LENTE

COMPACT

BEHEERSING VAN AUTOMATISERING

1994/1

KWARTAALBLAD EDP-AUDITING

Compact ®
Jaargang 21, nummer 1
Een uitgave van KPMG Klynveld EDP Auditors en Samsom BedrijfsInformatie, werkmaatschappij van Wolters Kluwer NV.
Het blad verschijnt 4 x per jaar.

Redactie
D. Steeman
(hoofdredacteur)
drs. R.G.A. Fijneman
prof. A.W. Neisingh
drs. P. Veltman

Redactiesecretariaat
Mw. I. de Koning,
Samsom BedrijfsInformatie,
Postbus 4,
2400 MA Alphen aan den Rijn
Tel.: 01720 - 66 746
Fax : 01720 - 66 569

Vormgeving
Bureau Karakter, Delft

Aan dit nummer werkten mee
P. van Berge
drs. H.G.Th. van Gils
prof. H.B. Moonen
prof. A.W. Neisingh
prof.dr.ir. R. Paans

Abonnementen
f 135,- per jaar incl. BTW. Losse nummers f 45,- 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.: 01720 - 6 68 00
Fax : 01720 - 7 59 33
Adreswijzigingen - ook tijdelijke - moeten minstens 8 weken voor de verschijningsdatum bekend zijn.

Uitgever
J.R.M. Masselink

NOTU
VAKTIJDSCHRIFTEN

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 ● privacy-wetgeving ● computercriminaliteit en nieuwe regelgeving.

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

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 Klynveld, KPMG Klynveld 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.

Beheersing van automatisering staat ditmaal centraal in Compact. Onder meer wordt ingegaan op de invloed van informatietechnologie op de beheersing van organisaties, de beheersing van de kosten en verbetering van de service van een rekencentrum, en de beheersing van kosten en baten van informatietechnolgie in het algemeen. Daarnaast is een artikel opgenomen over informatiebeveiliging, een belangrijk onderdeel van de te treffen beheersingsmaatregelen. Verscheidene auteurs besteden hierbij aandacht aan de invloed van wet- en regelgeving op de beheersing van automatisering.

Bij wijze van aanvulling hierop wil uw scheidende hoofdredacteur u gaarne wijzen op de in september gepubliceerde 'Code of Practice for Information Security Management'.
Deze code is onder de patronage van The Development for Enterprise en het British Standards Institution tot stand gekomen.

De Code of Practice moet van bijzondere betekenis worden geacht omdat hij, anders dan in het verleden het geval was, een normatief document is dat door een aantal vooraanstaande gebruikersorganisaties is opgezet. Indien deze code, die bedoeld is om tot ISO-standaard te worden verheven, in ruime mate door het bedrijfsleven wordt geadopteerd, zal dit voor accountants en EDP-auditors een krachtig hulpmiddel zijn bij controle en advies over beveiligmgsaspecten van de informatiehuishouding.

Tot op heden werden de normen op dit gebied door tal van professionele organisaties op het gebied van auditing en informatietechnologie aangedragen, doch nimmer vanuit de gebruikershoek. Deze normen werden door het bedrijfsleven dan ook altijd met een zeker wantrouwen bekeken.

Dat aan de code gezag zal worden toegekend nog voordat deze tot ISO-norm is verheven, kan worden ontleend aan de namen van de organisaties die de code gezamenlijk hebben ontwikkeld, te weten:
- The BOC Group;
- British Telecom;
- Marks and Spencer;
- Midland Bank;
- Nationwide Building Society;
- Shell International Petroleum Company;
- Shell U.K. Limited;
- Unilever.

In deze code zijn de volgende gebieden in hoofdstukken ondergebracht, waarbij tevens een tiental zogenaamde key controls (*) is gedefinieerd welke van fundamenteel belang worden geacht voor een adequate beveiliging.

1. *Security policy*
   1.1.1* Information security policy document
2. *Security organisation*
   2.1.3* Allocation of information security responsibilities
3. *Assets classification and control*
4. *Personnel security*
   4.2.1* Information security education and training
   4.3.1* Reporting of security incidents
5. *Physical and environmental security*
6. *Computer and network management*
   6.3.1* Virus controls
7. *System access control*
8. *System development and maintenance*
9. *Business continuity planning*
   9.1.1* Business continuity planning process
10. *Compliance*
    10.1.1* Control of proprietary software copying
    10.1.2* Safeguarding of company records
    10.1.3* Compliance with data protection legislation
    10.2.1* Compliance with security policy

Het verschil in invalshoek met accountantscontrole blijkt uit het feit dat voor accountantscontrole essentieel geachte
- scheiding tussen ontwikkel-, test- en uitvoeringsomgeving,
- logische toegangscontrole,
- handmatige correctieprocedures,

niet als key controls worden aangemerkt.

Verwacht kan worden dat de code als beleidsinstrument voor de leiding van ondernemingen zal worden gehanteerd.

Inmiddels is bekend geworden dat de code in het Nederlands zal worden vertaald, aangepast aan de Nederlandse situatie, vooral met betrekking tot de wetgeving.

Vooralsnog is de code onder nummer DISC PD0003 en ISBW 0.580.22536.4 verkrijgbaar via DISC,
2 Park Street,
London W1A 2BS.
Tel. 44(71) 6299 000.
Fax: 44(71) 603 2084.

De prijs bedraagt circa *f* 25.

D. Steeman RE RA

De invloed van informatietechnologie op de beheersing van organisaties

Prof. A.W. Neisingh RE RA

De inzet van computers heeft verstrekkende gevolgen voor de beheersing van organisaties. Verschillende vormen van het gebruik van informatietechnologie en de consequenties daarvan passeren de revue.

INLEIDING

In dit artikel wordt aandacht besteed aan de ontwikkeling van het gebruik van informatietechnologie in organisaties en de consequenties die dat heeft op de beheersing en de beveiliging van de geautomatiseerde gegevensverwerking. Het is daarbij niet de bedoeling diepgaande beschouwingen te geven doch veeleer om de problematiek te signaleren en oplossingsrichtingen aan te geven.

De ontwikkelingen in de automatisering (ofwel informatietechnologie) schrijden nog steeds voort. Het management wordt met gecompliceerde technologieën (netwerken, gedistribueerde databases, client/server-concepten, EDI-toepassingen) geconfronteerd, die direct of indirect de bedrijfsprocessen in de organisatie ondersteunen. De implementatie en de beheersing van deze technologieën in organisaties vinden op verschillende manieren plaats. Daarbij dient zich het vraagstuk aan wat de invloed van nieuwe informatietechnologie op de administratieve organisatie en interne controle is. De wijze van invulling van de normen op het gebied van de administratieve organisatie en interne controle is aan verandering onderhevig.
Het begrip informatietechnologie valt in algemene zin te definiëren als de technologie van het vastleggen, bewerken en opslaan van gegevens en het verschaffen van informatie. Het raakvlak met de bestuurlijke informatievoorziening in een organisatie blijkt uit deze definitie. De informatietechnologie vervult een ondersteunende rol bij het tot stand brengen en in stand houden van de bestuurlijke informatievoorziening, waarbij laatstgenoemd begrip zich niet beperkt tot de administratieve systemen, maar feitelijk de gehele bedrijfsvoering omvat .
Informatietechnologie kent vele verschijningsvormen. In dit artikel worden de ontwikkelingen in de informatietechnologie uiteengezet, zoals van batch- naar database-omgevingen, van mainframecomputers naar client/server-omgevingen, van losstaande informatiesystemen naar geïntegreerde systemen. Deze ontwikkelingen hebben invloed op de aard en omvang van het stelsel van maatregelen van interne controle in een organisatie.

In een recente publikatie van de Treadway-commissie in Amerika [COSO92] wordt het begrip 'internal control' gedefinieerd als een proces, ingevuld door het management en de overige werknemers, gericht op het verkrijgen van redelijke zekerheid omtrent het bereiken van doelstellingen met betrekking tot:

- de effectiviteit en efficiëntie van de bedrijfsprocessen;
- de betrouwbaarheid van de financiële rapportage;
- de overeenstemming met relevante wet- en regelgeving.

Van belang is te benadrukken dat effectiviteit en efficiëntie uitdrukkelijk worden genoemd, alsmede 'compliance' met wet- en regelgeving. Gezien de ontwikkelingen in Nederland op dit gebied (Wet persoonsregistraties, Wet computercriminaliteit en voorziene wijzigingen in de Wet op de telecommunicatievoorzieningen) zou uitbreiding van het begrip interne controle op zijn plaats zijn.

Kernbegrippen in [COSO92] zijn: proces, mensen, redelijke zekerheid en doelstellingen. Kortom een integrale benadering! Het definiëren van een beheersingsstructuur is geenszins een technisch proces. In [COSO92] worden vijf componenten benoemd die sterk met elkaar samenhangen en op basis waarvan de beheersingsstructuur dient te worden uitgewerkt. Deze componenten zijn: control environment, risk assessment, control activities, information and communication, en monitoring.

Zoals in het vervolg van het artikel zal worden toegelicht, kent informatietechnologie een toenemend aantal verschijningsvormen. Vele aspecten zijn verder van belang om te komen tot het definiëren van een toereikend stelsel van maatregelen van fysieke, organisatorische en logische aard. Het is de verantwoordelijkheid van het management te beslissen over niveau, aard en omvang van de te treffen maatregelen [Brou93].

VAN BATCH NAAR ONLINE/REALTIME

Terugkijkend op het oorspronkelijk gebruik van computers was er in de jaren zestig en zeventig sprake van massale batch-gewijze geautomatiseerde processen. Computersystemen waren uitstekend in staat voor de mens geestdodende arbeid over te nemen en te allen tijde de verwerking correct te laten plaatsvinden. Voor de gebruikersorganisatie betekende deze wijze van gegevensverwerking dat de invoer stapelsgewijze werd vastgelegd en aansluitend op volledigheid en juistheid werd gecontroleerd. Op deze wijze werd de basis van een betrouwbare gegevensverwerking gelegd. De autorisatiecontrole werd geëffectueerd door documenten te laten aanleveren vergezeld van aanbiedingsformulieren (en zo mogelijk tellingen) en geparafeerd door de verantwoordelijke functionaris. Vervolgens werd de correcte verwerking op eenvoudige wijze door de gebruikersorganisatie zelfstandig vastgesteld.

Problemen ontstonden toen het rechtstreeks verband tussen invoer en uitvoer begon te ontbreken.

Deze controle werd ook binnen het computercentrum door zogenaamde produktiecontroleurs uitgevoerd om daarmee tijdig vast te stellen dat het computercentrum de aan hem opgedragen werkzaamheden correct had uitgevoerd. Het was tenslotte altijd mogelijk dat afzonderlijke batches niet in de verwerking zouden worden meegenomen, dan wel dat een andere versie dan de laatste van het te verwerken bestand zou worden gebruikt.

Problemen ontstonden enigszins toen het rechtstreeks verband tussen invoer en uitvoer begon te ontbreken. De invoer bleef weliswaar stapelsgewijs aangeleverd worden, doch de verwerking leidde tot het al dan niet accepteren van posten op grond van criteria die reeds in bestanden aanwezig waren en/of op grond van rekenregels in programmatuur. Aan de hand van een voorbeeld wordt een en ander nader uitgewerkt.

Een ziektekostenverzekeringsmaatschappij ontvangt van vele verzekerden declaraties in verband met vergoeding van ziektekosten. De bij de declaratie gevoegde nota's worden ingevoerd en in een geautomatiseerd batch-gewijze georganiseerd proces verwerkt. In dit proces stelt de computer vast of uitkering van de ingediende nota kan geschieden op grond van de wijze waarop iemand verzekerd is (klasse, meeverzekering huis- en/of tandarts en dergelijke), terwijl verder wordt nagegaan of c.q. in hoeverre een door verzekerde overeengekomen eigen risico dient te worden verrekend dan wel reeds gedeeltelijk is verrekend. De uitvoer van de verwerking bestaat onder meer uit een bericht aan verzekerde dat een bedrag op zijn bank/girorekening zal worden bijgeschreven, met een specificatie van de posten die voor vergoeding in aanmerking zijn gekomen.
In dit voorbeeld ontbreekt een direct verband tussen de invoer en de uitvoer. Ook al wordt een totaal opgebouwd van de posten die niet tot uitkering zijn gekomen, dan nog zegt deze informatie niets over de volledigheid en juistheid van de uitkeringen omdat deze immers onder 'besturing' van de programmatuur op grond van polisvoorwaarden en andere criteria zijn bepaald. Hierdoor is de juistheid van de uitkeringen afhankelijk van de kwaliteit van de programmatuur en de integriteit van de bestanden waarin gegevens zijn vastgelegd op grond waarvan uitkeringen worden bepaald.
De verbandscontroles tussen invoer en uitvoer kunnen worden vervangen door cijferanalyses, die echter minder zekerheid bieden, aangevuld met detailcontroles.

Het ligt meer voor de hand in een dergelijke situatie te zoeken naar maatregelen die van beslissende invloed zijn op de beheersing van het proces. Deze kunnen onder meer worden gevonden in de kwaliteitswaarborgen in de verwerkingsorganisatie, het computercentrum, alsmede in die van ontwikkeling en onderhoud van systemen, de test-, acceptatie- en overdrachtsprocedure, het bibliotheekbeheer en dergelijke.
In het bijzonder dient de verantwoordelijke gebruiker de acceptatietest met behulp van een omvangrijke realistische testset uit te voeren.

De technologische ontwikkeling maakte het mogelijk de stap van batch-verwerking via online-invoervastlegging naar online/realtime-verwerking te maken. Hieronder dient dan te worden verstaan invoervastlegging op afstand met onvertraagde verwerking in de gegevensverzamelingen. Op vormen als pseudo update en dergelijke zal hier niet nader worden ingegaan.

Het zal duidelijk zijn dat in geval van invoervastlegging op afstand gevolgd door onvertraagde verwerking van de mutaties in het bijzonder bevoegdheids- en volledigheidscontroles op een geheel andere wijze dienen te worden gerealiseerd dan in een batch-gewijze verwerkingssituatie gebruikelijk is.

In systeemprogrammatuur voor online/realtime-gegevensverwerking kunnen maatregelen worden opgenomen ten aanzien van autorisatiecontrole en kan in de applicatieprogrammatuur een doorlopende nummering worden opgenomen ten behoeve van volledigheidscontroledoeleinden.
De verschuiving van interne-controlemaatregelen die door gebruikers worden uitgevoerd naar controles in systeem- en toepassingsprogrammatuur wordt aangeduid als migratie van controles [Vrie86].
De noodzaak om te steunen op de goede kwaliteit van de automatiseringsorganisatie komt bij deze verwerkingsvorm nog nadrukkelijker naar voren. Er dient zich echter een probleem aan en wel het volgende:
De functie van werkvoorbereider, degene die ervoor zorgt dat een programma op tijd wordt gestart, dat de daarbij behorende bestanden beschikbaar zijn en dergelijke, verschraalt. Immers, programmatuur is voortdurend operationeel en de bestanden dienen dientengevolge stand-by te zijn. In dat verband wordt ook de afzonderlijke functie van bewaarder van bestanden min of meer overbodig. Er is geen voortdurend gesjouw meer met magneetbanden en dergelijke. Ook de functie van produktiecontroleur komt te vervallen; het hanteren van totaalcontroles in het rekencentrum blijkt niet meer mogelijk te zijn.

Een andere ontwikkeling betreft de toenemende betekenis van gespecialiseerde functies binnen de automatiseringsorganisatie. De systeemprogrammeur, een specialist op het gebied van de besturingsprogrammatuur met de nadruk op de efficiëntie-aspecten, vervult een voor de kwaliteit van de dienstverlening door het computercentrum zeer belangrijke rol. In de loop van de tijd werden aan de stam van de technische ondersteuning nog vele specialisten toegevoegd; te noemen zijn netwerkbeheerders, database administrators, bibliotheekbeheerders, specialisten op onderdelen van besturingsprogrammatuur zoals het toegangscontrolesysteem en dergelijke. Daarmee wordt de functie technische ondersteuning nog moeilijker te managen dan zij al was.
Een oplossing dient te worden gezocht in het inrichten van een organisatie van kwalitatief toereikend niveau. Dat wil zeggen dat een permanent en evenwichtig stelsel van maatregelen van organisatorische, logische en fysieke aard dient te worden geïmplementeerd.

Waar zo'n sterke afhankelijkheid van de kwaliteit van de automatiseringsorganisatie in al haar geledingen ontstaat, zullen beschikbare beheersingshulpmiddelen in optima forma moeten worden gebruikt om vast te stellen dat de automatisering permanent voldoet aan de gedefinieerde eisen.

Spoedig zou blijken dat een verdergaand online/realtime-gebruik van computers slechts efficiënt mogelijk zou zijn wanneer tot een eenmalige opslag en gemeenschappelijk gebruik van gegevens zou worden overgegaan. In de hiernavolgende paragraaf zal op de problematiek van databases (en database-managementsystemen) worden ingegaan.

DE INTRODUCTIE VAN DATABASES

De introductie van databases was een logisch vervolg in het totaal van de ontwikkelingen van de informatietechnologie. Weliswaar hadden bedrijfsonderdelen gegevens nodig voor verschillende doeleinden, echter van betekenis werd een eenmalige, eenduidige en integere vastlegging ervan. Deze gegevens zouden dan beschikbaar zijn voor gemeenschappelijk gebruik en zelfs simultaan gebruik in de organisatie.
Een database is dan een geïntegreerde verzameling van gegevens waarvan de specificaties buiten de applicatieprogramma's om worden vastgelegd [Vand92].

Van betekenis werd een eenmalige, eenduidige en integere vastlegging van bedrijfsgegevens voor verschillende doeleinden.

Een database heeft als zodanig geen bestaansrecht; specifieke programmatuur - het database-managementsysteem - is ontwikkeld om opslag, gebruik, beveiliging en dergelijke te reguleren. Een afzonderlijke functie, de database administrator[1], is nodig om de database te beschrijven, de afzonderlijke verzamelingen ten behoeve van gebruikers te definiëren (technische ontwerpactiviteiten), gegevensgebruik, beveiliging van gegevens en dergelijke te organiseren.
Aangezien de database administrator de toegangsregels implementeert draagt hij onder meer verantwoordelijkheid voor de structuur waarmee de functiescheiding kan worden geëffectueerd.

