gebied is inmiddels heel wat onderzoek verricht, echter concrete resultaten in de vorm van algemeen geaccepteerde certificaten zijn er nog niet veel. De verwachting is dat dit in de nabije toekomst wel sterk zal veranderen. In het vervolg van dit artikel zullen twee ontwikkelingen worden besproken. Ten eerste de ontwikkeling vanuit de certificeringsbranche en ten tweede vanuit de accountants/EDP-auditorganisaties.



Figuur 2. Softwarecertificering in twee praktijkvarianten.

Softwarecertificering vanuit ISO

Meer dan vijf jaar geleden is de ISO-standaard 9126 ([ISO91]) verschenen met als doel kwaliteitsnormen voor softwareproducten te definiëren. Helaas is deze standaard nooit in het Nederlands vertaald. In de standaard zelf zijn zes kwaliteitseigenschappen opgenomen, terwijl in een bijlage nog een nadere onderverdeling van deze eigenschappen is weergegeven met in totaal 21 subeigenschappen. Tabel 2 geeft deze eigenschappen weer. Overigens valt daarbij op dat makkelijk verwarring kan ontstaan over het begrip reliability ofwel betrouwbaarheid. Uit de tabel blijkt duidelijk dat de terminologie afkomstig is van de computerbranche en niet van de accountancy. Betrouwbaarheid heeft in de softwaremarkt alles te maken met beschikbaarheid of herstelbaarheid, terwijl het accountancybegrip betrouwbaarheid in ISO-termen een functionaliteitsbegrip is.

Quality Characteristics (formal ISO 9126)	Quality (informative) subcharacteristics
Functionality	Suitability Accuracy Interoperability Compliance Security
Reliability	Maturity Fault tolerance Recoverability
Usability	Understandability Learnability Operability
Efficiency	Time behaviour Resource behaviour
Maintainability	Analysability Changeability Stability Testability
Portability	Portability

Tabel 2. Overzicht kwaliteitscriteria volgens ISO 9126.

Overigens is dat niet zo gek, omdat bij systeemonderzoeken die in het kader van de accountantscontrole worden uitgevoerd, soms blijkt dat ontwikkelaars alleen de operationele functionaliteit van eindgebruikers onderkennen en onderwerpen als betrouwbaarheid (in de zin van juistheid, volledigheid, tijdigheid en controleerbaarheid van de gegevensverwerking) nauwelijks aandacht geven. Door deze vorm van betrouwbaarheid als functionaliteit te zien, zou zij wellicht meer aandacht in het ontwerp, de programmatuur en de documentatie krijgen.

In 1992 is door de Stichting SERC in het kader van het zogenaamde QUINT-project (Quality in Information Technology) een boekje uitgebracht met een soortgelijke opzet als de ISO 9126-norm, waarin zelfs 32 kwaliteitscriteria zijn onderscheiden ([SERC92]). Voor ieder kwaliteitscriterium is een korte aanduiding van de betekenis gegeven en een aantal mogelijke maatregelen die voor dat kwaliteitscriterium van betekenis kunnen zijn. Bijzonder is dat ook meetindicatoren zijn weergegeven. Dat het meten van kwaliteit voor een aantal criteria nog erg moeilijk is moge blijken uit de toevoeging per kwaliteitscriterium van indicaties over de betrouwbaarheid en objectiviteit van de gegeven meetvoorschriften.

In 1996 is een tweede publicatie van het QUINT-project verschenen ([Zeis96]). Dit betreft deels een herziening van de eerste publicatie. Weer zijn 32 kwaliteitscriteria onderscheiden, die overigens niet geheel overeenkomen met de eerste keer. Hoewel in deze publicatie nadrukkelijk is getracht aan te sluiten op de ISO 9126-norm (alle 21 eigenschap-

Tabel 3. Overzicht van indicatoren voor het kwaliteitscriterium 'accuracy'.

Accuracy: attributes of software that bear on the provision of right or agreed results or effects.
Indicators for accuracy:
- *failure ratio*: the ratio of incorrect processed transactions to the total of presented transaction;
- *significant digits ratio*: the ratio of the implemented significant digits to the required significant digits;
- *manual conformance ratio*: the ratio of functions implemented and the matching product to the functions written in the user's manuals;
- *rounding treatment ratio*: the ratio of functions with the required rounding treatment to the total number of implemented functions.

pen van de ISO-norm zijn overgenomen) is toch besloten er nog elf aan toe te voegen. Het model wordt dan ook het *Extended ISO-model* genoemd. Het grote voordeel is weer dat getracht is zoveel mogelijk indicatoren voor de kwaliteitseigenschappen weer te geven. Als voorbeeld wordt toegelicht uit [Zeis96] de eigenschap 'accuracy' (zie tabel 3).

Wat hierbij opvalt is dat, hoewel het bovenstaande voorbeeld past in de rubriek 'functionality' er voor accountancybegrippen weinig overblijft van functionaliteit. Het zijn vooral indicatoren die passen bij de technische kwaliteit van de *programmatuur*, terwijl de accountant (en waarschijnlijk ook het gebruikersmanagement) bij juistheid vooral denk aan functionaliteit van het *informatiesysteem* (waarin de programmatuur natuurlijk wel een onderdeel is).

Tenslotte kan worden opgemerkt dat noch ISO noch QUINT een uitspraak doet over het minimale vereiste kwaliteitsniveau. ISO geeft waarderingen als *'a higher value is preferred'*. Natuurlijk is het niet mogelijk zonder de aard van de programmatuur te kennen hier bepaalde waarden aan toe te kennen. Wellicht dat door analyses van verzamelde meetgegevens in de toekomst voor bepaalde indicatoren classificatiewaarden kunnen worden vastgesteld. Maar dan blijft toch dat één bepaalde fout in een programma veel ernstiger kan zijn dan twintig andere fouten in dat programma. De betekenis van de fout is vooral afhankelijk van de betekenis van de fout in een bepaald informatiesysteem (of zelfs in een bepaalde situatie).

Overigens bestaat ook nog de ISO-norm 12119 uit 1994, getiteld 'Information technology, Software packages – Quality requirements and testing' ([ISO94]). In deze norm wordt zoveel mogelijk gebruikgemaakt van dezelfde kwaliteitscriteria als in ISO 9126. De norm zelf bevat de eisen te stellen aan softwarepakketten en instructies hoe een pakket te toetsen is aan die gestelde eisen. Overigens valt op dat bij de voorbeelden die gegeven worden van softwarepakketten uitsluitend pakketten worden genoemd als tekstverwerkers, spreadsheetprogramma's, databaseprogramma's, tekenpakketten en pakketten voor technisch of wetenschappelijk werk. Applicatieprogrammatuur wordt daarbij vreemd genoeg niet vermeld.
Het doel van de norm kan worden omschreven als:

a. Het moet duidelijk zijn welke functionaliteit het pakket heeft, hetgeen betekent dat er hoge eisen gesteld moeten worden aan de beschrijving van het softwareproduct, gebruikersdocumentatie en eventuele bijgeleverde programmatuur en gegevens.

b. Het pakket moet werken conform de beschrijving en de documentatie; dit houdt dus in dat dit uitgebreid getest moet worden. Het lijkt daarbij het meest efficiënt als daarvoor een evaluatie van de leverancierstest kan worden uitgevoerd. De norm bevat richtlijnen hoe 'third-parties' de tests moeten uitvoeren. Daarbij wordt uitgegaan van functioneel testen, omdat gestructureerd testen aan de hand van de broncode meestal niet mogelijk is (wordt meestal niet door de leverancier met het pakket geleverd).

Bij de auteurs zijn overigens nog geen voorbeelden van afgegeven certificaten bekend, noch van ISO 9126, noch van ISO 12119. In Nederland zijn dergelijke certificaten zeker nog niet afgegeven.

MEDEDELINGEN VAN ACCOUNTANTS OF EDP-AUDITORS

Door de grote accountantsorganisaties zijn inmiddels diverse 'certificaten' bij softwarepakketten afgegeven. Daarbij gaat het met name om financiële pakketten, hoewel uit de leveranciersmarkt inmiddels ook andersoortige pakketten worden aangemeld voor certificering. De administratieve toepassingen voeren echter nog steeds de boventoon.
De reden voor de vraag naar beoordelingen door accountants en EDP-auditors van pakketten is dat leveranciers naar de markt duidelijk willen maken dat de pakketten voldoen aan criteria die accountants hanteren en waarschijnlijk voor de meeste organisaties van toepassing zijn. Daarbij gaat het meestal om de volgende aspecten:
- controlability: biedt het pakket voldoende (interne controle) middelen om de integriteit en exclusiviteit te kunnen waarborgen;
- auditability: biedt het pakket voldoende middelen om vast te kunnen stellen hoe een bepaalde transactie door het systeem is verwerkt (audit trail);
- documentation: bevat het pakket duidelijke gebruikershandleidingen en systeembeheerdocumentatie;
- legal requirements: voldoet het pakket aan wettelijke voorschriften c.q. 'goed koopmansgebruik'.

Bovenstaande criteria zijn duidelijk ontleend aan software voor financiële toepassingen. Daarbij dienen overigens wel vaker additionele aandachtsgebieden te worden toegevoegd. Gedacht kan worden aan onderwerpen als euro- en millenniumgereedheid in het pakket, maar ook aan zaken als gebruikersvriendelijkheid en functionaliteit (zie ook [Sijbr97]). Zo is de gewenste functionaliteit van een financieel pakket voor de ene branche op een aantal deelgebieden duidelijk anders dan voor een andere branche.

Groot verschil met de ISO-normen is dat het hier meestal niet gaat om technische kwaliteitsaspecten, maar om functionele kwaliteitsaspecten. Daarmee is overigens ook het evalueren minder moeilijk geworden. Het is tenslotte eenvoudiger met behulp van testgevallen vast te stellen dat twee totalen op elkaar aansluiten, dan dat een programma minder dan twee fouten per duizend regels programmacode bevat.

Omdat pakketcertificering niet voor een specifieke organisatie wordt uitgevoerd, worden enkele 'standaard'-testgevallen gecreëerd. Met behulp van deze testgevallen wordt bepaald of aan de normen is voldaan ([Gils95]).