Als in een online/realtime-situatie gebruik wordt gemaakt van database-technologie dient men te bedenken dat verder bijzondere zorg en aandacht dienen te worden besteed aan de reconstructiemogelijkheden. Een reconstructie kan noodzakelijk zijn ingeval de computer dan wel de database ten gevolge van een calamiteit voor kortere of langere tijd buiten bedrijf geraakt. Met behulp van een logging-mechanisme kan ervoor worden zorg gedragen dat de database in de laatst bekende integere situatie wordt teruggebracht.
Een ander van belang zijnd beveiligingsmechanisme is dat van locking tegen concurrent update (gelijktijdig bijwerken). Ieder database-managementsysteem reikt mogelijkheden van beveiliging en

1 *Op de functie van data administration, verantwoordelijk voor het effectief en efficiënt gebruik van gegevens in de organisatie, wordt omdat deze in de gebruikersorganisatie is geplaatst, in dit artikel niet ingegaan [NGI90].*

continuïteit inmiddels aan. Echter, de organisatie is ervoor verantwoordelijk dat deze maatregelen adequaat worden geïmplementeerd.

BEHEERSINGSASPECTEN VAN GROOTSCHALIGE GEAUTOMATISEERDE GEGEVENSVERWERKING

De fysieke omvang en schaalgrootte van computers, en de inzet van (gespecialiseerd) personeel in een scala van functies hebben zich in de afgelopen decennia ingrijpend gewijzigd.

In de beginjaren van de geautomatiseerde gegevensverwerking (zestiger jaren) was de geheugencapaciteit van computers weliswaar beperkt, doch vele specialisten waren nodig om deze gegevensverwerking succesvol te laten verlopen. De computers werden vervolgens in snel tempo krachtiger.
Ten gevolge van de complexiteit - niet in het minst voor wat betreft de benodigde inzet van gespecialiseerd personeel - vond de gegevensverwerking centraal plaats. De invoervastlegging verplaatste zich in de loop der tijd van een centrale data entryfunctie naar de eindgebruiker.
De hiervoor beschreven situatie kan worden gekarakteriseerd als grootschalige centrale geautomatiseerde gegevensverwerking.

Online/realtime-toepassingen eisen een hoge graad van beschikbaarheid van de computersystemen.

Pas later (tachtiger jaren) zette zich een ontwikkeling in waarbij computers decentraal werden geïnstalleerd en met behulp van datacommunicatielijnen met elkaar werden verbonden. Hiervoor werd veelal gebruik gemaakt van zogenaamde midrange-systemen, die aanzienlijk minder inzet van (gespecialiseerd) automatiseringspersoneel vereisten. In het spraakgebruik wordt het gebruik van deze systemen kleinschalige automatisering genoemd.
In geval van een automatiseringsorganisatie van grote omvang zowel qua personele bezetting als qua gebruik van computersystemen is het mogelijk een evenwichtig stelsel van maatregelen van interne controle en beveiliging te implementeren. Immers, de in gebruik zijnde computerconfiguratie(s) verlangen de inzet van een groot aantal - gespecialiseerde - functies. Primair dient daarbij te worden gedacht aan een onderverdeling in maatregelen van organisatorische, logische en fysieke aard.
Organisatorische maatregelen behelzen functiescheiding, procedures en voorschriften. Te denken valt in dit verband aan de test-, acceptatie- en overdrachtsprocedure van programmatuur, systeemontwikkelingsmethoden, programmabibliotheekbeheer, documentatievoorschriften en noodvoorzieningenplannen.
Het is van belang een en ander niet slechts op papier te hebben geregeld, doch ook te effectueren, hetgeen veelal geschiedt door implementatie van maatregelen in (besturings)programmatuur.

Logische beveiligingsmaatregelen zijn beveiligingsmaatregelen die worden uitgevoerd door computerprogramma's. In ruime zin omvatten zij alle geprogrammeerde controles om inbreuken op de betrouwbaarheid, vertrouwelijkheid en beschikbaarheid te voorkomen, te signaleren of de nadelige gevolgen ervan te beperken [Velt91], [Leen93].

Het behoeft geen betoog dat maatregelen van logische beveiliging (autorisatiecontrole) bij toenemend gebruik van online/realtime-toepassingen van grote betekenis zijn. Autorisatiecontrole heeft betrekking op het vaststellen van bevoegdheden en aansluitend (eventueel) verstrekken van toegang tot gegevens in verband met actualisering ervan of verkrijging van inzage, en het doen vervallen van bevoegdheden.

Bij fysieke maatregelen valt te denken aan voorzieningen van bouwtechnische aard met betrekking tot het computercentrum, maatregelen in verband met brandpreventie en -detectie, bescherming tegen onrechtmatige toegang, noodstroomvoorziening, airconditioning en dergelijke. De nadruk ligt hierbij in eerste instantie op maatregelen van preventieve en detectieve aard en secundair op die van correctieve aard. Enerzijds kan worden betoogd dat de betekenis van deze maatregelen afneemt, omdat de 'logische' wanden van het centrum ten gevolge van het gebruik van online/realtime-toepassingen in feite worden verplaatst naar de gebruikersomgeving (en dat kunnen ook derden zijn, waarbij kan worden gedacht aan point of sale-toepassingen), anderzijds nemen fysieke maatregelen in betekenis toe omdat juist deze toepassingen een hoge graad van beschikbaarheid van de computersystemen eisen. Preventieve en detectieve maatregelen passen hierin bij uitstek.

Het treffen van maatregelen past in het proces van risicobeheersing, dat wil zeggen: 'het bewust, integraal en dynamisch onderkennen van alle gevaren (als gevolg van het gebruik van informatietechnologie) en het streven naar een permanent en evenwichtig pakket van maatregelen om die gevaren te beperken tot een voor het management aanvaardbaar (kosten)niveau'.
Risicobeheersing dient te worden geplaatst in het kader van het beleid ten aanzien van veiligheid en beveiliging zoals dat op strategisch niveau dient te worden vastgesteld.
Informatiebeveiligingsbeleid is in dit verband een afgeleide, waarbij overigens geldt dat de ondernemingsstrategie en het daaruit voortvloeiende/afgeleide informatiebeleid inclusief de concretisering in telematica- en automatiseringsbeleid van wezenlijke invloed zijn op met name de invulling op tactisch en operationeel niveau [IFAC91].

Een kenmerk van grootschalige automatisering is dat zowel systeemanalyse en -ontwikkeling als gegevensverwerking en de technische ondersteuning daarvan op grote complexe computersystemen plaatsvinden, meestal vanuit één centrale plaats in de organisatie en onder unieke leiding. Er is sprake van een omvangrijke professionele staf.

De afzonderlijke bedrijfsonderdelen systeemontwikkeling/onderhoud, computercentrum en technische ondersteuning dragen ieder een eigen verantwoordelijkheid voor de kwaliteit van de door hen geleverde diensten.
De gebruiker is opdrachtgever aan de afdeling Systeemontwikkeling ten aanzien van nieuwe toepassingen en onderhoud aan bestaande toepassingen. Zij voert deze werkzaamheden overeenkomstig de binnen die organisatie geldende werkmethoden, hulpmiddelen en voorschriften uit.
Het computercentrum draagt de verantwoordelijkheid voor de juiste en volledige verwerking van de aan haar bevoegd aangeboden gegevens met behulp van reeds bij het computercentrum aanwezige gegevensverzamelingen. De technisch specialisten zoals systeemprogrammeurs, database administrators, netwerkbeheerders en dergelijke verlenen operationele ondersteuning aan het computercentrum, doch daarenboven implementeren zij nieuwe versies van besturingssystemen en overige besturingsprogrammatuur. De betekenis van deze technische ondersteuning bij gebruik van grote en complexe computersystemen moet niet worden onderschat. De benodigde besturingsprogrammatuur is omvangrijk en vooral complex. Het vereist gespecialiseerde deskundigheid deze programmatuur geschikt te maken voor gebruik in een specifieke omgeving. Overigens geldt dat de door deze specialisten aangeleverde programmatuur door het computercentrum zal moeten worden getest alvorens deze operationeel te maken.
Een test-, acceptatie- en overdrachtsprocedure dient zowel voor toepassingsprogrammatuur waarin de eindgebruiker een belangrijke rol speelt te gelden, als voor (besturings)programmatuur. De rol van de gebruiker wordt in het laatste geval ingenomen door het computercentrum.

KLEINSCHALIGE AUTOMATISERING EN HAAR BEHEERSINGSPROBLEMEN

Op een aantal aspecten onderscheiden midrange-(=mini)systemen en de daarbij behorende organisatie, verder te noemen kleinschalige automatisering, zich van de op mainframe georiënteerde organisaties.

Wat houdt kleinschalige automatisering in?
Computers zijn qua omvang kleiner geworden, maar veel krachtiger (groter intern geheugen, tientallen tot honderden intelligente werkstations). De eisen die computers oorspronkelijk stelden aan de fysieke omgeving (onder andere temperatuurregeling) zijn niet langer noodzakelijk in geval van minicomputersystemen. De bediening is vereenvoudigd; waren oorspronkelijk werkvoorbereiders en operators noodzakelijk om de geautomatiseerde gegevensverwerking in goede banen te leiden, thans kunnen slechts in geringe mate opgeleide eindgebruikers de verwerking ordelijk laten verlopen.
Dit zijn dan ook de belangrijkste verschillen tussen grootschalige en kleinschalige automatisering, die verstrekkende gevolgen hebben voor de organisatorische, logische en fysieke beveiliging en derhalve voor de wijze waarop de organisatie wordt ingericht en beheerst.
Het meest tastbaar is de fysieke beveiliging. Hiervoor werd reeds aangegeven dat allerhande eisen die betrekking hebben op de condities waaronder computers werken, van geringer betekenis werden. Dit had tot gevolg dat deze eenvoudig bedienbare installaties in veel gevallen op de werkplek werden geïnstalleerd. De fysieke beveiligingsmaatregelen nemen dienovereenkomstig qua aard en omvang af, hetgeen van invloed is op het stelsel van algemene maatregelen van interne controle en beveiliging. De kleinschaligheid is ook van invloed op de aard en omvang van maatregelen van organisatorische aard. Voorheen een afzonderlijke automatiseringsfunctie waarbinnen mogelijkheden van functiescheiding, ondersteund door procedures, methoden, voorschriften en technieken mogelijk waren, nu integratie van in ieder geval de verwerkingsfunctie in de gebruikersorganisatie en dus in feite een doorbreking van een opgebouwde functiescheiding die voor de kwaliteit van de interne controle van grote betekenis is.

Voor wat betreft de ontwikkeling en het onderhoud van systemen kunnen we een ander risico waarnemen. Voorheen vond ontwikkeling in opdracht van de gebruikers plaats door afzonderlijk in de organisatie werkzame systeemanalisten, systeemontwerpers en programmeurs, waarna de eindgebruiker na een test besliste of programmatuur operationeel werd. Deze test-, acceptatie- en overdrachtsprocedure is van grote betekenis voor de organisatie. Thans bestaat de mogelijkheid voor eindgebruikers met behulp van vierde-generatietalen eigen programmatuur te ontwikkelen, te testen en in produktie te nemen, alsmede te onderhouden. Risico's te over! De risico's zijn in feite van velerlei aard: zo wordt de noodzaak tot documenteren veelal niet onderkend (de ontwikkelaar is immers de gebruiker), waarom zou de ontwikkelaar/gebruiker eigenlijk testen? Het is toch goed? Hij heeft het zelf gemaakt.

Ook in het opzicht van logische beveiliging onderscheidt de kleinschalige automatisering zich van de mainframe-organisaties. De mimicomputers bieden in de standaard aanwezige besturingsprogrammatuur over het algemeen een zeer uitgebreid toegangscontrolemechanisme en in sommige situaties (afhankelijk van de architectuur van de machine) een verdergaande mogelijkheid de beveiliging van de geautomatiseerde gegevensverwerking uitstekend te regelen. Zo'n toegangscontrolemechanisme is echter slechts effectief als het correct wordt geïmplementeerd en wordt onderhouden. En hier treffen we dan ook de zwakke plek in de organisatie aan. Een parttime-functie dient in principe eenmalig aan het werk te worden gezet voor het implementeren en - vervolgens zelden -

ten behoeve van het operationeel houden van het beveiligingsmechanisme. Bij voorkeur dienen deze werkzaamheden te worden uitgevoerd door iemand die geen rechtstreekse betrokkenheid heeft bij de dagelijkse geautomatiseerde gegevensverwerking. Deze functionaris dient wel over een redelijke kennis te beschikken van die automatisering en in het bijzonder van het besturingssysteem en het daaraan gekoppelde toegangscontrolemechanisme. Zo iemand wordt vrijwel niet gevonden. De vervolgens gekozen oplossingen leiden dan in mindere of meerdere mate automatisch tot een belangenvermenging.

Met het vorenstaande wil niet gezegd zijn dat kleinschalige automatisering per definitie onbeheersbaar, fraudegevoelig, risicovol en dergelijke is. Met een dosis inventiviteit en gevoel voor realiteitszin is in de meeste gevallen een betrouwbare, beheersbare en voortdurend operationele geautomatiseerde gegevensverwerking te realiseren.

DE BEHEERSING VAN PERSONAL COMPUTERS/NETWERKEN

Een verdere miniaturisering van computers vond in de jaren tachtig plaats. De introductie van de microcomputer of personal computer was een feit. De micro is een computer die, zoals de naam reeds zegt, is bedoeld voor persoonlijk computergebruik (PC).
Het gebruik van deze apparatuur op de werkplek heeft de introductie van een aantal risico's tot gevolg. Deze risico's gelden zowel met betrekking tot de beveiliging van de geautomatiseerde gegevensverwerking, als voor de betrouwbaarheid en vertrouwelijkheid van de gegevens.

De meest tastbare problematiek zal hierna als eerste de revue passeren.
Zowel in de grootschalige als in de kleinschalige omgeving werd enige vorm van organisatorische en logische beveiliging aangetroffen. In deze automatiseringsorganisaties achtte men zich bijvoorbeeld ook verantwoordelijk voor het regelmatig aanmaken van kopieën van programmatuur en bestanden om deze vervolgens elders beveiligd op te bergen. In de PC-omgeving is uitsluitend de gebruiker ervoor verantwoordelijk dat deze kopieën van bestanden en programmatuur op diskette worden gekopieerd en beveiligd worden opgeborgen. Wie kan deze discipline opbrengen? Het risico is dan aanwezig dat zowel originele gegevensverzamelingen als kopieën ervan op dezelfde (werk)plek aanwezig blijven, waardoor in geval van brand of diefstal zowel origineel als kopie verloren kan gaan.
Ook de fysieke beveiliging van de PC is moeilijker te regelen. Immers, reeds spoedig na de introductie van de PC werden de machines 'sjouwbaar' en vervolgens draagbaar. Was het tenslotte niet handig de computer 's avonds en in het weekend mee naar huis te nemen om allerhande activiteiten daar voort te zetten?
Wil men van deze mogelijkheden afzien dan zijn inventieve oplossingen mogelijk, zoals het bevestigen van de PC aan het bureau op de werkplek of met een staalkabel aan de grond. Verder kan worden gedacht aan het met behulp van een sleutel onderbreken van de stroomvoorziening. Ook tegen het ongeautoriseerd gebruik maken van op kantoren aanwezige PC's zijn maatregelen mogelijk. Te denken valt hierbij aan het afsluiten van de diskette-ingang, het verwijderen van toetsenbord/muis en dergelijke. Moet de situatie beter worden beveiligd, dan kan worden gedacht aan het vercijferen van op de vaste schijf aanwezige gegevens; de introductie in de PC van niet-vercijferde bestanden is dan per definitie niet mogelijk.

Met de introductie van de PC vond ook die van computervirussen plaats.
Onder een computervirus dient te worden verstaan een programma dat zichzelf kan dupliceren door zich aan andere programma's te hechten. Daarnaast heeft het de mogelijkheid zichzelf te camoufleren en te beschermen, en kan het een ongewenste functionaliteit bezitten [KPMG92].

Een adequate beheersing van de PC-omgeving is moeilijk te realiseren. Er is tenslotte slechts één gebruiker die verantwoordelijk is voor data entry, verwerking, alsmede in veel gevallen de ontwikkeling van programmatuur. Juist in dit soort situaties worden voor de controle en beveiliging van de automatiseringsinspanning zeer belangrijke procedures, zoals de test-, acceptatie- en overdrachtsprocedure, bibliotheekbeheer, documentatie en dergelijke, niet gehandhaafd/nageleefd. Van enige vorm van functiescheiding is uiteindelijk geen sprake meer.

In ieder geval dient men zich te realiseren dat de output die uit een PC beschikbaar komt niet per definitie goed is omdat deze op een geautomatiseerde wijze tot stand is gekomen.
Reeds spoedig na de introductie van de PC werden mogelijkheden geïntroduceerd de afzonderlijke PC's door middel van een netwerk met elkaar te verbinden. Het functioneren werd vervolgens ondersteund door in het netwerk een zogenaamde server op te nemen.
De verschillende eindgebruikers werden verlost van een aantal werkzaamheden, zoals het aanmaken van kopieën van programmatuur en bestanden. Ook kan de toegangsbeveiliging tot het netwerk beter worden geregeld dan die tot standalone personal computers. Zo kan als gevolg van de introductie van netwerken met daarin opgenomen een server, de beveiliging beter worden geëffectueerd. Vanzelfsprekend moeten nu eisen van (fysieke) beveiliging worden gesteld aan de server, omdat deze machine immers het kritische punt in het netwerk is geworden. Deze server vereist geen afzonderlijke koeling, geen voortdurende bediening en dergelijke, zodat hij op een afgesloten plaats kan worden geïnstalleerd. Wel dient een functionaris verantwoordelijk te worden gesteld voor het beheer ervan.
Het spreekt vanzelf dat bij het aanleggen van de bekabeling van het netwerk zorgvuldigheid dient te worden betracht, omdat anders op eenvoudige wijze op het netwerk zou kunnen worden ingebroken. De bekabeling die in kabelgoten door een

openbare parkeergarage loopt vormt een uitdrukkelijk risico voor de organisatie.
Overigens wordt opgemerkt dat een veel groter gevaar aanwezig is in de veelal gebrekkige beveiligingsmogelijkheden van netwerkbesturingsprogrammatuur.
Het zou hier te ver voeren allerhande specifieke controle- en beveiligingsmaatregelen weer te geven; het gebruik van PC's al dan niet gekoppeld in een netwerk biedt ondanks alles een scala van mogelijkheden om een adequaat niveau van beveiliging te realiseren.