Systeembeoordeling is daarentegen vaak bedrijfsspecifiek. Het is een beoordeling van een informatiesysteem in een organisatie (zie bijvoorbeeld [Koed96]). Het gaat daarbij dus niet meer om een losstaand pakket dat ten behoeve van de pakketcertificering op een afzonderlijk systeem zodanig is geconfigureerd dat optimaal aan de gestelde eisen wordt voldaan. Het is bijvoorbeeld denkbaar dat bepaalde installatieparameters van een pakket optimaal zijn voor de toegangsbeveiliging, maar minder gebruikersvriendelijk zijn of de performance van het systeem nadelig beïnvloeden. Gevolg daarvan kan zijn dat in een bepaalde organisatie wordt besloten de installatieparameters anders in te stellen waardoor wellicht de toegangsbeveiliging minder wordt, maar waarbij op andere aspecten beter wordt gescoord. Ook kan het zijn dat bepaalde functionaliteit niet eens gebruikt wordt; zo wordt bijvoorbeeld vaak geen gebruik gemaakt van de back-upmogelijkheden van een pakket omdat de systeembeheerder daarvoor andere generieke tools heeft.

Bij een systeembeoordeling kan ook direct worden ingespeeld op de administratieve organisatie bij een organisatie. Hierdoor zullen ook de relevante (gebruikers)controles zoals opgenomen in de administratieve organisatie deel uitmaken van de systeembeoordeling, en zelfs de general IT controls kunnen van grote betekenis zijn voor de goede opzet en werking van een specifiek informatiesysteem (denk daarbij met name aan de logische toegangsbeveiliging).

CONSEQUENTIES VOOR DE JAARREKENINGCONTROLE

Een overeenkomst tussen systeembeoordeling en softwarecertificering is dat beide ondersteuning kunnen bieden bij de jaarrekeningcontrole. De hedendaagse accountant gaat steeds meer systeemgericht controleren. Bij het systeemgericht controleren steunt de accountant op de maatregelen die binnen de organisatie zijn getroffen teneinde de risico's op fouten in het verwerkingsproces zoveel mogelijk te beperken. Dit betreft zowel geprogrammeerde als gebruikerscontroles. Een oordeel omtrent de kwaliteit van deze beide controles kan worden verkregen door een systeembeoordeling. Softwarecertificering geeft alleen een uitspraak over de kwaliteit van de mogelijkheden die worden geboden om geprogrammeerde controles te realiseren, maar zegt niets over het gebruik daarvan. Een dergelijke uitspraak heeft beperkte waarde, omdat hij alleen slaat op de *mogelijkheden* van het pakket. Een voorbeeld is controletechnische functiescheiding. Een boekhoudpakket dient te beschikken over de mogelijkheid tot implementatie van een gedegen controletechnische functiescheiding. Binnen certificering wordt beoordeeld of een pakket in staat is deze uit te voeren. Bij implementatie van het desbetreffende pakket binnen een organisatie geeft dit geen garanties voor de werking van de functiescheiding. De daadwerkelijke werking bij een organisatie dient steeds te worden beoordeeld. De accountant kan dus niet volstaan met de conclusie dat het pakket is gecertificeerd. Maar softwarecertificering kan wel een goede basis zijn voor systeembeoordelingen, omdat de belangrijkste aandachtsgebieden reeds in kaart zijn gebracht. De uitvoering van systeembeoordelingen op basis van een certificeringsrapport kan in de praktijk derhalve een stuk efficiënter zijn.

CONCLUSIE

Een organisatie heeft vaak niet de flexibiliteit (organisatorisch en financieel) om te switchen naar een ander pakket, dus een eenmaal gemaakte keuze betekent veelal dat langere tijd gebruikgemaakt moet kunnen worden van het pakket. Omdat softwarecertificering een uitspraak geeft over de kwaliteit van een pakket, kan zij een belangrijke ondersteunende rol spelen bij de selectie van een standaardpakket.

Bij certificering door accountantsorganisaties gaat het vooral om functionele kwaliteitsaspecten.

Vanuit de ISO-kant zijn er duidelijke ontwikkelingen om softwarecertificering meer inhoud te geven, naast de bekende certificering van kwaliteitssystemen à la ISO 9000. De beoogde ISO-richtlijnen voor softwarecertificering zullen met name inhoud geven aan de *technische* kwaliteit van de programmatuur en documentatie. In Nederland zijn op dit moment nog geen softwarecertificaten op grond van de ISO-richtlijnen afgegeven. In de richtlijnen worden met name voorbeelden gegeven van ondersteunende programmatuur als spreadsheets, databasepakketten, maar applicatiesoftware wordt daarbij niet genoemd!

Door de accountants- en EDP-auditorganisaties afgegeven beoordelingen van pakketten leveren ook een duidelijke bijdrage aan inzicht in de kwaliteit van een pakket. Echter, in dat geval betreft het met name de *functionele* aspecten van een pakket. Hoewel de eindgebruiker tijdens pakketselecties zelf goed in staat is functionele aspecten van een pak-

Drs. H.G.Th. van Gils RE RA
Is als senior EDP Audit Manager werkzaam bij KPMG EDP Auditors en is als docent EDP-auditing in het kader van de postdoctorale accountantsopleiding verbonden aan de Universiteit van Amsterdam. Hij is sinds 1978 actief op het terrein van EDP-auditing.

Drs. A.R.J. Basten
Is als assistent-EDP-auditor werkzaam bij KPMG EDP Auditors, business unit Financiële Dienstverlening, en houdt zich onder andere bezig met opdrachten op het gebied van softwarecertificering.

ket te beoordelen, blijkt het in de praktijk dat dan meestal aspecten als interne controle en audit trails minder aandacht krijgen.