In het voorgaande is stilgestaan bij de ontwikkelingen die zich met betrekking tot de wijze van gegevensverwerking hebben afgespeeld. Ook de organisatorische verschijningsvorm van het gebruik van informatietechnologie kwam aan de orde en wel met betrekking tot grootschalige automatisering (met behulp van mainframes), en ten opzichte van kleinschalige gegevensverwerking (met behulp van minisystemen) en PC-ontwikkelingen.
Er zijn echter ook andere ontwikkelingen, waarvan vermelding in dit artikel zeker niet mag ontbreken.

VERDEEL EN BEHEERS: ONTWIKKELINGEN STAAN NIET STIL

Outsourcing is een ontwikkeling waarbij de automatiseringsinspanning geheel (systeemontwikkeling en operationele gegevensverwerking) of gedeeltelijk (uitsluitend de operationele gegevensverwerking) buiten de organisatie wordt gebracht om zelfstandig voort te bestaan of te worden overgedragen aan een organisatie die hierin is gespecialiseerd. Aan een dergelijke ontwikkeling kunnen verschillende overwegingen ten grondslag liggen. In veel discussies komt naar voren dat organisaties van enige omvang zich willen ontdoen van die activiteiten die niet per se tot de kernfunctie van de organisatie worden gerekend. Automatisering valt daar nogal eens onder. Een achterliggende reden is vaak dat managen van de automatisering veelal niet eenvoudig is en van het management relatief veel tijd vraagt in verband met de snelle ontwikkelingen en niet in het minst de belangrijke investeringen die daarmee samenhangen.
Een andere overweging is het niveau van de kosten terug te brengen door de activiteiten onder te brengen in organisaties die zijn gespecialiseerd in het managen van automatisering. Het kostenvoordeel dat hierdoor wordt behaald, bestaat vaak uit twee delen, te weten een deel dat wordt bereikt door stroomlijning van de organisatie, afslanking, introduceren van goede procedures en richtlijnen, werkinstructies en dergelijke (dit voordeel had de organisatie zelf dus ook kunnen behalen), en een tweede deel dat ontstaat doordat de organisatie die de verwerking overneemt, kan genieten van de voordelen van economy of scale, het ingeslepen zijn van haar organisatie in de specifieke operationele verwerking en dergelijke.
De afspraken tussen gebruiker en dienstverlener worden tegenwoordig verwoord in zogenaamde service level agreements (serviceniveau-overeenkomsten), waarin derhalve rechten en verplichtingen van uitbesteder en computercentrum dienen te zijn geregeld.

Organisaties willen zich ontdoen van die activiteiten die niet per se tot de kernfunctie worden gerekend.

Downsizing heeft betrekking op het overbrengen van delen van de operationele gegevensverwerking naar de werkplek. De betekenis van de centrale automatisering neemt daarbij af, terwijl de eindgebruiker een grotere verantwoordelijkheid ten aanzien van de operationele gegevensverwerking voor zijn organisatie-onderdeel krijgt. Deze ontwikkeling is ingetreden nadat krachtige minicomputersystemen beschikbaar kwamen en PC's en PC-netwerkoplossingen tot de mogelijkheden gingen behoren. Aan de hiermee verband houdende controle- en beveiligingsproblematiek is in het voorgaande uitgebreid aandacht besteed.

Het gebruik van vierde-generatietalen neemt in betekenis toe. Alhoewel het gebruik van deze talen is bedoeld voor de eindgebruiker, zijn ze oorspronkelijk aangewend door de automatiseringsorganisatie zelf. Nu de eindgebruikers steeds vaker het gemak van gebruik van dergelijke talen inzien, worden ook de risico's die aan het gebruik verbonden zijn, zichtbaar. Gewezen kan worden op het zeer inefficiënt programmeren door eindgebruikers die niet echt ter zake deskundig zijn. Gevolg hiervan kan zijn dat programmatuur tijdens de uitvoering de performance van de machine belangrijk beïnvloedt.
Verder kan - wellicht ten overvloede - worden genoemd het niet naleven van voor de kwaliteit van de geautomatiseerde gegevensverwerking van belang zijnde procedures en voorschriften. In dit verband kan worden gedacht aan het reeds eerder genoemde achterwege blijven van de test-, acceptatie- en overdrachtsprocedure, omdat de gebruiker zowel ontwikkelaar, gebruiker als verwerker is.
Mede hierdoor wordt vaak niet de noodzaak gevoeld een adequate documentatie op te bouwen.

Keuring en certificering van informatietechnologieprodukten (hardware, software, toepassingsprogrammatuur) heeft ten doel tot een kwaliteitsverbetering van IT-produkten te komen. Reeds in de jaren tachtig zijn activiteiten gestart om te komen tot de keuring en certificering van kwaliteitsborgingssystemen en van programmatuur. Internationaal is de ISO 9000-standaard geïntroduceerd, die zich richt op certificering van kwaliteitssystemen, waarbij voor wat betreft het gebruik van informatietechnologie kan worden gedacht aan systeemontwikkelingsorganisaties en softwarehouses.
Keuringsnormen voor toepassingsprogrammatuur zijn in ontwikkeling. De in Duitsland in gebruik

zijnde DIN-voornorm, die wordt gehanteerd bij de beoordeling van standaardpakketten, is voor Nederlands gebruik in de tweede helft van de jaren tachtig weliswaar aangepast doch sindsdien zelden toegepast. Niettemin worden standaardpakketten, en ook specifiek ontwikkelde programmatuur regelmatig getest aan normen. Deze normen, waar deze worden gebruikt door EDP-auditors, zijn veelal slechts toegesneden op betrouwbaarheids- en beveiligingsaspecten. Verwacht kan worden dat een verdere uitwerking van de toetsingsnormen zal plaatsvinden.

ELECTRONIC DATA INTERCHANGE

Electronic Data Interchange (EDI) staat voor de verzending van berichten (orders, facturen, betaalopdrachten) volgens standaardafspraken langs elektronische weg. Essentieel daarbij is het (in vergaande mate) ontbreken van tussenkomst van menselijk handelen, zodat communicatie tussen geautomatiseerde systemen van verschillende organisaties ontstaat.
In toenemende mate wordt gebruik gemaakt van EDI. Daarbij blijkt dat het toepassen van EDI niet alleen een technische aangelegenheid is, maar met name nogal wat vergt van een organisatie.
Onder invloed van EDI zullen de oorspronkelijke structuur en opzet van de interne organisatie (administratieve organisatie) veranderen, immers er ontstaat een in mindere of meerdere mate papierloze organisatie. Derhalve dienen maatregelen te worden getroffen, opdat nog steeds van een adequate kwaliteit van de organisatie kan worden gesproken.
Belangrijke pijlers in de administratieve organisatie zijn de (primaire) vastleggingen, de functiescheidingen alsmede de interne-controleprocedures.

Onder invloed van EDI zijn primaire vastleggingen steeds minder beschikbaar op papieren gegevensdragers, maar meer en meer in elektronisch formaat. Dit impliceert dat waarde moet worden toegekend aan de juistheid en volledigheid van deze elektronisch opgeslagen gegevens. Naarmate EDI verder geïntegreerd is met de interne automatisering, eist dit verdergaande algemene beheersmaatregelen met betrekking tot de kwaliteit van de automatisering(sorganisatie). Immers, ten gevolge van de onzichtbaarheid van de mutaties moet op een andere wijze worden voorzien in zekerheid. Dat wil zeggen, de gebruiker moet kunnen steunen op de handhaving en naleving van beheersingsmaatregelen in de automatiseringsorganisatie.

Interne-controlemaatregelen en -procedures die in een traditionele situatie zijn opgezet, zullen ten gevolge van de introductie van EDI op een andere wijze moeten worden gerealiseerd. Voorheen veelal handmatig uitgevoerde controles zullen in een situatie met EDI (nagenoeg) volledig geautomatiseerd worden uitgevoerd. De betrouwbaarheid van deze geprogrammeerde controles hangt af van de algemene beheersmaatregelen inzake automatisering.

Een technische consequentie van EDI betreft de communicatie langs elektronische weg. Punten van aandacht hierbij zijn de authenticiteit van de betrokken partijen, alsmede de integriteit en onloochenbaarheid van de verzonden berichten. Onder meer met behulp van de hedendaagse encryptietechnieken bestaan uitstekende mogelijkheden de authenticiteit en de integriteit te waarborgen [Lith92].

DATACOMMUNICATIE

Op verschillende plaatsen in dit artikel is reeds gewezen op het gebruik van datacommunicatiefaciliteiten. De introductie van datacommunicatie in een omgeving van geautomatiseerde gegevensverwerking betekent als het ware dat de muren van het rekencentrum worden verlegd naar de afzonderlijke terminals. Van belang is te onderkennen dat een risicogebied wordt geïntroduceerd: gebruikmaking van de datacommunicatie-infrastructuur betekent in principe dat een ieder via deze faciliteiten in andermans computersystemen zou kunnen binnendringen. Het management zal zich ervan bewust moeten zijn dat controle- en beveiligingsmaatregelen moeten worden getroffen om de risico's ter zake te beheersen.
Enerzijds, doch maatregelen van deze strekking moeten al lang zijn genomen, kunnen deze maatregelen worden gevonden in het implementeren van een toegangscontrolesysteem dat iedere gebruiker vraagt naar zijn identiteit en een persoonlijk kenmerk (password). Dat neemt overigens niet weg dat iemand door het aannemen van een valse identiteit (door trial en error of door diefstal verkregen passwords) als ongeautoriseerde toch toegang tot het geautomatiseerde systeem zou kunnen krijgen.
Anderzijds ligt het risico in de wijze waarop gegevens over datacommunicatielijnen worden verzonden. Verzenden van berichten in klare taal betekent dat kennisneming hiervan in principe mogelijk is, en wel vanaf iedere plek waar men toegang tot het netwerk zou kunnen krijgen. Dit kan dus ook de schakelkast van de PTT in een wijk zijn.
Indien kennisneming van gegevens niet problematisch wordt geacht doch het correct overbrengen van het bericht van grote betekenis is, kan over het bericht met behulp van een algoritme een controlegetal worden berekend dat aan het bericht wordt toegevoegd. De ontvanger hoeft slechts dezelfde routine over het bericht uit te voeren om vervolgens het controlegetal, de zogenaamde Message Authentication Code (MAC), te verkrijgen en te kunnen vergelijken.
Ingeval zwaardere eisen aan de vertrouwelijkheid van het datacommunicatieverkeer worden gesteld, moet worden overwogen andere encryptiemethodieken toe te passen. In dat geval wordt het bericht onder besturing van sleutels geheel vercijferd en gaat in geheimtaal naar de plaats van bestemming. Met iedere plaats van bestemming moeten afspraken worden gemaakt over de tijdens het encryptieproces gebruikte sleutels. In de organisatie zal overigens grote aandacht dienen te worden besteed aan sleutelbeheer, tenslotte heeft iedere afnemer een eigen sleutel uitgewisseld met de oorspronke-

lijke zender. Een en ander is geen sinecure, maar de eisen gesteld aan de integriteit van het gegevenstransport kunnen deze maatregelen vereisen.

Het datacommunicatieverkeer kan adequaat worden beveiligd, doch specifieke omstandigheden zullen moeten uitwijzen op welke manier het management de risico's kan beheersen.

INTEGRATIE VAN TELEFONIE EN GEAUTOMATISEERDE GEGEVENSVERWERKING

Geautomatiseerde gegevensverwerking en telefonie zijn qua ontwikkeling altijd hun eigen weg gegaan. De introductie van online- en online/real-time-gebruik van informatietechnologie betekende weliswaar het gebruik van telefonievoorzieningen, maar leidde niet tot enige vorm van integratie hiermee.
Ook de telefonie ontwikkelde zich; er ontstonden zowel openbare telefooncentrales als bedrijfstelefooncentrales die volledig gecomputeriseerd zijn. Afgezien van het gebruik van specifieke programmeertalen kunnen (bedrijfs)telefooncentrales en computers als gelijk worden beschouwd.

In de tot nu toe bestaande praktijk betekende een en ander beheersmatig, dat de geautomatiseerde gegevensverwerking veelal onder leiding stond van een directeur Automatisering, terwijl de verantwoordelijkheid voor de telefooncentrale over het algemeen was ondergebracht bij een hoofd Algemene Dienst, dan wel een andere afdeling die een algemene functie in het bedrijf vervulde.
Nu het mogelijk is zowel data, spraak, beeld als tekst over hetzelfde medium te verzenden en de afhankelijkheid van beide computers even groot is, ligt het in de verwachting dat integratie van de verantwoordelijkheid voor telefonie en automatisering in organisaties zal plaatsvinden. Dit betekent dus dat de telefonievoorzieningen onderhevig dienen te zijn aan het beveiligings- en controleregime zoals dat geldt voor de geautomatiseerde gegevensverwerking.
In dit verband is het verder van groot belang aandacht te besteden aan de kwaliteitsaspecten met betrekking tot netwerken. De kwaliteit van de organisatorische opzet van netwerkmanagement is van wezenlijke betekenis voor de beschikbaarheid van de netwerkvoorzieningen en de efficiëntie van het gebruik.

JURIDISCHE ASPECTEN VAN DE INFORMATIETECHNOLOGIE

De juridische problematiek met betrekking tot de informatietechnologie is gevarieerd. Het voert op deze plaats te ver beschouwingen te geven. Een uitgebreide behandeling ervan vindt plaats in [Duth93] en [Kemn93].

Twee wetten die rechtstreeks van invloed zijn op de kwaliteit van de organisatie van de automatisering worden hier kort aangestipt. Het betreft de per 1 juli 1990 geheel in werking getreden Wet persoonsregistraties (WPR) en de op 1 maart 1993 in werking getreden Wet computercriminaliteit (WCC).

De WPR richt zich op de bescherming van de persoonlijke levenssfeer en behandelt in dit verband onder meer de rechten en verplichtingen van houders en bewerkers van persoonsregistraties, alsmede de rechten van geregistreerden. Voor organisaties is artikel 8 van betekenis, omdat daarin wordt aangegeven dat 'de houder van een registratie zorg moet dragen voor de nodige voorzieningen van technische en organisatorische aard ter beveiliging van een persoonsregistratie tegen verlies of aantasting van de gegevens en tegen onbevoegde kennisname, wijziging of verstrekking daarvan. Voor de bewerker geldt een zelfde plicht voor het gedeelte van de apparatuur dat hij onder zich heeft, waarmee de registratie wordt gevoerd.'

Niet wordt aangegeven wat onder 'de nodige voorzieningen' wordt verstaan. Uit dit artikel zal duidelijk zijn geworden dat een eenduidig antwoord niet mogelijk is. Het is immers de verantwoordelijkheid van het management het niveau, de aard en de omvang van maatregelen (het stelsel) vast te stellen in relatie tot de aanvaarde restrisico's [KPMG93-1].
In de Wet persoonsregistraties zijn strafbepalingen opgenomen.

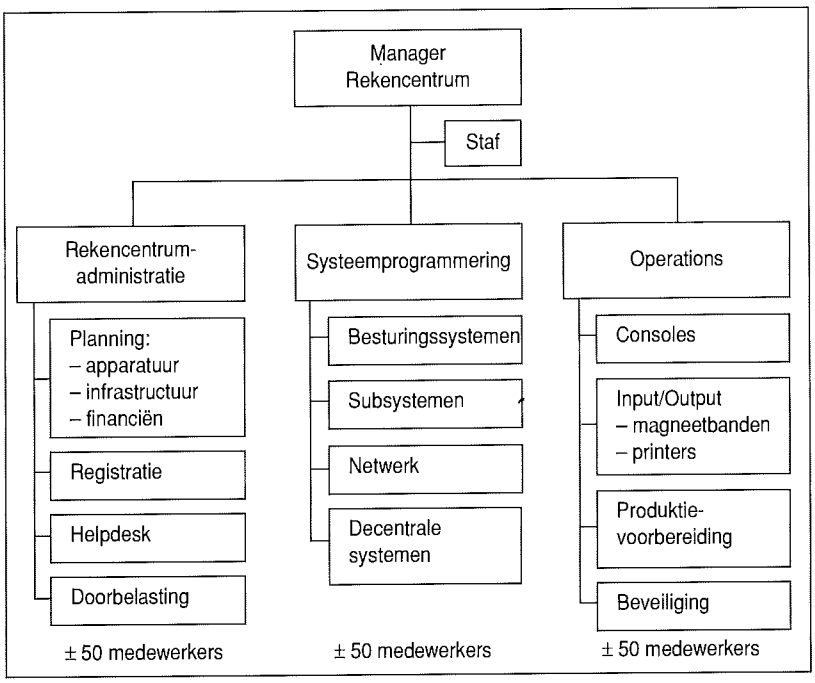
De Wet computercriminaliteit (WCC) bevat een viertal artikelen. In artikel 1 wordt een reeks wijzigingen in het Wetboek van Strafrecht weergegeven, terwijl artikel 2 wijzigingen in het Wetboek van Strafvordering behelst. Artikel 3 omvat een wijziging van BW 2: 393 lid 4 en wel de verplichting van de deskundige (= accountant) ten minste melding te maken van zijn bevindingen met betrekking tot de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking. Overigens zij opgemerkt dat tijdens de behandeling van het wetsontwerp door de minister van Justitie is uitgesproken, dat het gaat over bevindingen van de accountant die zijn opgedaan in het kader van de jaarrekeningcontrole. Artikel 4 tot slot houdt een wijziging in van de Wet op de telecommunicatievoorzieningen [KPMG93-2].
Tijdens de behandeling van het wetsontwerp is door de minister van Justitie aangegeven dat het gaat over bevindmgen van de accountant die zijn opgedaan in het kader van de controle van de jaarrekening.

De WCC stelt beveiliging van de geautomatiseerde gegevensverwerking weliswaar niet uitdrukkelijk en expliciet verplicht; echter tijdens de behandeling van de WCC in de Tweede Kamer is een amendement aanvaard dat tot een volgens betrouwbare bron ongewenst neveneffect heeft geleid. Er is daarbij namelijk een tweetal zogenaamde 'culpose delicten' toegevoegd, ofwel strafbepalingen die niet op *opzet* van de dader zien, maar op diens *schuld* aan een bepaalde strafbare gedraging of gebeurtenis. Ten gevolge van deze bepalingen is

ORGANISATIE VAN HET REKENCENTRUM

Ieder rekencentrum heeft een unieke vorm voor de technische infrastructuur en organisatie, waarbij een sterke gelijkenis herkenbaar is met sneeuwvlokken. De fraaie pluriformiteit van sneeuwvlokken vindt haar oorzaak in hun vormingsproces, waarbij iedere vlok een uniek pad door de lucht volgt. Tijdens de reis van de wolk naar de aarde komen zij alle door luchtgebieden met verschillende kenmerken, zoals ten aanzien van temperatuur en luchtvochtigheid, en kennen zij verschillende activiteitsgebieden aan hun moleculair oppervlak. Het resultaat van deze verschillende trajecten is een unieke vorm per vlok. Dit komt overeen met de vorming van rekencentra, waarbij men met verschillende structuren van de overkoepelende organisaties en met verschillende gebruikersorganisaties wordt geconfronteerd. Daarnaast is het vormingsproces onderhevig aan de interne krachtenvelden binnen deze organisaties, en de verschillende attitudes en ambities van generaties van managers en professionals. Voor een verdere toelichting op de pluriformiteit binnen de geautomatiseerde gegevensverwerking wordt verwezen naar [Paan91, Paan93].
Ondanks de verschillen in structuren en namen herkent men binnen ieder centrum een aantal overeenkomstige functies. Hiervoor zullen in het kader van dit artikel de onderstaande namen en functieomschrijvingen worden gehanteerd (zie figuur 1):

Figuur 1. Een hypothetisch rekencentrum met ongeveer 150 medewerkers en een conventionele organisatiestructuur staat model voor de praktijk.



1. Manager Rekencentrum

Deze beschikt over het algemeen over een kleine staf, die zich bezighoudt met het voorbereiden van strategische beslissingen en het onderhouden van contacten met andere organisaties. Het invoeren van een stafgroep is een kenmerk voor veel organisaties die neigen naar bureaucratie, waar hogere managers persoonlijke assistenten benoemen om zichzelf zo verder te isoleren van de werkvloer en toch enige grip te behouden op de gebeurtenissen.

2. Rekencentrumadministratie

Hoewel deze groep van afdelingen veelal een andere naam of vorm heeft, zijn de volgende activiteiten herkenbaar in vrijwel alle rekencentra:

a. Planning
Deze afdeling stelt de aanvragen op voor nieuwe apparatuur en nieuwe infrastructurele voorzieningen, zoals energievoorziening, koelapparatuur, bekabeling, verhoogde vloerruimte, opstelling van consoles, PTT-aansluitingen, enz. Zij plannen de werkzaamheden van externe monteurs en bouwvakkers, en begeleiden deze tijdens de uitvoering van werkzaamheden. Daarnaast beheert deze afdeling de budgetten met betrekking tot apparatuur, infrastructuur, programmatuuraanschaf en licenties.

b. Registratie
Iedere gebruiker dient te beschikken over een user-id, wachtwoord en accountnummer voordat toegang kan worden verkregen tot de diensten. De afdeling Registratie verstrekt, op basis van aangeleverde informatie over klanten en contracten, toegangsbevoegdheden aan de gebruikers. Dit is grotendeels een administratief proces waarbij alle toegekende bevoegdheden en verwijzingen naar de contracten op ordelijke wijze worden vastgelegd.

c. Helpdesk
Iedere gebruiker wordt op onvoorziene tijdstippen geconfronteerd met problemen, zoals een tikfout tijdens het wisselen van een wachtwoord of een dienst welke niet correct blijkt te functioneren. Deze gebruikers bellen dan de Helpdesk, waar getracht wordt eenvoudige problemen direct op te lossen of de gebruikers te adviseren over hoe zij de dienst dienen te gebruiken. Hierbij wordt gebruik gemaakt van flow-charts met de te stellen vragen en mogelijke antwoorden, om zo de eisen voor specifieke kennis voor de Helpdesk-medewerkers laag te houden. Blijkt het probleem te ingewikkeld te zijn of te worden veroorzaakt door andere operationele problemen binnen het rekencentrum, dan beperkt de Helpdesk zich tot vastlegging van de klacht en delegeert de afhandeling aan een meer gespecialiseerde afdeling. De Helpdesk is het aanspreekpunt voor alle externe gebruikers en zorgt ook voor de terugkoppeling van informatie naar de gebruikers, om zo te voorkomen dat gebruikers rechtstreeks contact opnemen met operators en systeemprogrammeurs.

d. Doorbelasting
In de computers en netwerken zijn faciliteiten aan-

wezig voor de registratie van het gebruik van de technische componenten door de informatiesystemen en de gebruikers. De afdeling Doorbelasting verwerkt deze informatie, combineert deze met de accountnummers van de gebruikers en stelt de rekeningen voor de doorbelasting op. De volgende termen worden hierbij gehanteerd:
- *Logging:* de vastlegging.
- *Accounting:* het combineren van de informatie over het gebruik van de componenten met de accountnummers en zo vaststellen wie wat heeft gebruikt.
- *Billing:* het opstellen van de rekeningen.

De doelstelling van deze afdeling is het zichtbaar maken van de kosten voor de gebruikers. Afhankelijk van het beleid van de overkoepelende organisatie wordt soms volstaan met het gebruik alleen te rapporteren, bijvoorbeeld indien er geen interne verrekening hoeft plaats te vinden en het rekencentrumbudget uit de algemene middelen wordt voldaan. Binnen andere bedrijven, zeker als deze een taak vervullen als servicebureau en diensten leveren aan andere bedrijven, worden de kosten doorbelast.

De gemiddelde omvang van de afdeling Rekencentrumadministratie is vijftig personen, van wie veelal een aanzienlijk gedeelte bezig is met het ontwikkelen, installeren en onderhouden van geautomatiseerde hulpmiddelen om de interne processen te ondersteunen en te verbeteren. Dit kunnen hulpmiddelen zijn voor het begeleiden van de Helpdesk-medewerkers bij het afhandelen van vragen van gebruikers (*expert systems*), database-pakketten voor het ondersteunen van Registratie en Doorbelasting, programma's voor het automatisch doorsturen van registratie-informatie naar verschillende systemen, enz. Er zijn centra bekend waar meer dan vijftig verschillende lokaal ontwikkelde programma's aanwezig zijn ter ondersteuning van de bovengenoemde processen, waarbij veelal de initiële ontwerper reeds lang geleden is vertrokken, nauwelijks documentatie aanwezig is en men bij voortduring onderhoud pleegt en aanpassingen aanbrengt. Hierbij blijkt dat het 'verborgen' programmeer/onderhoudswerk vaak meer menskracht vereist dan de primaire processen zelf, zodat het onduidelijk is of men hier spreekt over een operationele afdeling of over een 'development shop'.

3. Systeemprogrammering

Het besturingssysteem en de bijbehorende standaard-programmapakketten vereisen ondersteuning door specialisten, de systeemprogrammeurs. Zij installeren deze programmatuur, zetten het om van confectiewerk naar maatwerk, op maat gesneden voor de specifieke omgeving van dit rekencentrum, voeren onderhoud uit en bewaken de huidige en toekomstige kwaliteit van de dienstverlening (responsietijden, prestatiebeheer en capaciteitsplanning). Daarnaast vervullen zij vaak de oneigenlijke taak van ontwikkelaars voor lokale modificaties van de standaardprogrammatuur, gebaseerd op wensen van de interne automatiseringsorganisatie of de externe gebruikers. Bovendien participeren zij in vele interne werkgroepen die de installatie van nieuwe informatiesystemen voorbereiden, de automatisering van interne IT-processen ondersteunen, interne standaardisatie van bijvoorbeeld naamgeving voor bestanden voorbereiden, enz.
Over het algemeen is de afdeling Systeemprogrammering onderverdeeld op basis van de te ondersteunen programmatuur en bevat zij groepen of afdelingen voor het basisbesturingssysteem, subsystemen zoals database/datacommunicatie-pakketten, netwerkbeheersystemen en decentrale middelgrote systemen. De gemiddelde omvang van deze afdeling is vijftig medewerkers.

4. Operations

De basiswerkzaamheden van deze afdeling zijn het starten en stoppen van de besturingssystemen en subsystemen volgens een voorgeschreven protocol, het begeleiden van de systemen door het volgen van de boodschappen op de consoles, het verstrekken van de juiste commando's en het afhandelen van de input/output. Dit laatste heeft betrekking op het bevestigen van de juiste magneetbanden op de tape-units en het verwerken van de papieruitvoer van de printers.
Veelal is er een speciale groep of afdeling voor de voorbereiding van de produktie; deze medewerkers stellen de procedures op, bieden de opdrachten aan voor de operationele jobs en schrijven de handleidingen voor de operators. Deze werkzaamheden zijn grotendeels gekoppeld aan het interne beheer van het rekencentrum, zoals het omschakelen naar nieuwe versies van het besturingssysteem, onderhoud aan schijfgeheugens (backup en restore) en beheer en registratie van de magneetbanden. Daarnaast voert Operations werkzaamheden uit namens de gebruikersorganisaties, zoals het tijdig starten en stoppen van informatiesystemen en het aanbieden van de produktiejobs. Veel van deze werkzaamheden zijn in het verleden bij Operations ondergebracht, maar behoren in feite bij de gebruikersorganisaties thuis. Andere activiteiten die functioneel niet thuishoren bij deze afdeling, maar hier vaak wel worden uitgevoerd, zijn het ontwikkelen van hulpmiddelen voor *automated* of *unattended operations* en automatisering van de interne processen. Ook bij deze afdeling is de gemiddelde omvang ongeveer vijftig personen.

5. Beveiliging

Veelal beschikt men over één of meer beveiligingsfunctionarissen die procedures opstellen en de naleving hiervan bewaken. Aangezien men gewoonlijk de manager van de afdeling Operations als de eigenaar van de systemen beschouwt, is deze functie vaak onderdeel van de afdeling Operations. Het aantal beveiligingsfunctionarissen is afhankelijk van de omvang van de organisatie en van de vertrouwelijkheid van de te verwerken gegevens.

6. Change en problem management[1]

Deze functie is niet expliciet vermeld in figuur 1,

1 *Onder change en problem management wordt in dit artikel verstaan het beheer van de wijzigingen en problemen in de operationele omgeving. Het gelijknamige proces dat behoort bij de ontwikkeling en het onderhoud van toepassingsprogrammatuur wordt hier buiten beschouwing gelaten.*

maar wordt over het algemeen ondergebracht bij de afdeling Operations. Binnen deze functie worden alle aanvragen voor wijzigingen door de afdelingen Planning en Systeemprogrammering geregistreerd en beoordeeld, en wordt de voortgang van de afhandeling van problemen bewaakt. Deze wijzigingen en problemen kunnen betrekking hebben op de programmatuur beheerd door het centrum (exclusief de toepassingen), de apparatuur en de technische infrastructuur. Bij het hier gepresenteerde centrum met acht mainframes is het aantal wijzigingen ongeveer vijfduizend per jaar, dus zo'n twintig per werkdag. Sommige hebben betrekking op een klein detail, zoals een fix voor de PL/1 compiler, terwijl andere betrekking hebben op de installatie van een compleet mainframe.
Zoals hierboven aangegeven vindt binnen deze organisatie veel ontwikkelwerk plaats ter ondersteuning van de interne processen van de automatisering, waarbij het veelal niet duidelijk is of deze werkzaamheden betrekking hebben op het ontwikkelen van nieuwe functies of het uitvoeren van onderhoud. Vaak wordt de term onderhoud in dit kader, vooral gezien het informele karakter van de activiteiten, gebruikt voor het uitbreiden van de functionaliteit van de lokale hulpmiddelen. Daarnaast heeft veel onderhoud betrekking op het aanpassen van de zelf ontwikkelde programmatuur aan nieuwe versies van de standaard-programmaprodukten.

Het 'verborgen' of 'gecamoufleerde' ontwikkel- en onderhoudswerk binnen rekencentra heeft in de loop der decennia een aanzienlijke omvang bereikt. Dit is oneigenlijk gebruik van de daar beschikbare menskracht, aangezien deze professionele medewerkers een opleiding en training hebben gekregen voor een primair operationeel gerichte functie en veelal de basisvaardigheden van een programmatuurontwikkelaar ontberen. Vandaar dat de kwaliteit van de lokaal ontwikkelde programmatuur, inclusief de onderhoudbaarheid en de documentatie, vaak veel te wensen overlaat.

Groeiproces

Het gemiddelde rekencentrum, waarvoor ons hypothetisch rekencentrum model staat, heeft over het algemeen de volgende groeifasen doorgemaakt:

1975
Vier mainframes en 20 medewerkers, waarvan één voor Planning, tien voor Operations en vijf systeemprogrammeurs. De leiding bestond uit een manager Operations en een manager Systeemprogrammering, die beiden rapporteerden aan de manager van het rekencentrum.

1980
Vijf mainframes en 50 medewerkers, als een platte organisatie verdeeld over de afdelingen:
- Planning en Registratie (welke ook als Helpdesk en Doorbelasting functioneerde);
- Console operations (inclusief Werkvoorbereiding),
- Input/output operations;
- Systeemprogrammering (voor besturingssystemen en subsystemen);
- Netwerk-systeemprogrammering.

Iedere afdeling had een manager, die allen rapporteerden aan de manager van het rekencentrum.

1985
Tien mainframes en 100 medewerkers, waarbij het concept van een platte organisatie werd verlaten. Er kwam een laag van managers voor groepen van afdelingen tussen de afdelingsmanagers en de manager van het rekencentrum, en er werd een stafgroep gevormd voor de algemene coördinatie.

1990
Acht mainframes en 150 medewerkers volgens figuur 1, geleid door zeventien managers. Dit zijn 18,75 medewerkers per mainframe, terwijl er in 1975 slechts vijf per mainframe waren. Deze toename met 275% overtreft de groeisnelheid van organisaties volgens de Wet van Parkinson [Park60].

1992
Bij een streven naar bezuiniging op de automatisering werd door het topmanagement voorgesteld het aantal medewerkers en managers te verminderen. Het rekencentrum stelde dat hij zijn functie alleen naar behoren kon vervullen met ten minste 180 medewerkers, waarop het topmanagement in plaats van vermindering besloot tot bevriezing van het aantal arbeidsplaatsen op het huidige aantal van 150.

Op basis van de bovenstaande functionele beschrijving en geschiedenis worden hieronder de voornaamste problemen en bronnen van inefficiëntie nader beschouwd.

INCOMPATIBILITEIT

Eén der grootste problemen bij het verminderen van de kosten van de automatisering is de grote diversiteit in de systemen en hun onderlinge incompatibiliteit. Niets is uitwisselbaar en alles vereist specifieke lokale vaardigheden. Indien men uit overwegingen van schaalvergroting systemen wil samenvoegen of groepen systemen onder centraal beheer wil plaatsen, blijken deze zodanig verschillend te zijn dat een langdurig migratieproces nodig is. Pas na het converteren van de desbetreffende systemen naar een gestandaardiseerde opzet, kan men voordelen verkrijgen uit een schaalvergroting. In deze paragraaf wordt ingegaan op de oorzaken van deze diversiteit, namelijk de unieke lokale modificaties en conventies (zie figuur 2).

Lokale modificaties

Het besturingssysteem en de standaard-program-

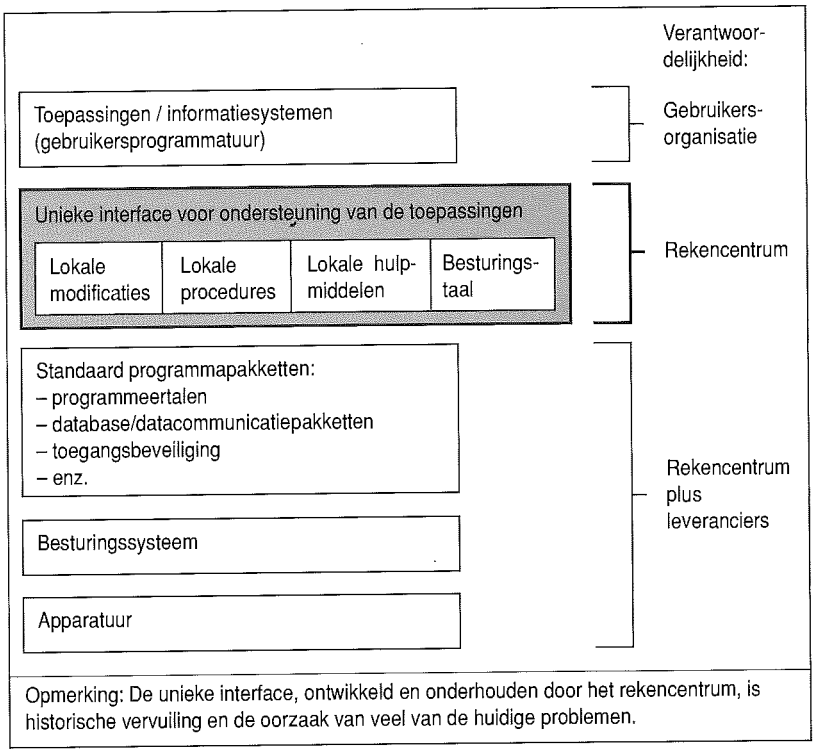
maprodukten worden door leveranciers aangeleverd op magneetband. Systeemprogrammeurs ontvangen deze magneetbanden, kopiëren de inhoud naar schijven en voeren een generatieproces uit. Dit houdt in dat programmatuur op maat wordt gesneden voor de desbetreffende omgeving. Zo wordt aan het besturingssysteem bekend gemaakt op welke I/O-adressen de schijfgeheugens aangesloten zijn, de printers, de tape-units, enz. Tijdens dit generatieproces bestaat ook de mogelijkheid om *lokale modificaties* aan te brengen in de vorm van wijzigingen van de systeemcode en aanvullingen, zoals *user SuperVisor Calls* (user-SVC's), *appendages* en *exit-routines*. Ook na afronding van het generatieproces kan het operationele systeem later nog worden uitgebreid met dergelijke modificaties. De redenen om lokale modificaties aan te brengen zijn onder andere:

1. *Het leveren van aanvullende functionaliteit*
Het besturingssysteem bevat een aantal functies ter ondersteuning van de informatiesystemen en de gebruikers. Als een systeemprogrammeur de gebruikers bijvoorbeeld een mogelijkheid wil bieden hun jobs in de wachtrij voor verwerking van een hogere prioriteit te voorzien, moet een aanvullende functie worden toegevoegd. Dit kan een user-SVC zijn, waarmee de volgorde van jobs in de wachtrij wordt beïnvloed.