De pakketcertificering door accountants en EDP-auditors is primair van betekenis voor applicatieprogrammatuur en in het kader van pakketselectietrajecten.
De accountant kan slechts gedeeltelijk steunen op de certificering bij zijn jaarrekeningcontrole. Hij/zij dient zich altijd een oordeel te vormen omtrent de wijze waarop de cliënt het pakket heeft geïmplementeerd, de mogelijkheden benut en hoe het pakket aansluit op de administratieve organisatie. Het voordeel voor de accountant is gelegen in het feit dat certificering goed inzicht biedt in de controleerbaarheid van het pakket en derhalve een goede en efficiënte basis vormt voor een specifieke systeembeoordeling.

Een combinatie van procescertificering (ISO 9000) en softwarecertificering is naar ons oordeel geen doublure. De procescertificering (of de inschaling volgens CMM) zegt vooral iets over de ontwikkelorganisatie en moet vertrouwen in de leverancier bieden voor de toekomst. De softwarecertificering daarentegen moet vertrouwen geven in een bepaald product op dit moment.

LITERATUUR

[Gils95] H.G.Th. van Gils, *Certificatie van een standaardpakket voor financiële administraties*, Compact 1995/4.

[Gold95] D.R. Goldenson, J.D. Herbsleb, *After the Appraisal: A systematic Survey of Process Improvement, its Benefits and Factors that Influence Success*, Software Engineering Institute, CMU/SEI-95-TR-009, 1995.

[ISO91] ISO/IEC 9126: *Information technology – Software product evaluation – Quality Characteristics and guidelines for their use*, 1991.

[ISO94] ISO/IEC 12119: *Information technology – Software packages – Quality requirements and testing*, 1994.

[Koed96] M.J.A. Koedijk en W.A. de Munck, *System Review Services*, Compact 1996/3.

[Paul93] M.C. Paulk, B. Curtis en M.B. Chrissis, *Capability Maturity Model, version 1.1*, IEEE Software, July 1993.

[SERC92] Stichting SERC, *Het specificeren van software-kwaliteit: een praktische handleiding*, Kluwer Bedrijfswetenschappen, Deventer 1992.

[Sijbr97] H.E. Sijbring, *Pakketmededeling: de vlag moet de lading dekken*, Compact 1997/3.

[Zeis96] Bob van Zeist, Paul Hendriks, Robbert Paulussen en Jos Trienekens, *Kwaliteit van softwareprodukten, Praktijkervaringen met een kwaliteitsmodel*, Kluwer Bedrijfswetenschappen, Deventer 1996.

DE CODE VOOR INFORMATIEBEVEILIGING ALS BASIS VOOR CERTIFICATIE

Dr. ir. P. L. Overbeek

EDP AUDITORIUM

Inleiding

Door de toenemende distributie is belangrijke bedrijfsinformatie tegenwoordig op steeds meer plaatsen beschikbaar. Dit is het gevolg van ondermeer twee trends. Ten eerste wordt, door de opkomst van de decentrale automatisering, informatie op veel meer plaatsen verwerkt dan voorheen. Ten tweede wordt dit veroorzaakt door veranderingen in de organisatie van het werk, samen te vatten als de opkomst van de 'netwerkorganisatie': bedrijven gaan steeds vaker partnerships en andere relaties aan waarbij bedrijfsinformatie, of delen van de IT-infrastructuur, mede voor derde partijen toegankelijk (moeten) zijn.
Om te voorkomen dat hierdoor de kwetsbaarheid van de organisatie toeneemt, moet binnen een organisatie of, in het geval van een informatische relatie, ook tussen organisaties, een stelsel van uniforme spelregels voor de informatiebeveiliging worden gehanteerd. De Code voor Informatiebeveiliging voorziet hierin in de vorm van een eenvoudig managementraamwerk en een evenwichtig stelsel van maatregelen die een 'baseline' vormen voor informatiebeveiliging. Veel bedrijven hanteren de Code inmiddels als uitgangspunt voor hun informatiebeveiliging.

Ter versterking van het vertrouwen is het nu ook mogelijk een uitspraak over het voldoen aan de Code te onderbouwen met een certificaat. Ruim een jaar geleden startte het project Accreditatie en Certificatie van Beveiligingssystemen. Dit project heeft geleid tot een schema voor evaluatie en certificatie tegen de Code voor Informatiebeveiliging. Het project is gesteund door het Ministerie van Economische Zaken, dat hiermee het belang van informatiebeveiliging voor het bedrijfsleven nogmaals onderstreept. In het project namen naast de Raad voor Accreditatie en het ICIT[1] tevens vertegenwoordigers uit het bedrijfsleven deel via, onder andere, VNO/NCW en Fenit, alsmede toonaangevende Nederlandse industrieën en banken. Bovendien heeft nauw overleg plaatsgevonden met partijen in het Verenigd Koninkrijk en enkele Scandinavische landen. Hoewel het ieder land vrij staat zelf eigen certificeringsschema's te ontwikkelen, is de verwachting dat dit certificatieschema internationaal zal worden erkend.

Dit artikel geeft, met de voltooiing van dit project, de achtergronden van het ontwikkelde certificatieschema. In de inzet zijn de belangrijkste aandachtspunten van de Code nogmaals samengevat.

Waarom certificatie tegen de code

De *Code voor Informatiebeveiliging* is een leidraad voor praktische informatiebeveiliging. In de eerste plaats is het de opzet van de Code in eigen huis orde op zaken te kunnen stellen. De Code verschaft de basis om zelf effectieve beveiligingsplannen te ontwikkelen, te implementeren, de uitvoering te 'meten' en bovenal dit geheel goed te managen. Bovendien is de Code bedoeld als referentiekader, als *gemeenschappelijke* basis, voor (elektronische) zakenpartners. In zaken moet men op elkaar kunnen vertrouwen. Dat geldt ook wanneer organisaties afhankelijk worden van (de beveiliging bij) partners waarmee elektronisch zaken worden gedaan, bijvoorbeeld bij gebruik van elektronische handel (EDI) of elektronische post. Door de opkomst van outsourcing neemt bovendien de afhankelijkheid van service providers belangrijk toe. De Code is inmiddels een veelgebruikt referentiedocument tussen zakenpartners onderling (gebruik van de Code in convenanten en interchange agreements) en tussen service providers en hun klanten (gebruik van de Code in service level agreements). Ter versterking van het vertrouwen tussen deze partners is het nu mogelijk een uitspraak over het voldoen aan de Code te onderbouwen met een certificaat. Dit certificaat wordt door een onafhankelijke derde partij afgegeven na uitvoering van een gedegen audit.

Uitgangspunt bij de ontwikkeling van het certificatieschema is dat het een relatief 'licht' schema moet zijn: geen duimendikke handboeken die niet worden gelezen noch worden gebruikt; geen torenhoge procedurele overhead; wel een goed gebruik van kennis en resources binnen de organisatie door intensieve samenwerking in het auditproces; en procesgerichte audits door auditors met aantoonbare kennis en ervaring met informatiebeveiliging en met de organisatie. De certificatie moet als stimulans worden ervaren en niet als ballast – geheel conform de opzet van de Code zelf.

De voordelen van certificatie tegen de code

Een certificaat geeft zowel binnen een organisatie als tussen organisaties meer vertrouwen in de opzet en het bestaan van het managementsysteem voor de informatiebeveiliging en van het getroffen stelsel van maatregelen. Aangezien de Code uitgaat van een managementcyclus, die mede wordt ondersteund door periodieke interne reviews of self assessments en het certificaat alleen geldig blijft bij periodieke externe controle-audits, kan men ook meer vertrouwen hebben dat het beoogde niveau van beveiliging ook *blijvend* wordt geboden. Aangezien de evaluatie kan steunen op de resultaten van de interne self assessments kunnen de kosten van het certificatieproces relatief gezien beperkt blijven.
Voor een service provider kan het bijvoorbeeld zeer aantrekkelijk zijn om in een service level agreement

1. Stichting Instituut ter bevordering van de keuring en Certificatie van Informatie Technologie.

De Code voor Informatiebeveiliging
De Code voor Informatiebeveiliging is een inmiddels breed geaccepteerde samenbundeling van *best practices* voor informatiebeveiliging. De Code steunt op twee principes: ten eerste zal iedere organisatie die structureel aandacht besteedt aan informatiebeveiliging hier een managementstructuur voor nodig hebben. Dit benadrukt het uitgangspunt dat ook informatiebeveiliging een normale managementtaak is. Ten tweede is er een verzameling maatregelen die men redelijkerwijs mag verwachten in een organisatie. In de tabel staan de categorieën waarin deze maatregelen vallen, samengevat. Met de Code kan relatief eenvoudig een evenwichtig pakket maatregelen op maat van de organisatie worden gemaakt; en dat is precies de kracht van de Code.

de Code als uitgangspunt te nemen en, om aan te tonen dat dit uitgangspunt wordt gehaald, een Certificaat tegen de Code te halen. Ook in een interchange agreement kunnen partijen afspreken dat ze zich aan de Code zullen houden en deze afspraak wederom onderbouwen met een Certificaat.

Verschillende mogelijkheden voor evaluatie en certificatie

Het vertrekpunt van het nu ontwikkelde schema wordt gevormd door de 'Eigen Vereisten'. Dit is een stelsel normen die door en voor de organisatie zijn afgeleid van de Code voor Informatiebeveiliging, ofwel de Code die op maat gemaakt is voor de eigen organisatie. De evaluatie vindt plaats in twee stappen (deze worden later nog in detail toegelicht): in het documentatieonderzoek wordt gevalideerd dat dit normenstelsel inderdaad een juiste en voor de organisatie passende 'vertaling' van de Code vormt. In het implementatieonderzoek wordt onderzocht of de 'Eigen Vereisten' daadwerkelijk zijn geïmplementeerd.
Het schema kent verschillende mogelijkheden voor evaluatie en certificatie. Ten eerste zijn er twee sporen, namelijk de 'Eigen Verklaring' en het 'Certificaat'. Ten tweede zijn er twee niveaus: de 'Basisbeveiliging' en de 'Geavanceerde Beveiliging'.