2. *Het wijzigen van bestaande functies*
De systeembeheerder kan bijvoorbeeld een bepaalde syntax opstellen voor de wachtwoorden. Het systeem biedt de mogelijkheid een aantal syntaxregels in te voeren, zoals het gebruik van alfabetische, numerieke en alfanumerieke velden op bepaalde posities. Stelt de systeembeheerder echter dat een wachtwoord geen voornaam mag bevatten, dan is er een exit-routine noodzakelijk waarin aan de hand van een woordenlijst alle nieuwe wachtwoorden worden gecontroleerd. Dit is een password checker. Door het installeren van deze exit-routine wordt de syntaxverificatie van het systeem veranderd.

3. *Noodzakelijk voor standaardprodukten*
Veel programmapakketten vereisen een modificatie van het systeem. Zo zullen database/datacommunicatie-pakketten eigen user-SVC's en exit-routines introduceren, bijvoorbeeld voor uitwisseling van informatie tussen verschillende geheugengebieden en voor direct gebruik van functies van het besturingssysteem. Deze modificaties worden met het programmapakket meegeleverd en worden geïnstalleerd door de systeemprogrammeurs.

4. *Noodzakelijk voor lokale conventies*
De prioriteiten van jobs, de vastlegging van activiteiten, de toekenning van schijfruimte voor datasets en vele andere activiteiten van het systeem kunnen worden beïnvloed via exit-routines en appendages. Deze worden lokaal ontwikkeld door systeemprogrammeurs ter ondersteuning van de lokale conventies voor informatieverwerking.



Figuur 2. Schematische weergave van de opbouw van een middelgroot of groot computersysteem.

Soms hebben de lokale modificaties betrekking op specifieke apparatuur die is aangesloten op het mainframe, zoals een AS/400 welke via een kanaal is gekoppeld. Via speciale lokale programmatuur wordt deze verbinding bijvoorbeeld benut voor een toepassing die deels op het mainframe en deels op de AS/400 wordt verwerkt. Ook voor gekoppelde Original Equipment Manufacturer (OEM) apparaten zijn vaak speciale programmatische faciliteiten vereist.

Lokale procedures en hulpmiddelen

Veel rekencentra hebben tussen de binnenkomst van het eerste mainframe in de zestiger of zeventiger jaren en nu een heel stelsel van lokale conventies ontwikkeld, dat is vertaald in een combinatie van programmatuur en een verzameling van *lokale procedures*. Daarnaast hebben zij veel pakketten aangekocht van verschillende leveranciers, die nu worden benut door toepassingen van gebruikers en informatiesystemen. Dit zijn de *lokale hulpmiddelen*, welke in sommige rekencentra wel beschikbaar zijn en in andere niet.

Ook op het gebied van de *besturingstaal*, de Job Control Language (JCL), bestaan er vele lokale afspraken. Zo worden vaak groepen opdrachten voor bepaalde veelgebruikte functies al gereedgezet en gedocumenteerd voor de gebruikers, om op deze wijze een lokale standaardisatie van veel activiteiten af te dwingen.

De oorzaken van deze ontwikkelingen liggen veelal eerder op het emotionele vlak dan dat zij een

rechtvaardiging vinden binnen de zakelijke doelstellingen van het rekencentrum [Broo75]. Op basis van een verlangen naar creatieve activiteiten stellen systeemprogrammeurs, operators en andere medewerkers modificaties en uitbreidingen voor, waarvan de ontwikkeling en de implementatie door het lokale management worden goedgekeurd. Hierbij spelen, misschien onbewust, minder rationele aspecten een rol, zoals het streven naar het verzamelen van meer verantwoordelijkheden binnen de eigen afdeling, het zo garanderen van de werkgelegenheid binnen deze afdeling en de wens de eigen medewerkers tevreden te houden. Het resultaat van deze ontwikkelactiviteiten is, mede door de geïsoleerde opstelling van veel rekencentra in het verleden, de creatie van een unieke vorm van dienstverlening. Dit was in de ogen van de initiatiefnemers noodzakelijk om de afnemers te ondersteunen en het beeld van het rekencentrum als dienstverlenende instantie te bevestigen.

Datgene wat gedurende ruim twee decennia is gegroeid aan lokale ontwikkelingen kan niet eenvoudig worden verwijderd en er is voortdurend menskracht nodig voor het onderhoud.

Gevolgen van incompatibiliteit

In figuur 2 is aangegeven dat de lokale faciliteiten een interface vormen tussen de standaardprogrammatuur, aangeleverd door de leveranciers, en de toepassingen van de gebruikersorganisaties. Het kernprobleem hierbij is dat, zoals hierboven geschetst, deze interface vrijwel *uniek* is per rekencentrum of zelfs, binnen sommige rekencentra, per systeem of per groep van systemen. De gevolgen van deze in het verleden ingevoerde unieke interface zijn:

1. Aangezien de toepassingen gebruik maken van de interface, kan deze niet meer worden verwijderd zonder de produktie in gevaar te brengen. Een migratie naar een ongemodificeerd systeem is, door de complexiteit van de bestaande informatiesystemen, verre van eenvoudig.

2. Het onderhoud van deze interface is in de loop der jaren een kostbare zaak geworden voor de afdelingen Systeemprogrammering en Operations. Veel van de lokale faciliteiten zijn ontwikkeld zonder gebruik te maken van standaard-interfaces van het systeem, zijn niet of slecht gedocumenteerd en zijn niet geschikt voor nieuwere versies van het besturingssysteem. Het resultaat is een voortdurende onderhoudsactiviteit, te zamen met de noodzaak regelmatig gedeelten van de lokale code te herschrijven.

3. De medewerkers die hebben bijgedragen aan het ontwikkelen van de interface zijn vaak al vertrokken naar andere functies, andere afdelingen of andere bedrijven. Door de afwezigheid of, indien aanwezig, de matige kwaliteit van de documentatie is moeilijk na te gaan hoe specifieke modificaties werken en hoe men deze moet onderhouden.

4. Het rekencentrum is en blijft verantwoordelijk voor de unieke interface. Terwijl voor problemen met de standaardapparatuur en -programmatuur onderhoudscontracten zijn afgesloten met de leveranciers, waarmee een deel van de verantwoordelijkheid bij de leveranciers is ondergebracht, zal het rekencentrum zelf alle problemen met de lokale interface moeten oplossen.

5. Doordat informatiesystemen afhankelijk zijn van deze lokale interface, is de *transporteerbaarheid* geweld aangedaan. Het overbrengen van een informatiesysteem naar een ander mainframe of een ander rekencentrum levert daardoor ernstige en soms zelfs onoverkomelijke problemen op.

6. Bij het consolideren van rekencentra blijken de lokale interfaces niet uitwisselbaar te zijn, waardoor men na de consolidatie nog de ervaringen van medewerkers van alle samengevoegde centra nodig heeft om de lokale interfaces te onderhouden. Hierdoor worden voordelen ten gevolge van de schaalvergroting bij consolidatie deels teniet gedaan.

Datgene wat gedurende ruim twee decennia is gegroeid aan lokale ontwikkelingen kan niet eenvoudig worden verwijderd en er is voortdurend menskracht nodig voor het onderhoud.

Bij deze *historische vervuiling* is sprake van een managementproblematiek. Ondanks dat er vrijwel nooit verzoeken waren van de gebruikersorganisatie voor al deze faciliteiten, hebben deskundigen binnen de automatisering steeds op eigen initiatief voorgesteld extra of gewijzigde functionaliteit te bieden. Veelal gebeurde dit met nobele intenties, omdat men de systemen veiliger wilde maken of het gebruikersgemak wilde vergroten. Veel automatiseringsmanagers hebben deze ontwikkeling actief gesteund of oogluikend toegestaan. Een motivatie die men nog steeds verneemt in deze omgevingen is: *'prima, weer brood op de plank'* Zowel het topmanagement als het management van de gebruikersorganisaties was niet op de hoogte of niet geïnteresseerd, zodat de deskundigen in kwestie binnen de rekencentra nimmer enig tegengas kregen. Hierbij was sprake van het door dr. K.IJ. Mollema [Moll91] gesignaleerde paternalisme, waarbij de automatiseerders ook zonder expliciete verzoeken van de gebruikers wisten wat goed was voor die gebruikers. In de tijd dat men over voldoende budgetten beschikte, kon men zonder enige zakelijke rechtvaardiging of kosten/baten-analyse bouwen aan de systemen, waarmee complete kaartenhuizen aan lokale conventies werden geconstrueerd.

Nu men de kosten moet verminderen en in dat kader tracht informatiesystemen te transporteren, de werklast van verschillende computers samen te

voegen, rekencentra te consolideren en automatiseringsorganisaties in omvang te reduceren, ontdekt men dat zoiets vaak onmogelijk is door deze kaartenhuizen. Hierbij is de naam kaartenhuis voor de unieke interface opzettelijk gekozen: vaak blijkt dat als men maar iets verandert in dit stelsel, het geheel niet meer werkt. Alles hangt met alles samen, waardoor een stapsgewijze afbouw van de lokale conventies veel deskundigheid en een zorgvuldige voorbereiding en planning vereist.

Verbeteren van compatibiliteit

Het analyseren van problemen toont veelal aan hoe men deze kan oplossen. Als men de incompatibiliteit van systemen wil verminderen is daarvoor, mede gezien de menselijke aspecten van de professionele medewerkers die hun geesteskinderen zien verdwijnen, een doelgericht beleid nodig. Men zal namelijk veel weerstand, zowel vanuit de eigen organisatie als van de zijde der afnemers, moeten overwinnen. Gebaseerd op de bovenstaande analyse moet dit beleid de volgende stappen omvatten:

1. Kwantificeer de voordelen van het verbeteren van de compatibiliteit, zoals de centrale installatie en onderhoud van de programmatuur, uitbesteding van specifieke werkzaamheden, reductie van de onderhoudskosten van de lokale modificaties en procedures, transporteerbaarheid van toepassingen, enz. Het beleid moet op een degelijke financiële rechtvaardiging zijn gebaseerd ter vereenvoudiging van de acceptatie door de betrokkenen.

2. Definieer een standaard waaraan alle systemen moeten voldoen, zoals een basisplatform dat standaard-programmapakketten bevat, onderhouden door leveranciers.

3. Sta geen lokale wijzigingen toe van het basisplatform. De gehele verantwoordelijkheid voor deze programmatuur ligt bij de leveranciers en moet daar blijven liggen. Iedere wijziging zal nieuwe incompatibiliteit veroorzaken en het streven naar uitwisselbaarheid en transporteerbaarheid teniet doen.

4. Gebruik dit basisplatform op alle nieuwe systemen en op die bestaande systemen waar men met relatief lage kosten de lokale afwijkingen kan elimineren.

5. Eis voor alle nieuwe toepassingen dat zij passen op het basisplatform en alleen gebruik maken van door de leveranciers gedocumenteerde interfaces en functies, waarbij de leveranciers de functionele compatibiliteit garanderen voor de toekomstige versies van deze standaardprogrammatuur.

6. Benoem de oude, niet naar het basisplatform gemigreerde systemen tot een *sterfhuisconstructie*. De doelstelling van deze constructie is een toekomstige verwijdering van de afwijkende systemen door het afbouwen of transporteerbaar maken van de momenteel ondersteunde informatiesystemen. Dit houdt in dat op deze systemen geen nieuwe toepassingen meer mogen worden geïnstalleerd, geen nieuwe ontwikkelingen meer mogen worden uitgevoerd en het onderhoud tot het uiterste minimum wordt gereduceerd, alleen gericht op het in de lucht houden van deze systemen. Deze status van *'verouderend systeem'* moet duidelijk worden gecommuniceerd aan de afnemers, zodat zij bij hun nieuwe plannen voor hun toepassingen niet voor verrassingen komen te staan.

7. Voer sancties in voor de afnemers die hun toepassingen niet aanpassen aan het basisplatform. Dit kan in de vorm van een lagere kwaliteit van de dienstverlening of via financiële maatregelen, zoals het verhogen van de door te belasten kosten. Alleen als het afwijken van de standaarden zichtbare gevolgen heeft voor de afnemers, zullen deze bereid zijn tot migratie over te gaan.

Het uiteindelijke doel is alle systemen van het basisplatform te voorzien en alle toepassingen daarvan gebruik te laten maken. Niettemin kan men in een eerdere fase, als slechts een gedeelte van het rekencentrum is gemigreerd naar de standaard, al gebruik maken van de voordelen van schaalvergroting en de transporteerbaarheid van de toepassingen, ter verlaging van de totale kosten.

Aan de afnemers die hun verzet tegen een migratie voortzetten en hun incompatibele toepassingen willen continueren, kan men de eis stellen dat zij de hieraan gekoppelde kosten vergoeden.

Aan de afnemers die hun verzet tegen een migratie voortzetten en hun incompatibele toepassingen willen continueren, kan men de eis stellen dat zij de hieraan gekoppelde kosten vergoeden. Dit impliceert dat alle kosten voor de in het sterfhuis ondergebrachte systemen worden geïsoleerd en rechtstreeks in rekening worden gebracht aan de desbetreffende afnemers. Als men daarnaast een kostenreductie bereikt voor de systemen met het basisplatform, zal er een financiële prikkel ontstaan die de afnemers motiveert te participeren in deze noodzakelijke standaardisatie-activiteit.

INZET VAN MENSKRACHT

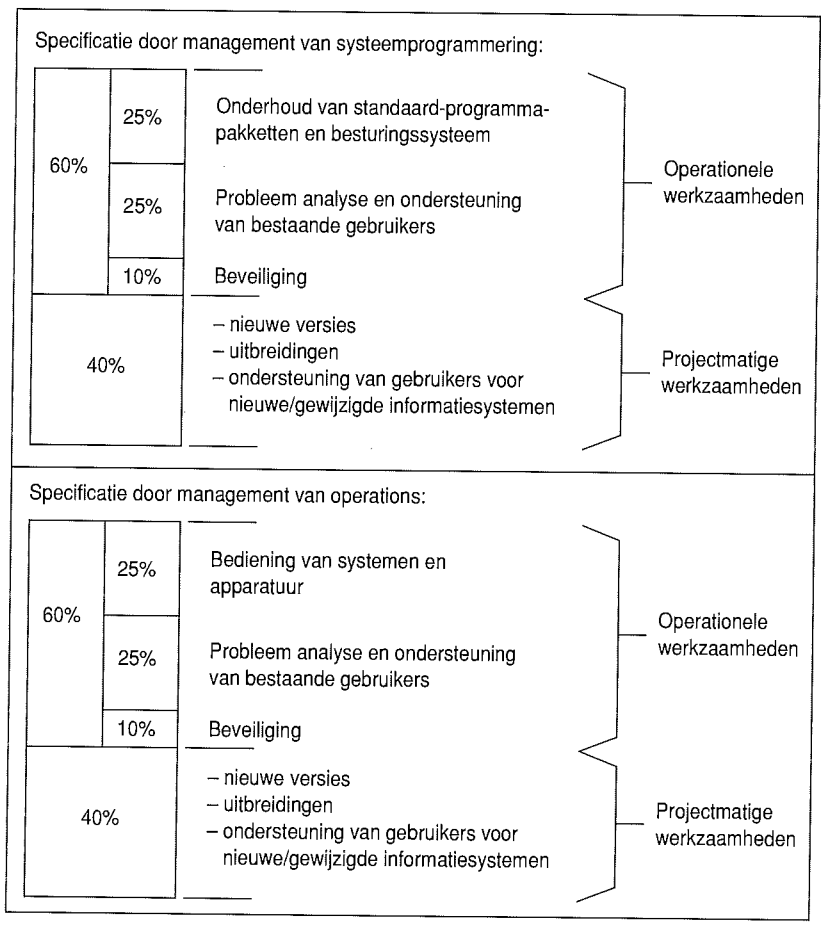
Bij het beschouwen van de inzet van menskracht binnen het rekencentrum blijkt dat het lokale management of niet weet hoeveel tijd de medewerkers besteden aan de verschillende werkzaamheden, of tracht een mogelijk gebrek aan produktivi-

teit te camoufleren met een rookgordijn. Aan EDP-auditors in opleiding wordt daarom de volgende boodschap meegegeven: 'Als automatiseerders informatie verstrekken over menskracht in de vorm van een verantwoording van de huidige activiteiten, een schatting van de kosten of een voorspelling van de toekomstige besparingen, verifieer dan het realiteitsniveau van deze informatie'.
Veelal wordt men geconfronteerd met onduidelijkheid, onwetendheid, rookgordijnen of een ongefundeerd overmatig optimisme, waardoor steeds een nader onderzoek naar meer realistische informatie over de inzet van menskracht noodzakelijk is. Automatisering is niet vergelijkbaar met een fabriek of werkplaats, waar de produktiviteit relatief eenvoudig wordt gemeten en waar de activiteiten op ondubbelzinnige wijze waarneembaar zijn. In deze paragraaf wordt ingegaan op de eigen visie van het automatiseringsmanagement op de inzet van menskracht.

Verantwoording van de huidige werklast

Binnen een rekencentrum met mainframes zijn gemiddeld 150 personen werkzaam voor het installeren en onderhouden van de systemen en het ondersteunen van de dienstverlening. Deze populatie is historisch gegroeid over twee of meer decennia. Gezien het streven naar kostenreductie mag men nu de kritische vraag stellen of dit aantal echt noodzakelijk is voor de kernactiviteiten. In het kader van deze vraag heeft de auteur van dit artikel een onderzoek uitgevoerd bij een aantal bestaande rekencentra naar de werkelijke activiteiten van deze medewerkers.

Figuur 3. Verdeling van de werkzaamheden in de bestaande, conventionele organisatie van het rekencentrum.