De 'Eigen Verklaring' wordt uitgegeven door de organisatie zelf. De 'Eigen Verklaring' is een *conformiteitsverklaring* waarin het verantwoordelijke management verklaart te voldoen aan de relevante categorieën uit de Code, zoals gespecificeerd in de 'Eigen Vereisten'. De 'Eigen Verklaring' wordt uitgegeven op basis van een door de organisatie zelf uitgevoerde interne review, de 'Zelfbeoordeling'. De 'Eigen Verklaring' wordt geheel onder verantwoordelijkheid van de organisatie zelf uitgegeven. Wel zijn er voorwaarden gesteld aan het proces dat door de organisatie wordt gevolgd bij het uitgeven van deze verklaring. Er zijn geen beperkingen aan deze 'Eigen Verklaring', hoewel de gedachte uiteraard wel is de 'Eigen Verklaring' te laten volgen door een echt Certificaat.
Het Certificaat wordt afgegeven door een onafhankelijke erkende certificatie-instelling. Deze instellingen worden geaccrediteerd door de Raad voor Accreditatie (RvA) en dienen aan de criteria van de Raad te voldoen. Het Certificaat wordt afgegeven op basis van een audit van het management-

Tabel 1. De tien categorieën voor beveiligingsmaatregelen in de Code voor Informatiebeveiliging.

Beveiligingscategorieën	Trefwoorden uit de categorie
Beveiligingsbeleid	Doelstellingen voor informatiebeveiliging vastleggen: beschrijving van de te bereiken of na te streven situatie in termen van de bedrijfsbelangen.
Organisatie van de beveiliging	Beveiligingsfuncties, taken en verantwoordelijkheden, coördinatie, samenhang en rapportagelijnen.
Classificatie en beheer van de bedrijfsmiddelen	Rubriceringsschema's vormen het verband tussen de waarde, bijvoorbeeld van informatie, en de daarbij behorende beveiligingsmaatregelen. Inzicht is nodig in de informatiemiddelen en de verantwoordelijken voor deze middelen.
Personeel	Training, security awareness, veilig gedrag op de werkvloer, aannamebeleid en functioneringsbeoordeling.
Fysieke beveiliging & omgeving	Beveiliging van en in de infrastructuur, ook zaken als stroomvoorziening, datacommunicatielijnen, koeling, etc.
Computer- en netwerkbeheer	Beheer van de technische beveiliging; incidentrapportages; veilige systemen veilig *houden*.
Toegangsbeveiliging	Toegangsbeheersing en -autorisatie.
Bouw & onderhoud van systemen	Aandacht voor de nodige beveiligingsfunctionaliteit en veilige ontwikkel- en onderhoudsmethoden leiden 'zeker' tot veilige systemen, die ook veilig blijven.
Continuïteitsplanning	Calamiteitenopvang, rampenplannen, uitwijk.
Toezicht	EDP-audit, interne controle.

systeem voor informatiebeveiliging van de organisatie. Ook voor het certificatietraject stelt het management een conformiteitsverklaring op. In het certificatieonderzoek kan, zo de organisatie dit wenst, mede worden gesteund op de zelfbeoordelingen of interne audits die reeds binnen de organisatie plaatsvinden. Het (zelf)beoordelen van de naleving van de eigen regels is een verplicht onderdeel van de Code, hetgeen de efficiëntie van de auditactiviteiten ten goede komt. Indien het onderzoek positief wordt afgesloten, wordt een Certificaat verleend. Op verzoek van de organisatie wordt het Certificaat vermeld in het register dat het ICIT hiervoor bijhoudt. Het Certificaat heeft een geldigheid van drie jaar. Ieder jaar vindt een controle-audit plaats. Bij grote niet-beheerste wijzigingen in de organisatie of geconstateerde non-conformiteiten vervalt het Certificaat.

Het certificeringsschema onderscheidt twee niveaus, namelijk de Basisbeveiliging en de Geavanceerde Beveiliging. Op beide niveaus is zowel een 'Eigen Verklaring' als een Certificaat mogelijk.
Voor het niveau 'Basisbeveiliging' dient de organisatie ten minste de bekende *Key Controls* uit de Code te hebben geïmplementeerd. De organisatie geeft hiertoe een 'Conformiteitsverklaring' uit en zorgt voor doeltreffende en aantoonbare implementatie.
Voor het niveau 'Geavanceerde Beveiliging' dient de organisatie voor alle categorieën uit de Code aan te geven welke van toepassing zijn en deze selectie te onderbouwen door middel van een risicoanalyse of vergelijkbare methode. Ook bij de Geavanceerde Beveiliging geeft de organisatie een 'Conformiteitsverklaring' uit.
Het staat organisaties vrij zelf het bij de complexiteit en het ambitieniveau van de organisatie passende niveau te kiezen. Het is bijvoorbeeld goed denkbaar dat kleinere organisaties zullen volstaan met de Basisbeveiliging en nooit zullen doorgroeien naar de Geavanceerde Beveiliging.

Het certificatieproces

Indien de organisatie besluit 'op te gaan' voor het Certificaat is de eerste stap in het certificatieproces de aanvraag tot certificatie. De organisatie moet de 'Conformiteitsverklaring' gereed hebben. De certificatie-instelling stelt een auditteam samen met auditors die ten minste vier jaar IT-ervaring hebben en ten minste twee jaar ervaring met informatiebeveiliging. Bovendien moeten de auditors aantoonbare auditervaring hebben. De tweejarige postdoctorale EDP-auditopleiding is echter niet verplicht.
De tweede, optionele, stap is de uitvoering van een proefbeoordeling. Hierin wordt een globale indruk verkregen en wordt een beeld gevormd van de haalbaarheid van een Certificaat.
De derde stap is het documentatieonderzoek. In dit onderzoek wordt vastgesteld of de conformiteitsverklaring en de bijbehorende documentatie voldoen aan de gestelde eisen, met name de selectie van categorieën uit de Code met een verantwoording. Indien non-conformiteiten worden vastgesteld, wordt de audit niet eerder voortgezet dan nadat deze zijn verholpen.
De vierde en meest omvangrijke stap is de implementatiebeoordeling. Zoals gezegd zijn hier voor de organisatie en de certificatie-instelling in onderling overleg verschillende benaderingen te kiezen. Indien de organisatie een goede interne managementstructuur kent met goede interne controles of zelfbeoordelingen bestaat het grootste deel van het werk van de certificatie-instelling uit het beoordelen van deze werkzaamheden. Daarnaast zal de certificatie-instelling ook onafhankelijke waarnemingen uitvoeren (interviews en verwerven van 'evidence'). De verdeling van werkzaamheden tussen organisatie en certificatie-instelling is dus niet vastgelegd, er zijn hier de nodige vrijheidsgraden.

De laatste stap is de beslissing tot certificatie. Indien geen non-conformiteiten zijn blijven bestaan en de onvermijdelijke tekortkomingen niet te ernstig zijn, kan het Certificaat worden verleend. Bij de eerstvolgende periodieke controle-audit worden uiteraard met name de geconstateerde tekortkomingen opnieuw onder de loep genomen. Vast onderdeel van de controle-audit vormt ook de beoordeling van het 'veranderingsmanagement': is de organisatie of haar werkwijze gewijzigd, en welke aanpassingen heeft zij daarvoor getroffen in de informatiebeveiliging.

Reikwijdte van het Certificaat

De opzet van dit certificatieproces op basis van de Code is het vertrouwen tussen de interne en externe partners te bevorderen. Niet meer en niet minder. De werkwijze in het certificatieproces kent een aantal beperkingen. Aangezien een groot deel van de werkzaamheden op steekproeven en door de organisatie zelf door middel van self assessments aangedragen 'evidence' gebaseerd is, is de werkwijze niet bestand tegen boze opzet of fraude. Ook is de beoordeling van de technische implementatie indirect: de 'compliance-test' wordt beoordeeld en niet de implementatie zelf. Hier zijn aanvullende audits voor nodig. Qua diepgang kan worden gesproken over een volledige audit tussen een quick scan en een third-partymededeling in. Omdat de nationale en internationale ervaring met dit soort evaluaties nog beperkt is, kan ook nog moeilijk gesproken worden van een uniforme aanpak (dat is echter een kwestie van tijd aangezien het streven gericht is op internationale harmonisatie, dit naast de reeds lopende nationale afstemming tussen certificatie-instellingen). Sterk punt is het accent op het managementraamwerk voor informatiebeveiliging: de organisatie stelt van de Code afgeleide normen, implementeert deze, houdt toezicht op de implementatie, stuurt zo nodig de implementatie, en analyseert periodiek of een bijstelling van de normen nodig is.

Tot slot

Twee organisaties hebben reeds bij de Raad voor Accreditatie een verzoek tot erkenning als certificatie-instelling voor dit schema ingediend. Naar verwachting kunnen na de zomer de eerste Certificaten worden uitgereikt.

Dr.ir. P.L. Overbeek
Is als EDP Audit Manager werkzaam binnen de business unit Technical Auditing van KPMG EDP Auditors. Hij heeft ervaring met een breed scala van advies- en auditopdrachten op het gebied van informatiebeveiliging, met name inzake het risicomanagement van informatie en informatietechnologie.

EURO EN HET JAAR 2000, AUTOMATISERINGSCONTRACTEN OP DE HELLING?

Mr. D.J. Mensink

'Amsterdam' leerde ons korte tijd geleden dat er formeel overeenstemming is over de invoering van één euro binnen de EMU-lidstaten. Dat is hoopgevend voor sommigen onder ons, anderen zien de komst met lede ogen tegemoet. Nu valt er echter weinig of niets te veranderen aan de invoering (of het moeten opschriften zijn op de rand van de munten). De automatiseringsbranche heeft er een nieuwe deadline bij, naast die andere met betrekking tot het millenniumprobleem. In dit verband is er niet alleen sprake van inhoudelijke vraagstukken en problemen, ook zijn er nogal wat vragen met betrekking tot de automatiseringscontracten (meer specifiek service-contracten) op het gebied van onder andere financiële software.