Aangezien in het verleden tijdens iedere planningscyclus voornamelijk aandacht werd besteed aan de delta's, namelijk de toename of afname van het aantal personen per project of afdeling, was een inventarisatie een geheel nieuw fenomeen voor de automatiseerders. De volgende vraag werd voorgelegd aan de afdelingsmanagers: 'Hoeveel van de menskracht binnen uw afdeling wordt besteed aan operationele activiteiten, hetgeen inhoudt het ondersteunen van de bestaande informatiesystemen in een stabiele situatie, en hoeveel aan andere projecten?' In hoofdlijnen zijn de antwoorden voor de afdeling Systeemprogrammering als volgt samen te vatten (zie figuur 3):

1. 60 procent van het werk had betrekking op operationele werkzaamheden in een stabiele omgeving en werd genoemd 'het brandend houden van de kachel'. Dit betrof 30 van de 50 systeemprogrammeurs. De onderverdeling was:

a. 25 procent van het werk was gericht op het onderhoud van bestaande besturingssystemen in een stabiele situatie, hetgeen alleen het aanbrengen van noodzakelijke correcties inhoudt. Deze worden als Program Temporary Fixes (PTF's) maandelijks aangeboden door de leverancier en worden door systeemprogrammeurs aangebracht en getest. Van de 50 waren dus 12,5 medewerkers bezig met deze activiteit, volgens de opgave van de manager Systeemprogrammering. Het aanpassen van de lokale modificaties was geen onderdeel van deze post, aangezien deze voornamelijk worden aangepast bij nieuwe versies van het besturingssysteem. Deze waren uitgesloten volgens de vraagstelling.

b. 25 procent, dus ook 12,5 medewerkers, was bezig met probleemanalyse en het oplossen van klachten, die via de Helpdesk of andere kanalen binnenkwamen. Bij de onderzoeker resulteerde dit in de verbaasde vraag: 'Is de kwaliteit van de geleverde diensten zo laag?' Een aanzienlijk gedeelte van de te behandelen klachten had betrekking op de lokale afwijkingen ten opzichte van standaard-programmapakketten en operationele problemen met lokaal ontwikkelde informatiesystemen, waarbij men in het ontwikkelstadium onvoldoende rekening had gehouden met de vereisten van een operationele omgeving. Gezien het onvoorspelbare karakter van de problemen gaven veel managers de voorkeur aan het reserveren van een aanzienlijke hoeveelheid extra menskracht, om zo op calamiteiten voorbereid te zijn.

c. 10 procent, dus 5 medewerkers, was betrokken

bij beveiliging. Dit was onder andere het ontwikkelen van lokale modificaties van de programmatuur voor logische toegangsbeveiliging, aangevuld met het ondersteunen van de afdelingen Registratie en Helpdesk. Ook het ontwikkelen van nieuwe hulpmiddelen voor deze afdelingen werd onder het onderwerp beveiliging opgenomen, aangezien men dit als een essentiële activiteit beschouwde.

2. De resterende 40 procent van het werk, dus 20 medewerkers, had betrekking op projectmatige activiteiten. Uit een specificatie bleek dat de meeste van deze projecten niet werden uitgevoerd op verzoek van afnemers, maar gericht waren op een verbetering van de interne processen van de automatiseringsorganisatie. Er werden projecten genoemd zoals het geautomatiseerd transporteren van een nieuw, getest besturingssysteem naar de acht mainframes en het herzien van de naamgeving van de datasets en bestanden van de systeemprogrammeurs. Slechts een beperkt aantal projecten had betrekking op verzoeken van afnemers voor ondersteuning bij gewijzigde informatiesystemen of voor installatie van nieuwe informatiesystemen.

Zoals aangegeven in figuur 3 kwamen de antwoorden van de afdeling Operations sterk overeen met die van Systeemprogrammering. Ook van andere managers kwamen overeenkomstige antwoorden. Globaal besteedde iedere afdeling 60 procent van de menskracht aan het in de lucht houden van de bestaande diensten. Deze verdeling was volstrekt niet in lijn met de verwachtingen van het topmanagement bij de aanvang van dit onderzoek.

EVALUATIE VAN DE VERANTWOORDING

Na afronding van de inventarisatie naar de inzet van menskracht werd de volgende vraag voorgelegd aan de desbetreffende afdelingsmanagers: 'Welke activiteiten kunnen worden afgestoten of uitgesteld ter besparing van menskracht?' Ook hierbij waren de antwoorden unaniem: alle managers vonden dat, als er een besparing zou worden geforceerd, de door de afnemers gevraagde projecten maar moesten worden uitgesteld. Op het onderdeel 'operationele werkzaamheden' was geen enkele besparing mogelijk, terwijl geen enkele manager één van de interne projecten aanbood voor uitstel. Dit was een sterk signaal dat de aandacht voor het belang van de gebruiker sterk was verminderd bij de onderzochte organisaties.

Een verdere evaluatie gaf aan dat de specificatie niet geheel objectief was. De werkelijke factor onderhoud bij Systeemprogrammering lag eerder ruim onder de 10 procent in plaats van op de genoemde 25 procent, terwijl ook de 25 procent probleemanalyse en ondersteuning van bestaande gebruikers veel te hoog was ingeschat door de managers. Met betrekking tot het onderwerp beveiliging was de conclusie dat veel van deze activiteiten niet thuishoorden bij de afdeling Systeemprogrammering en dienden te worden stopgezet of te worden gedelegeerd aan andere afdelingen.

Tijdens dit onderzoek bleek dat een deel van de werktijd in het geheel niet kon worden verklaard op basis van de functionele verantwoordelijkheden; het management had geen verklaring voor dit 'gat' in het overzicht en veronderstelde dat dit werd veroorzaakt door onduidelijke definities van de gehanteerde begrippen. Bij andere afdelingen, zoals Operations, Registratie en Doorbelasting, werden vergelijkbare conclusies getrokken. Ook daar waren sommige arbeidsplaatsen duidelijk betrokken bij de kernactiviteiten, terwijl het nut van andere arbeidsplaatsen op geen enkele wijze duidelijk werd. Een nader onderzoek toonde aan dat een deel van het 'gat' was gerelateerd aan ontwikkeling en lokale modificaties, een activiteit die veelal nauwelijks expliciet is te herkennen in de planning van de menskracht van een rekencentrum.

Alle managers vonden dat, als er een besparing zou worden geforceerd, de door de afnemers gevraagde projecten maar moesten worden uitgesteld.

Soms wordt de vraag naar mogelijkheden voor besparingen op menskracht gesteld door het topmanagement. Veelal beantwoordt het automatiseringsmanagement deze vraag op dezelfde wijze als hierboven is aangegeven, namelijk met het voorstel om de door de afnemers gevraagde projecten te schrappen. Dit zijn vaak projecten die samenhangen met plannen van het topmanagement voor nieuwe diensten en iedere vertraging van deze ambitieuze plannen is ongewenst. Het resultaat van deze discussie is gewoonlijk de gevraagde bezuinigingen achterwege te laten en het huidige aantal arbeidsplaatsen te bevriezen.

Variatie in aantallen

Een ander kenmerk van het onduidelijke beleid is het 'spelen met aantallen', zodra wordt gevraagd om een uitsplitsing van de kosten per informatiesysteem. Een gegeneraliseerd voorbeeld hiervan is uitgewerkt in figuur 4 op de volgende pagina. Als het management niet zeker weet hoe de menskracht wordt ingezet in het kader van de zakelijke doelstellingen van de overkoepelende organisatie, wordt de beantwoording van vragen vaak afhankelijk van de vraagstelling. Stel dat een rekencentrum werkt voor twee grote gebruikersorganisaties, namelijk ABC en XYZ, die beide gebruik maken van een eigen informatiesysteem. Deze afnemers zijn een onderdeel van de overkoepelende organisatie. Zolang er sprake is van een normale

Vraag 1. *Hoe moeten de medewerkers worden doorbelast aan de gebruikersorganisaties?*
Het antwoord luidt (MJ = mensjaren):

Operationele ondersteuning (overhead bij doorbelasting) 70 MJ	Informatie-systeem ABC 40 MJ	Informatie-systeem XYZ 40 MJ	De som is 150 MJ

Vraag 2. *Als het informatiesysteem ABC wordt overgedragen aan een ander rekencentrum, hoeveel arbeidsplaatsen kunnen dan worden ingeleverd?*
De huidige bezetting wordt dan als volgt gespecificeerd:

Operationele ondersteuning 85 MJ	ABC 10 MJ	XYZ 55 MJ	De som is 150 MJ

Vraag 3. *De gebruikersorganisaties verlangen een specificatie van de in hun ogen te hoge overhead.* Dan wordt de volgende indeling gepresenteerd:

Operationele ondersteuning 30 MJ	ABC 60 MJ	XYZ 60 MJ	De som is 150 MJ

Figuur 4. Specificatie van de werkzaamheden, waarbij de gepresenteerde aantallen afhankelijk zijn van de vraagstelling. De som blijft hierbij constant.

planningscyclus zal de manager van het rekencentrum de inzet van menskracht als volgt verantwoorden:

1. 70 mensjaren worden besteed aan de infrastructuur waarin de informatiesystemen worden verwerkt, zoals de besturingssystemen, beveiliging, bediening, netwerken, enz. Deze kosten worden gezien als overhead.

2. 40 mensjaren zijn direct gerelateerd aan het informatiesysteem ABC en eveneens 40 aan XYZ. Deze kosten worden, verhoogd met de overhead voor de infrastructuur, doorbelast aan de afnemers.

Op zich is dit een redelijke verdeling; een aanzienlijk gedeelte van de werkzaamheden heeft betrekking op het leveren van een omgeving waarin de informatiesystemen kunnen draaien en wordt terecht als overhead beschouwd.

Stel dat afnemer ABC nu overweegt zijn informatiesysteem onder te brengen bij een onafhankelijk servicebureau. De vraag die nu wordt gesteld aan de manager van het rekencentrum is: 'Hoeveel arbeidsplaatsen besparing levert dit op?' Aangezien de oorspronkelijke verdeling door onduidelijkheid van de verantwoording van de werkzaamheden op drijfzand was gebaseerd, zal de manager het zekere voor het onzekere nemen en alleen die arbeidsplaatsen inleveren die werkelijk direct gerelateerd zijn aan het informatiesysteem ABC. Met een forse veiligheidsmarge is hij bereid tien arbeidsplaatsen in te leveren (zie figuur 4). De post operationele ondersteuning wordt daarbij verhoogd van 70 tot 85 arbeidsplaatsen: hierdoor zal het verdwijnen van ABC slechts een marginaal besparingseffect hebben, aangezien deze infrastructuur nog steeds in stand moet worden gehouden voor XYZ. Met deze schatting heeft hij de zekerheid dat het topmanagement van de overkoepelende organisatie de plannen van ABC niet zal steunen: de kosten van het inhuren van computertijd en ondersteuning bij een extern servicebureau zullen de besparing van tien arbeidsplaatsen ruim overtreffen. Voor de overkoepelende organisatie impliceert zo'n overstap van ABC een verhoging van de kosten. Op deze wijze wordt ABC geforceerd de diensten van dit rekencentrum te blijven afnemen en verandert er niets in de doorbelasting.

Spelen met getallen komt veel voor in de automatisering. Zolang er geen duidelijke functiebeschrijvingen bestaan voor de afdelingen en algemeen aanvaarde normen voor het aantal arbeidsplaatsen per functie, is het voor EDP-auditors en topmanagement moeilijk, zo niet onmogelijk, zich een objectief beeld te vormen van de werkelijke kosten van de ingezette menskracht per informatiesysteem.

NORMEN VOOR ARBEIDSPLAATSEN

Bij de rekencentra heeft de afgelopen twee decennia een aanzienlijke wildgroei plaatsgevonden, waarbij de groeisnelheid van de organisatie die van 5,2 tot 6,6 procent per jaar volgens de Wet van Parkinson [Park60] ruim overtrof. Hierbij zijn vele arbeidsplaatsen gecreëerd en gerechtvaardigd die bij een objectieve beschouwing niet direct bijdragen aan de doelstellingen van het rekencentrum. Het blijkt zeer moeilijk te zijn in deze omgeving een reductie van het aantal arbeidsplaatsen te realiseren, aangezien de ter zake deskundige managers behoren tot de organisatie van het rekencentrum en geen enkel belang hebben bij een dergelijke vermindering.

Een evaluatie van de benodigde menskracht in een rekencentrum dient daarom niet uit te gaan van de huidige organisatie, maar te starten vanaf de basis. Indien men een *nieuw rekencentrum* moet creëren, start men met het inventariseren van de kernactiviteiten en de daarmee geassocieerde functies voor de medewerkers, welke daarna worden vertaald in aantallen arbeidsplaatsen. Dit is de gebruikelijke 'zero base budgeting'-benadering.

De volgende doelstelling van het hypothetisch rekencentrum geldt als uitgangspunt (zie het organogram in figuur 5): Het leveren van een omgeving voor de verwerking van informatiesystemen met databases en een netwerk, inclusief de ondersteuning van de gebruikers.

Bij deze casus wordt verondersteld dat, op basis van deze doelstelling, acht mainframes zijn geïnstalleerd, namelijk:
- een netwerkbeheersysteem;
- een backup van het netwerkbeheersysteem;
- vier produktiemachines (gebaseerd op het aantal te leveren diensten en de operationele werklast);
- een backup-systeem voor de produktie, dat

ook wordt gebruikt als onderhouds- en testomgeving van systeemprogrammeurs;
- een developmentsysteem voor applicatieprogrammeurs.

De relevante kwaliteitseisen, overeengekomen via service level agreements (SLA's) met de gebruikersorganisaties, zijn bijvoorbeeld:

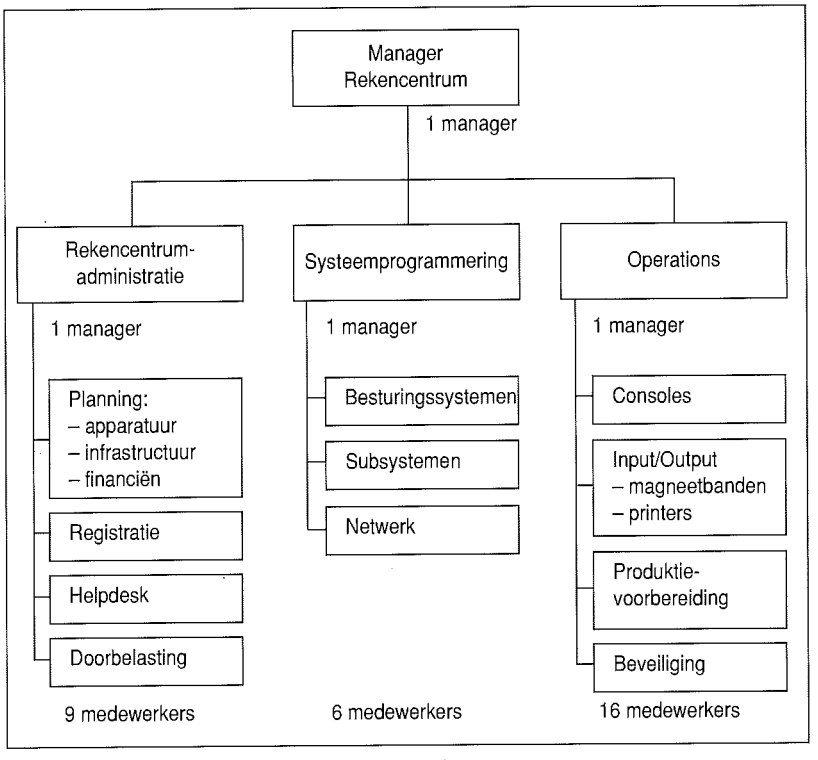
- Beschikbaarheid van de interactieve diensten op werkdagen van 06.00 tot 23.00 uur.

- Op de overige tijden en tijdens feest- en weekenddagen mogen de diensten onbemand worden geleverd.

- Beschikbaarheid van de Helpdesk op werkdagen van 08.00 tot 18.00 uur, daarna wordt de telefoon op werkdagen opgenomen door operators.

- Afhandeling van magneetbanden en papieruitvoer gedurende 24 uur per werkdag.

De doelstelling en de kwaliteitseisen bepalen het aantal benodigde medewerkers, waarbij de volgende schatting is gebaseerd op waarnemingen in de dagelijkse praktijk van bestaande rekencentra. Hierbij is onderscheid gemaakt naar het aantal personen dat *werkelijk* aan de onderstaande functies werkt en de andere medewerkers, die betrokken zijn bij lokale modificaties, programmatuurontwikkeling en andere activiteiten die niet direct passen binnen de genoemde doelstelling. De schatting voor een minimaal vereiste bezetting van dit centrum is:



Figuur 5. Het rekencentrum met een minimale personeelsbezetting van 35 personen, dat in staat is de primaire doelstelling te vervullen.

1. Afdeling Rekencentrumadministratie.

Hier zijn vier gescheiden functies te onderkennen:

a. *Planning.* Minimaal twee personen zijn nodig voor het opstellen van aanvragen voor nieuwe apparatuur en infrastructurele voorzieningen, het plannen van de werkzaamheden van externe monteurs en bouwvakkers, en het begeleiden van deze werkzaamheden.
Daarnaast is er een deeltijdfunctie voor het bestellen van nieuwe programmatuur en het administreren van licenties en budgetten. Vaak wordt deze functie gecombineerd met die van de rekencentrumsecretaresse.
Een backup voor vakanties is niet nodig bij deze functie, aangezien de medewerkers bij het opstellen van de plannen al rekening kunnen houden met hun vakanties.

b. *Registratie.* In het kader van de afgesloten contracten met de gebruikersorganisaties dienen user-ids, wachtwoorden en accountnummers te worden toegekend. Indien men beschikt over het juiste database-pakket voor het geordend vastleggen van deze informatie, kan men volstaan met twee medewerkers voor deze grotendeels administratieve functie.

c. *Helpdesk.* Van 08.00 tot 18.00 moet iemand de telefoon opnemen voor klachten en vragen van gebruikers. In principe kan hierbij een *voice-computer* worden ingezet, zoals momenteel bij veel rekencentra reeds gebeurt. Men kan daarna volstaan met twee medewerkers, waarbij met de collega's binnen deze afdeling wordt afgesproken dat zij tijdens vakanties en ziekte assisteren met het opnemen van de telefoon. Hierbij past de opmerking dat een voice-computer zeer geschikt is voor het spreiden van de werklast van de Helpdesk, aangezien gebruikers een verzoek voor terugbellen kunnen inspreken, en kan worden gebruikt om de binnenkomende gesprekken in te delen op basis van de urgentie van het verzoek.
Een voice-computer is zeer geschikt voor het spreiden van de werklast van de Helpdesk.

d. *Doorbelasting.* Hierbij nemen wij aan dat de programmatuur voor het rapporteren van het gebruik van de systeemcomponenten door informatiesystemen en gebruikers, en het printen van de rekeningen al is geïnstalleerd. Het definiëren van de klanten en hun accountnummers is daarna grotendeels een eenmalige activiteit, waarvoor tijdelijke medewerkers kunnen worden ingehuurd. Daarna zijn de operationele activiteiten beperkt tot het verwerken van wijzigingen in het klantenbestand, het maandelijks printen en controleren van de rekeningen en overzichten, en het herstellen van fouten. In deze stabiele omgeving zijn twee medewerkers voldoende voor het afhandelen van de lopende zaken.

Deze afdeling kan functioneren met negen personen, inclusief de rekencentrumsecretaresse. Bij

multifunctioneel optreden van een aantal medewerkers kan afwezigheid door vakanties, ziekte, enz. binnen redelijke grenzen worden opgevangen.

2. Afdeling Systeemprogrammering

a. Voor generatie van het besturingssysteem en de standaardprogrammatuur zijn twee systeemprogrammeurs voldoende, mits men slechts één type besturingssysteem ondersteunt. Bij meer typen neemt het aantal systeemprogrammeurs overeenkomstig toe vanwege de specifieke deskundigheden.

b. Voor onderhoud van deze programmatuur is één systeemprogrammeur voldoende. Deze brengt de maandelijks door de leverancier verstrekte correcties aan via grotendeels geautomatiseerde procedures. Hierbij is het niet nodig zelf het wiel uit te vinden, aangezien veel rekencentra dat al hebben gedaan en men op die ervaringen een beroep kan doen.

c. Voor de installatie en het onderhoud van netwerkprogrammatuur zijn twee systeemprogrammeurs nodig.

Bij deze schatting geldt een aantal aannames:
- Lokale projecten voor programmatuurontwikkeling zijn niet toegestaan, evenmin als interne projecten die niet expliciet worden gefinancierd door de gebruikersorganisaties.
- Lokale modificaties zijn eveneens *niet* toegestaan, met uitzondering van modificaties die als onderdeel van een programmapakket worden aangeleverd.
- Er wordt alleen gebruik gemaakt van standaardprogrammatuur of programmatuur ontwikkeld door applicatieprogrammeurs met duidelijke afspraken over de verantwoordelijkheid voor het oplossen van fouten in de programmatuur.
- Het beheer van de databases en het uitvoeren van reorganisatie-werkzaamheden voor deze databases wordt gezien als een verantwoordelijkheid van de gebruikersorganisaties.
- Er wordt geen ondersteuning gegeven voor decentrale systemen, aangezien die alle buiten het rekencentrum zijn opgesteld binnen de gebruikersorganisaties.

Om ook tijdens vakanties, ziekte en cursussen over voldoende deskundigheid te beschikken kan men overwegen het aantal systeemprogrammeurs met één te verhogen. Dat zijn dus zes personen voor deze afdeling.

3. Afdeling Operations

a. Voor het wekelijks starten van de systemen, de console-bewaking en de afhandeling van magneetbanden en papieruitvoer zijn drie shifts noodzakelijk, gezien de 24 uur/werkdag-dienstverlening. Indien men de consoles in de omgeving van de tape-units en printers plaatst kunnen deze operators multifunctioneel optreden, zodat met een bezetting van drie operators per shift kan worden volstaan. Hierbij gelden de volgende veronderstellingen:

- Veel papieruitvoer wordt decentraal geprint (het aantal bij de gebruikers opgestelde decentrale printers is aanzienlijk toegenomen gedurende de laatste jaren).

- Veel handelingen zijn geautomatiseerd via programmatuur voor *unattended operations*. Ook hierbij is het niet nodig zelf het wiel uit te vinden, aangezien de vereiste programmatuur en ervaringen op de vrije markt beschikbaar zijn.

- Er zijn correcte en goed hanteerbare operator-handboeken aanwezig.

- De gebruikers dragen zelf zorg voor het tijdig starten en afhandelen van hun produktiejobs, bijvoorbeeld via een pakket waarin men de starttijdstippen en de volgorde van de jobs kan opgeven.

Voor de drie shifts zijn minimaal negen personen nodig. Indien men rekening houdt met ziekte, vakanties, ADV en cursussen, is er sprake van een vermenigvuldigingsfactor van ongeveer 1,25. Men kan dus volstaan met elf personen.

b. Voor de overige activiteiten van Operations zijn vijf personen nodig:
- één voor het documenteren van de dagroutines voor de shifts en het bijhouden van de operator-handboeken;
- één voor het voorbereiden van alle periodieke produktieroutines en het gereedzetten van de jobs die door operators worden gestart;
- één voor het onderhoud van de schijfruimte en het beheer van het automatische migratie/backup-pakket voor datasets en bestanden;
- één voor problem en change management;
- één voor beveiliging.

Deze vijf personen dienen als groep samen te werken en kunnen tijdens vakanties, ziekte en cursussen grotendeels voor elkaar waarnemen. In een groep van vijf personen waarbij de meeste activiteiten niet tijd-kritisch zijn, is het functioneren als elkaars backup realistisch.

De schatting van zestien personen voor de afdeling Operations is mede gebaseerd op de veronderstelling dat alle informatiesystemen geheel compleet worden aangeleverd door of namens de gebruikersorganisaties, inclusief alle operationele procedures en besturingsopdrachten. Operations is betrokken bij de acceptatie en neemt daarna de systemen in produktie. Het past beslist niet bij de kernactiviteiten om Operations zelf de besturingsopdrachten te laten bouwen: dat is een verantwoordelijkheid van de organisatie namens welke de desbetreffende programmatuur wordt geëxecuteerd.

4. Management

In het verleden werd verondersteld dat voor iedere afdeling van ten hoogste tien medewerkers een manager nodig was en dat afdelingen functioneel gegroepeerd moesten worden onder hogere managers. Het blijkt echter bij recente reorganisaties binnen de automatisering dat managers prima in staat zijn leiding te geven aan grotere groepen en dat een platte organisatie met een minimaal aantal managementlagen ook goed functioneert. Vandaar dat voor deze organisatie slechts vier managers worden voorgesteld, namelijk:

a. de manager van het rekencentrum;
b. de manager van de afdeling Rekencentrum-administratie;
c. de manager van de afdeling Systeemprogrammering;
d. de manager van de afdeling Operations.

Voor de kernactiviteiten van dit rekencentrum zijn 35 personen nodig. Hierbij is al rekening gehouden met opvang van de werkzaamheden tijdens vakanties enz. Er wordt verondersteld dat bij een gelijktijdige afwezigheid van een groot aantal medewerkers in bepaalde perioden, zoals rond de Kerst en in de zomermaanden, eventuele voorziene problemen met de dienstverlening worden opgelost door het gebruik van enkele tijdelijke medewerkers. Bij gestructureerde processen en adequate documentatie kunnen deze snel worden ingewerkt.

Een belangrijke conclusie bij de waarnemingen is de zeer beperkte afhankelijkheid van het aantal mainframes. Voor de meeste medewerkers maakt het nauwelijks verschil of het centrum over twee of twaalf mainframes beschikt. De werklast van Systeemprogrammering wordt voornamelijk bepaald door het aantal te ondersteunen programmapakketten en de stabiliteit van deze programmatuur, terwijl de werklast van de administratieve medewerkers wordt bepaald door het aantal gebruikers. Alleen bij de afdeling Planning is er een enigszins lineair verband tussen de werklast en het aantal te installeren of te verplaatsen mainframes. Bij de afdeling Operations is de werklast voornamelijk afhankelijk van het aantal magneetbanden en de hoeveelheid papieruitvoer die per dag moet worden afgehandeld.
Deze conclusie is van belang voor een mogelijke verdere kostenreductie, aangezien deze de basis vormt voor besparingen via consolidatie en outsourcing. Door de geringe afhankelijkheid tussen werklast en het aantal mainframes kan men door schaalvergroting aanzienlijke besparingen realiseren. Dat wil zeggen centralisatie van werkzaamheden voor een aantal rekencentra.

TER AFSLUITING

In rekencentra wordt hard gewerkt en veel medewerkers zetten zich volledig in ter realisatie van hun doelstellingen, zelfs door avonden en weekends door te werken. Helaas vinden er, door een falend managementbeleid, activiteiten plaats die op geen enkele wijze bijdragen aan de zakelijke doelstellingen van de overkoepelende organisatie. Veel van deze activiteiten zijn op laag niveau geinitieerd of impliciet aanvaard, en hun kosten zijn vrijwel niet controleerbaar noch beheersbaar. Daarom wordt gepleit voor het omvormen van de bestaande rekencentra naar zelfstandige produktie-eenheden die zich volledig richten op de kernactiviteiten, namelijk het leveren van een betrouwbare infrastructuur voor de verwerking van informatie- en datacommunicatiesystemen. Alle ballast dient hierbij te worden geëlimineerd. Dit artikel levert een norm voor de menskracht welke men nodig heeft voor deze zeer sterk doelgericht opererende organisatie.

Hierbij wordt tevens gepleit voor het afstoten van alle activiteiten die op impliciet of expliciet verzoek van de gebruikersorganisaties worden uitgevoerd en zijn gerelateerd aan specifieke informatiesystemen. Doordat deze activiteiten in het verleden bij het rekencentrum zijn ondergebracht, verdwenen zij in de grote 'pot', verdween hun herkenbaarheid en werden hun kosten verdeeld over alle gebruikers. Hierdoor verdween tevens de prikkel tot het optimaliseren van de individuele processen en het reduceren van de kosten. Door deze specifieke activiteiten terug te plaatsen bij de hierom verzoekende organisatie, krijgt deze organisatie inzicht in de werkelijke kosten en heeft daarmee een hefboom om optimalisatie te forceren. Er wordt in dit artikel niet aangedrongen op collectief ontslag, maar op het onderbrengen van de juiste activiteiten bij de juiste instanties, die ieder zelfstandig kunnen streven naar optimalisatie en kostenreductie.

LITERATUUR

[Broo75] F.P. Brooks Jr., *The Mythical Man-month*, Addison-Wesley Publishers, Reading 1975.

[Glei89] J. Gleick, *Chaos, de Derde Wetenschappelijke Revolutie*, Contact, Amsterdam 1989 (de Engelstalige versie is: J. Gleick, *Chaos, Making a New Science*, Penguin Books, New York 1988).

[Moll91] K.IJ. Mollema, *Zichtbaarheid van Informatiekwaliteit*, Samsom, 1991.

[Paan91] R. Paans, *Verspillen of Investeren in Automatisering: de Managementproblematiek*, oratie Vrije Universiteit Amsterdam, 1991 (verkrijgbaar via Postdoctorale EDP Audit Opleiding, telefoon 020-5484629).

[Paan93] R. Paans en M.H.E. Gianotten, *Management van Computercentra: van Chaos naar Orde*, Giarte Management & Informatie, 1993 (dit boek kan worden besteld via Giarte M&I, Postbus 94828, 1090 GV Amsterdam, telefoon 020-6941334).

[Park60] C. Northcote Parkinson, *De Wet van Parkinson, Oefeningen in Beleid*, Scheltema & Holkema, Amsterdam 1960.

Prof.dr.ir. R. Paans RE
Is in 1986 gepromoveerd op performance- en beveiligingsaspecten van mainframes met het IBM MVS-besturingssysteem bij prof.dr. I.S. Herschberg. Sinds 1984 was hij werkzaam bij IBM, onder andere als Manager Corporate Programs van het Europese hoofdkantoor. In dit kader was hij betrokken bij standaardisatie van de dienstverlening en kostenreducties in de operationele omgeving.
Sinds 1 januari 1994 is hij vennoot van KPMG Klynveld EDP Auditors te Amsterdam. Daarnaast is hij hoogleraar bij de Postdoctorale EDP Audit Opleiding van de Vrije Universiteit te Amsterdam en Europees redacteur van het tijdschrift Computers & Security.

Accountant en de kosten- en baten-beheersing van informatietechnologie

Prof. H.B. Moonen RE RA

Mede ingegeven door de vele IT-projecten die veel duurder bleken dan begroot en door de alsmaar stijgende uitgaven aan automatisering, staat het beheersen van de kosten van informatietechnologie steeds hoger op de prioriteitenlijst van managers. Doordat accountants zich de laatste jaren steeds meer zijn gaan profileren in hun adviesfunctie gekoppeld aan de controle van de jaarrekening, worden zij in toenemende mate geconfronteerd met deze problematiek.

INLEIDING

In het kader van zijn traditionele adviesfunctie wordt de controlerend accountant meer en meer geconfronteerd met vragen over de kwaliteitsaspecten van de automatisering. Met name managers uit het midden- en kleinbedrijf schakelen de accountant in bij het besluitvormingsproces voor nieuwe investeringen in informatietechnologie.

Daarnaast wordt de accountant geacht zinvol te kunnen reageren op vragen als:
- geven we niet te veel geld uit aan automatisering;
- investeren we wel in de goede systemen;
- is decentralisatie niet veel goedkoper;
- moeten we nog meer gaan automatiseren.

Hiervoor dient hij op de hoogte te zijn van de problematiek van het beheersen van de kosten en de baten van informatietechnologie.

In dit artikel wordt eerst ingegaan op de algemene problematiek bij het beheersen van de kosten en de baten van informatietechnologie. Hierbij wordt aandacht geschonken aan de voor de accountant herkenbare oorzaken van problemen die afbreuk doen aan een adequate beheersing. Vervolgens wordt zowel voor de kosten als voor de baten van informatietechnologie aangegeven welk inzicht minimaal vereist is voor een accountant om de problemen met betrekking tot de kosten- en batenbeheersing bij informatietechnologie op een verantwoorde wijze te kunnen beoordelen. Ten slotte wordt, voor de accountant in het kader van zijn adviesfunctie, een drietal methoden beschreven waarmee de beheersing van kosten en baten van informatietechnologie in organisaties kan worden beoordeeld.

PROBLEMEN BIJ HET 'BEHEERSEN' VAN DE KOSTEN VAN INFORMATIETECHNOLOGIE

Een aantal jaren geleden stond het beheersen van de kosten van informatietechnologie niet hoog op de prioriteitenlijst van de meeste managers van middelgrote tot grote ondernemingen. De geldkraan stond als het ware open en als projecten dreigden te mislukken werd deze kraan simpelweg wat verder open gedraaid. De laatste jaren is een kentering opgetreden. De tendens is nu om de kosten van automatisering veel kritischer te bekijken. Mede ingegeven door de vele IT-projecten die veel duurder bleken dan begroot en door de vaak alsmaar stijgende uitgaven aan automatisering staat het beheersen van de kosten van informatietechnologie steeds hoger op de prioriteitenlijst van de managers. Voor de accountant is het van belang op de hoogte te zijn van de mogelijkheden op het gebied van het beheersen van kosten van informatietechnologie. In ieder geval dient hij de problemen te herkennen en oorzaken aan te geven.
Op een aantal van deze problemen wordt hierna ingegaan.

IT-budget

Vaak ontbreekt in organisaties een voldoende gedetailleerd IT-budget. De uitgaven aan informatietechnologie worden niet afgezet tegen een van tevoren door het management geaccordeerde taakstelling, waardoor de basis voor een adequate kostenbeheersing ontbreekt.

Procesbeheersing

In het algemeen worden de processen rondom informatietechnologie in de praktijk nog onvoldoende beheerst. Afgezien van een dikwijls gebrekkige of zelfs niet bestaande feitelijke registratie van de bestedingen in uren en geld, geeft men zich vaak onvoldoende rekenschap van de risico's, zoals:
- het effect van nieuwe ontwikkelingstechnieken;
- het toepassen van 'non proven' software;
- weerstanden bij de gebruiker;
- uitloop bij testen.

Met name tijdens de systeemontwikkeling/implementatie ontbreekt het aan inzicht in kosten, doordat de risico's die worden gelopen onvoldoende in kaart zijn gebracht. Dit heeft overigens niet alleen gevolgen voor de beheersing van de kosten van informatietechnologie maar ook voor de kwaliteit van de informatietechnologie (bijvoorbeeld de betrouwbaarheid van het informatiesysteem).

Nieuwe ontwikkelingen

Veelal ontbreekt het aan continue aandacht van het management voor nieuwe ontwikkelingen en mogelijkheden op het gebied van de structurele aanpak van informatietechnologie. Hierbij kan worden gedacht aan zaken als make or buy, uitbesteding of inhouse, decentralisatie of centralisatie. Het management van veel organisaties is van deze ontwikkelingen niet of onvoldoende op de hoogte en mist daardoor inzicht in alternatieve mogelijkheden voor een betere beheersing van de kosten en de baten.

Informatievoorziening aan het management

Het management is vaak niet goed geïnformeerd omtrent de voortgang van automatiseringsprojecten en heeft onvoldoende kennis van typisch IT-gerichte middelen om de kosten te verminderen en/of de efficiency te verhogen. Voorbeelden zijn: CASE-tools, vierde-generatietalen, reengineering, objectgeoriënteerd programmeren.

IT-investeringen

Investeringen in informatietechnologie worden nogal eens economisch slecht onderbouwd en vrijwel volledig vanuit een te technische invalshoek opgesteld. Alternatieve mogelijkheden voor het verkrijgen van een IT-produkt worden niet of onvoldoende toegelicht. Zo worden door softwareontwikkelingsafdelingen van ondernemingen projecten gelanceerd zonder daarbij grondig te kijken naar de noodzaak van de projecten of te onderzoeken of het aanschaffen van een standaardpakket wellicht voordeliger is.

BEHEERSING VAN DE IT-KOSTEN

Voor de beheersing van IT-kosten is het noodzakelijk dat een meetinstrumentarium wordt ontwikkeld.

Inzicht in de kosten van informatietechnologie

Problemen op het gebied van de beheersing van IT-kosten zullen of zouden zich normaliter moeten manifesteren in door de organisatie geregistreerde IT-kosten. Wil de accountant de ontwikkelingen op het gebied van kosten van automatisering bij een cliënt kunnen volgen, dan zal hij minimaal inzicht moeten hebben in deze kosten. Daarvoor is het noodzakelijk dat in de onderneming een adequate registratie plaatsvindt van investeringen in hardware en software en van de jaarlijks toe te rekenen kosten uit deze investeringen. Voor wat betreft de ontwikkeling van applicatiesystemen dient een projectadministratie aanwezig te zijn, waarbij niet moet worden vergeten ook de uren van de betrokken gebruikers te registreren.