Een mogelijk contractueel struikelblok tussen leveranciers en klanten betreffen de functionele aanpassingen aan softwarepakketten die noodzakelijk zijn door de komst van de Euro. Het betreft hier met name financiële software, hoewel er eigenlijk weinig zakelijke software is te bedenken waarin geen valutavelden zitten. Dus: het betreft hier niet zozeer de geldigheid van het contract waarmee de software is gekocht maar meer de functionele geschiktheid van de gekochte software om bijvoorbeeld te kunnen factureren met euro's. In de automatiseringswereld heerst een voorzichtige tactische tweeslachtigheid: enerzijds dient veel software te worden aangepast, anderzijds is niet helemaal duidelijk of dit werkzaamheden zijn die vallen onder servicecontracten dan wel of er hier sprake is van meerwerk dat op basis van opdrachtverstrekking zal worden verricht. Inschattingen hebben het over zes maal zoveel manuren aanpassingen in het geval van de euro in vergelijking met het oplossen van het 2000-probleem. Dit heeft te maken met het feit dat de invoering van de euro niet een enkele bedrijfsbeslissing veronderstelt maar dat er meerdere strategieën zouden zijn om deze omslag binnen de computerprogramma's te realiseren. Tussen haakjes: het millenniumprobleem moet niet worden onderschat. De kosten voor aanpassing van de software zijn aanzienlijk, en, zoals eerder hier en op andere plaatsen de laatste tijd zo vaak gesteld, het millenniumprobleem heeft een zeer harde deadline.

Betalen voor aanpassingen

In verband met de invoering van de euro is het belangrijk om vroegtijdig te bepalen wie de noodzakelijke aanpassingen zal gaan betalen in de software. Dit is van belang omdat gedurende een bepaalde periode gelijktijdig met euro's en guldens gewerkt moet worden (multi-currency systemen). Het is soms verdedigbaar dat deze aanpassingen onder de bepalingen van de onderhoudscontracten vallen. Een aantal softwareleveranciers huldigt (gelukkig) dit standpunt en zal derhalve de kosten via de normale onderhoudsvergoedingen doorberekenen. Het is echter ook mogelijk dat er onderhoudscontracten zijn die niet voorzien in softwareveranderingen als gevolg van wettelijke aanpassingen. Bedrijven die geen onderhoudscontract hebben, of een onderhoudscontract dat de euro-aanpassingen niet dekt, zullen al snel moeten investeren in de benodigde aanpassingen. Dit geldt evenzo voor maatwerksoftware of aanpassingen op standaardsoftware.

Voor wat betreft het 2000-probleem speelt er geen multidatumprobleem of iets van dergelijke aard. Hoewel leveranciers met betrekking tot hun standaardprogrammatuur 'certificering' van de software voor het jaar 2000 marketingtechnisch interessant zullen vinden en derhalve zelf een belang zullen hebben bij de 2000-bestendigheid van de software, zullen ook verkochte maatwerkapplicaties moeten worden aangepast om ook in het laatste jaar van deze eeuw en verder te kunnen blijven functioneren.

Verantwoordelijkheid

Indien gekeken wordt naar de verantwoordelijkheid voor aanpassing van de software zijn er juridisch gezien niet zoveel verschillen tussen de invoering van de euro en het millenniumprobleem. Er zijn ruwweg twee situaties te onderkennen:

1. In het afgesloten licentiecontract en/of de onderhoudsovereenkomst garandeert de leverancier de geschiktheid van het pakket om te kunnen werken met de euro en de werkzaamheid van het pakket op het moment dat het 2000 wordt en met name ook na de jaarwisseling.

2. Noch in het afgesloten licentiecontract, noch in de onderhoudsovereenkomst garandeert de leverancier enige geschiktheid van het pakket met betrekking tot de euro en het jaar 2000.

In situatie 1 lijkt de situatie voor de opdrachtgever ideaal. Toch kan ook in dit geval de opdrachtgever met lege handen komen te staan. Indien de leverancier er onverhoopt niet in slaagt de conversie correct te realiseren, zal uiteindelijk een schadeclaim kunnen worden ingediend. Deze zal dan conform de aansprakelijkheidsbepalingen moeten worden afgewikkeld. Mocht aansprakelijkheid zijn uitgesloten, dan heeft de opdrachtgever grote kans met lege handen achter te blijven. Veelal is aansprakelijkheid beperkt en zal niet alle schade worden vergoed. Het is daarom raadzaam aandacht te besteden aan garanties van de leverancier gecombineerd met schadevergoedingsbepalingen en verzekering van de leverancier tegen dergelijke aanspraken. In situatie 2 geldt op zich hetzelfde als gesteld onder 1, zij het dat de stormbal hier nog eerder dan in de eerste situatie moet worden gehesen.

Daarnaast is er het probleem van de kosten met betrekking tot de noodzakelijke aanpassingen. Indien hierover geen overeenstemming is bereikt en contractueel niets is afgesproken, kan de opdrachtgever voor aanzienlijke kosten komen te staan. Dit probleem zal in de komende jaren nadrukkelijker gaan spelen omdat er naar verwachting schaarste

zal ontstaan aan programmeurs die de conversiewerkzaamheden kunnen verrichten. De prijzen voor deze vorm van dienstverlening zullen waarschijnlijk dus gaan stijgen. Een contractueel af te spreken prijsbeheersingsmechanisme is in dit verband dan ook aan te raden.

Het is derhalve verstandig om in een vroegtijdig stadium de relevante automatiseringscontracten (huidige en toekomstige) aan een onderzoek te laten onderwerpen om te bezien waar juridische risico's liggen en welke partij in uw geval de kosten moet dragen die gemoeid zijn met de noodzakelijke aanpassingen van uw informatiesystemen. Wellicht kunnen eventuele daaropvolgende contractonderhandelingen een herverdeling van risico's bewerkstelligen.

Mr. D.J. Mensink
Is freelance informaticajurist en als zodanig onder andere werkzaam bij KPMG EDP Auditors.

KPMG EDP Auditors
Samsom BedrijfsInformatie