Budgettering van IT-kosten

De vorengenoemde registratie van de werkelijke kosten is de aanzet tot het kennen van wat reeds besteed werd. Veel beter is het uiteraard om de kosten te prognosticeren in afdelingsbudgetten of

projectbudgetten. Dit maakt het mogelijk in de loop van het jaar of in de loop van de projectontwikkeling de kosten te analyseren en bijvoorbeeld aan het einde van een project een projectevaluatie te maken ondersteund door een financiële analyse. Als bij wijze van voorbeeld een afdelingsbudget wordt genomen, dan dienen daarin minimaal de volgende kosten te worden geïdentificeerd:

- een splitsing van de kosten per IT-activiteit (systeemontwikkeling, onderhoud en produktie);
- een splitsing per kostensoort (personeel, technologie en overige);
- een splitsing van de projectkosten in inzet van gebruikers/derden/automatiseerders en hardware/software.

In de literatuur zijn goed uitgewerkte budgetmethoden voorhanden, zodat hier volstaan wordt met een korte aanduiding.

Zijn de kosten van informatietechnologie vaak nog wel boven water te tillen, de baten daarentegen zijn vaak niet te definiëren, laat staan te achterhalen.

IT-kostenratio's

Indien men beschikt over een registratie die inzicht in de IT-kosten verschaft, is het goed mogelijk aan de hand van ratio's een beeld te krijgen van de mate van ontwikkelingen van de kosten in de tijd. Tevens is het mogelijk vergelijkingen te maken met de IT-kostenontwikkeling in andere ondernemingen. Er bestaan uitgebreide in databases vastgelegde ervaringsratio's per branche, die als maatstaf kunnen dienen om de positie van een onderneming in relatie tot de branchegenoten te beoordelen.

Voorbeelden van normen zijn:

- IT-kosten per medewerker;
- IT-kosten als percentage van de omzet;
- systeemontwikkelingskosten als percentage van de IT-kosten;
- systeemonderhoudskosten als percentage van de IT-kosten;
- verwerkingskosten als percentage van de IT-kosten.

De waarde van dit soort ratio's zal sterk toenemen als de ratio's over een langere periode bijgehouden zijn. Sterke fluctuaties in de waarden van de ratio's zijn een signaal om een nadere analyse uit te voeren.

PROBLEMEN BIJ HET 'BEHEERSEN' VAN DE BATEN VAN INFORMATIETECHNOLOGIE

Naast het kostenvraagstuk zal voor de informatietechnologie ook de rendementsvraag aan de orde moeten komen. Het identificeren en traceren van de baten is vaak een groter probleem dan het beheersen van de kosten van informatietechnologie. Kunnen de meeste managers kostenbeheersing van informatietechnologie nog wel plaatsen in hun gedachtenwereld (zeker gezien de trend van algehele kostenbeheersing binnen het bedrijfsleven), het beheersen van de baten van informatietechnologie is veel minder vanzelfsprekend en vaak een onbekend fenomeen. Zijn de kosten van informatietechnologie vaak nog wel boven water te tillen (zij het soms met enige moeite), de baten daarentegen zijn vaak niet te definiëren, laat staan te achterhalen.

Identificatie van de baten

Als belangrijkste oorzaak dat de batenbeheersing van informatietechnologie niet of nauwelijks van de grond komt, kan worden genoemd het moeilijk kunnen identificeren en toerekenen van de IT-baten en vervolgens het vertalen van de baten in financiële cijfers.
Het identificeren van de baten van informatietechnologie is afhankelijk van de soort IT-toepassing. Een IT-toepassing die een administratief proces ondersteunt zal bijvoorbeeld andere baten genereren dan een IT-toepassing die een produktieproces ondersteunt.
Nadat de baten zijn geïdentificeerd kunnen deze op een drietal niveaus in de organisatie worden onderkend, namelijk:

- de baten voor de organisatie als geheel;
- de baten voor de afdeling/processen;
- de baten voor het individu (de gebruikers).

De IT-baten zullen bij voorkeur zichtbaar moeten worden gemaakt via kengetallen, ratio's, etc. in het kader van performance-management. Met name zal daarbij aandacht moeten worden gegeven aan ratio's die zich richten op ondersteuning van:

- geformuleerde bedrijfsdoelstellingen;
- kritische bedrijfsprocessen;
- beheersprocessen.

Procesfactoren

Problemen bij het beheersen van de informatietechnologie worden veroorzaakt door de ongunstige effecten van een aantal proces- en omgevingsfactoren.
Zo leidt een instabiele omgeving (hetzij binnen de organisatie, hetzij buiten de organisatie) ertoe dat de eisen/wensen van de gebruikers kunnen veranderen waardoor een systeemontwikkelingsproject niet de vooraf begrote resultaten oplevert.

INZICHT IN DE BATEN VAN INFORMATIETECHNOLOGIE

In een IT-investeringsaanvraag zullen de baten zo gedetailleerd mogelijk kwalitatief moeten worden bepaald. Tevens dient hierbij rekening te worden gehouden met de meetbaarheid van deze 'normen' achteraf (nacalculatorisch). Er zal een uiterste inspanning moeten worden geleverd om op het oog niet-meetbare of niet-kwantificeerbare baten op deze wijze te vertalen in beheersbare baten.
Bij het beheersen van de kosten van informatietechnologie werd de noodzaak van het hanteren van ratio's al onderkend. Ook meetbare baten moeten zoveel mogelijk worden vertaald naar ratio's. Voorbeelden hiervan zijn besparingen in:
- de kosten per orderregel;
- de arbeidskosten per eenheid produkt;
- de voorraadkosten als percentage van de omzet.

Overigens hoeven het niet altijd financiële ratio's te zijn. Het is ook mogelijk ratio's te definiëren die een indicatie geven van het beheersen van de baten zonder dat er een direct verband is met financiële middelen.

METHODEN VAN ONDERZOEK VAN DE ACCOUNTANT

Zoals hiervoor aangegeven is, zijn de problemen rond de kosten- en batenbeheersing bij informatietechnologie groot en is tijdige signalering van deze problemen niet eenvoudig. Om als accountant zicht te krijgen op de wijze waarop de kosten en baten van informatietechnologie worden beheerst, zijn daarom extra inspanningen noodzakelijk. Hiervoor is een aantal methoden ontwikkeld.

Audit van een IT-investeringsaanvraag

Doordat veel organisaties in de praktijk problemen ondervinden met het beoordelen van IT-investeringen wordt de beoordeling vaak slechts summier uitgevoerd of compleet achterwege gelaten. In sommige gevallen wordt de accountant gevraagd een IT-investeringsaanvraag te auditen.
De IT-investeringsaudit richt zich onder meer op:
- de volledigheid van de IT-investeringsaanvraag;
- de kosten en baten die in de investeringsaanvraag zijn onderkend;
- de maatregelen die zijn voorzien om risico's (bijvoorbeeld budget- of tijdsoverschrijding) te verkleinen.

De audit zelf is in twee delen gesplitst. Het eerste deel van de audit bestaat uit een formele beoordeling van de investeringsaanvraag (voldoet de aanvraag aan richtlijnen van de organisatie, is de aanvraag volledig genoeg voor de inhoudelijke beoordeling). Het tweede gedeelte is de inhoudelijke beoordeling, waarbij de investeringsaanvraag wordt geanalyseerd en beoordeeld.

In de zomereditie van Compact van 1993 [Bigg93] is het artikel 'De audit van een IT-investeringsaanvraag' opgenomen, waarin de methode uitvoerig is beschreven en uitgewerkt aan de hand van een tweetal casussen.

Door bij de audit te starten met de formele beoordeling kan worden voorkomen dat investeringsaanvragen aan een relatief arbeidsintensieve inhoudelijke beoordeling worden onderworpen. Indien namelijk bij de formele beoordeling wezenlijke tekortkomingen worden gesignaleerd, zal de accountant de audit onderbreken om deze tekortkomingen te bespreken en te laten corrigeren.
Een audit van een IT-investeringsvoorstel heeft een gunstig effect op het beheersen van de kosten en de baten van informatietechnologie. Immers, potentiële IT-investeringen met onbeheersbare kosten worden tijdig gesignaleerd en hetzelfde geldt voor IT-investeringen met onbeheersbare baten.

Doordat veel organisaties in de praktijk problemen ondervinden met het beoordelen van IT-investeringen wordt de beoordeling vaak slechts summier uitgevoerd of compleet achterwege gelaten.

IT-projectaudit

In de praktijk blijkt dat door onvoldoende beheersing van de IT-projecten de organisatie geconfronteerd wordt met tegenvallende resultaten, zoals:
- overschrijding van de doorlooptijd/kosten;
- moeizaam invoeringstraject;
- onvoldoende functionaliteit;
- onvoldoende aanpassing organisatie;
- onvoldoende betrouwbare werking;
- onverwacht nadelige consequenties voor personeel en organisatie.

Overigens zijn er wel signalen die een onvoldoende beheersing van een IT-project aangeven. Signalen zijn bijvoorbeeld een overschrijding van de planning/begroting per fase, weerstand of onvoldoende betrokkenheid van de gebruikers, slechte voortgangsrapportages of een hoog ziekteverzuim/slechte sfeer binnen de projectgroep.

Een projectaudit maakt gebruik van dit soort signalen en richt zich primair op de diverse risico's die verbonden zijn aan het project. Daartoe kan een zestal risicocategorieën worden onderscheiden:
- *Tijd.* Worden deelsystemen op tijd opgeleverd?
- *Geld.* Vindt ontwikkeling plaats tegen begrote

Prof. H.B. Moonen RE RA Is vennoot bij KPMG Klynveld EDP Auditors en hoogleraar EDP-auditing aan de Katholieke Universiteit Brabant, tevens lid van het bestuur van de EDP Auditors Association Chapter Benelux. Sinds 1965 is hij betrokken bij het auditen en adviseren op het gebied van de kwaliteit van de automatisering. Vanaf 1963 tot 1983 was hij werkzaam bij de Interne Accountantsdienst van N.V. Philips, waarvan de laatste vijf jaar als verantwoordelijke partner voor EDP-audit.

en aanvaardbare kosten met juiste afweging tussen kosten en baten?
- *Kwaliteit.* Voldoet het systeem aan de eisen van de gebruikers/ondernemingsstandaarden?
- *Organisatie/acceptatie.* Wordt het systeem door de organisatie geaccepteerd?
- *Techniek.* Is het systeem technisch aanvaardbaar?
- *Informatie/documentatie.* Wordt het systeem adequaat gedocumenteerd (onderhoudbaarheid)?

Vervolgens is een aantal indicatoren te onderkennen die deze risicocategorieën beïnvloeden. Eén daarvan is de projectomvang. Als het een groot project betreft (lange doorlooptijd, veel partijen en dergelijke) worden met name risico's gelopen op het gebied van tijd en geld (niet op tijd binnen budget afronden), kwaliteit (niet conform eisen/wensen, die tussentijds veranderen), organisatie (geen acceptatie als gevolg van doorlooptijd project, gebruikers voelen zich niet meer betrokken) en informatie (documentatie up-to-date houden voor een dergelijk omvangrijk project). Een andere indicator is de projectbemanning. Indien de projectbemanning niet voldoet (te veel externe medewerkers, veel parttimers, onvoldoende kennis en ervaring, etc.) worden met name risico's gelopen op het gebied van tijd en geld, kwaliteit en informatie (documentatie onvoldoende). Door op deze wijze via een projectaudit de relevante risico-indicatoren in kaart te brengen, worden de risico's die verbonden zijn aan een project duidelijk geïdentificeerd en kan men tijdig het project bijsturen respectievelijk beëindigen.

Audit van de effectiviteit en efficiëntie van informatietechnologie (quick scan)

De doelstelling van een onderzoek naar de effectiviteit en efficiëntie van informatietechnologie, uitgevoerd volgens de quick scan-methode, is primair het verkrijgen van inzicht in de mate van effectiviteit en efficiëntie van de geautomatiseerde gegevensverwerking en daarnaast het op het spoor komen van tekortkomingen bij de kostenbeheersing van IT-activiteiten.
De auditobjecten hierbij zijn de informatiesystemen, de gebruikers, de automatiseringsafdeling en de procedures en richtlijnen.

Informatiesystemen. Hierbij wordt voornamelijk gekeken naar de ondersteuning van de organisatie door informatiesystemen en naar de kwaliteit van die systemen.

Gebruikers. Beoordeeld worden de betrokkenheid van de gebruikers bij het automatiseringsproces en de kennis en vaardigheden van de gebruikers om informatietechnologie toe te passen.

Procedures en richtlijnen. De audit richt zich op de kwaliteit van de procedures in de organisatie en de richtlijnen van het management.

Automatiseringsafdeling. Tijdens de audit komen vragen aan de orde als: hoe ziet de IT-organisatie eruit, welke middelen heeft zij tot haar beschikking en hoe gaat zij daarmee om? Wat is de kennis en wat zijn de vaardigheden van de medewerkers van automatisering?

Het eindresultaat van de audit is een rapportage waarbij indicaties worden gegeven of:
- de informatiesystemen de behoeften van de gebruikers goed ondersteunen;
- er nog leemten zijn in de automatisering van bepaalde processen/functies;
- de automatiseringsafdeling efficiënt met haar middelen omgaat;
- de gebruikers voldoende betrokken zijn bij de automatisering;
- de informatiesystemen technisch voldoen.

TOT SLOT

Doordat accountants zich de laatste jaren steeds meer zijn gaan profileren in hun adviesfunctie gekoppeld aan de controle van de jaarrekening, worden zij in toenemende mate geconfronteerd met de problematiek van de kosten- en de batenbeheersing bij informatietechnologie.
Het management beschikt vaak niet over voldoende IT-kennis en -ervaring en mist vaak de expertise voor een adequate beheersing van IT-kosten en -baten.
De accountant in zijn signalerende functie kan het management wijzen op de problematiek en eventueel samen met EDP-auditors de gesignaleerde problemen analyseren.

LITERATUUR

[Bigg93] S.R.M. van den Biggelaar en P.P.M.G.G. Brouwers, *De audit van een IT-investeringsaanvraag*, Compact 1993/2.

Informatiebeveiliging: de tijd is rijp

Drs. H.G.Th. van Gils RE RA

Informatiebeveiliging móet, daarover bestaat tegenwoordig geen verschil van mening, maar hoe? Omvangrijke, kwantitatieve risico-analyses hebben in het verleden ondanks hoge kosten vaak niet de gewenste resultaten opgeleverd.
In dit artikel wordt beschreven hoe in plaats van met een alomvattende risico-analyse met behulp van deelanalyses achtereenvolgens tactische normen en een concreet beveiligingsplan kunnen worden opgesteld. Hierbij wordt ook kort stilgestaan bij de voor- en nadelen van een alternatieve benadering, gebaseerd op baseline controls.

INLEIDING

Zo langzamerhand breken voor de makers van beveiligingsbeleidsdocumenten betere tijden aan. Na jaren van theoretische studiebijeenkomsten, werkgroepen, motiverende brieven aan (en namens) het management, vereenvoudigde risico-analyses, benoemingen tot security officers, regelgeving als de Wet persoonsregistraties en uiteindelijk de Wet computercriminaliteit, lijkt bijna iedereen zo langzamerhand te beseffen dat informatiebeveiliging niet alleen geld kost, maar dat bepaalde (ongewenste) gebeurtenissen de organisatie op nog veel hogere kosten (direct of indirect) kunnen brengen. Daarnaast blijken de inmiddels getroffen maatregelen al een behoorlijke kostenpost te zijn, zonder dat steeds duidelijk is welke bedreigingen nu precies zijn afgedekt.

Veel organisaties hebben altijd al bepaalde beveiligingsmaatregelen getroffen. In een aantal gevallen is dat gebeurd nadat organisaties werden geconfronteerd met situaties die de informatievoorziening negatief beïnvloedden. Voorbeelden daarvan zijn een brandje in de computerzaal of een schijf die defect raakt (gegevensverlies), een niet-getest programma dat naar de produktie-omgeving wordt overgezet of de aanschaf van een pakket dat bepaalde functiescheiding in de organisatie niet ondersteunt (fraude of onjuiste informatie). Ook zijn er duidelijke externe impulsen te onderkennen zoals regelgeving (voor banken) door De Nederlandsche Bank, de eerder genoemde Wet computercriminaliteit en artikelen over hacking en virussen.

De belangrijkste nieuwe impulsen worden gegeven door ontwikkelingen in netwerken, open systemen en interne en externe elektronische datacommunicatie. Overigens speelt daarbij ook de 'marketing' een bepaalde rol. Net zoals veel bedrijven zich sterk maken voor het verkrijgen van een ISO 9000-kwaliteitscertificaat, vinden steeds meer managers dat een informatiebeveiligingsbeleid er gewoon hoort te zijn. Niet alleen de accountant of EDP-auditor vraagt ernaar, maar steeds vaker ook de handelspartners indien datacommunicatie/EDI om de hoek komt kijken.

In dit artikel wordt ingegaan op het concretiseren van (strategisch) informatiebeveiligingsbeleid. Daartoe worden normen (voor het tactisch niveau) uit het beleid afgeleid, op grond waarvan voor de organisatie een afgebakend geheel van beveiligingsmaatregelen kan worden voorgesteld. Ten slotte wordt in dit artikel de functionele beveiligingsorganisatie belicht, ter ondersteuning van de handhaving van de getroffen maatregelen.

INFORMATIEBEVEILIGING

Wat informatiebeveiliging betreft is er in de loop der jaren een golfbeweging te zien geweest.
In de beginfase waren geautomatiseerde informatiesystemen niet betrouwbaar en werd smalend gesproken in termen als 'het komt uit de computer, dus het moet wel goed zijn (maar niet heus)'. Vooral werden maatregelen getroffen in de sfeer van continuïteit (beschikbaarheid van kopie-bestanden en invoerlijsten) en goede controles op de uitvoer (gebruikercontroles). Na verloop van tijd is de techniek behoorlijk stabiel geworden en zijn in applicaties veel geprogrammeerde controles opgenomen, waardoor 'gewone' fouten steeds zeldzamer zijn geworden. Onlangs gaf een directeur aan dat alleen zijn externe accountant nog af en toe computerlijsten liet doortellen. Zijn eigen personeel wist wel beter ... 'een computer kan goed tellen, daar is hij voor gemaakt, dus als het uit de computer komt ...'.
Deze houding is algemeen gangbaar geworden. Echter, deze is alleen te rechtvaardigen als op de een of andere manier is verzekerd dat de geautomatiseerde gegevensverwerking 'beheerst' plaatsvindt.

Inmiddels blijkt dat door de voortschrijdende technologie een organisatie steeds weer wordt geconfronteerd met veranderende ontwikkeltools, IT-platformen, netwerkstructuren en toenemende functionaliteit van besturingsprogrammatuur. Dat heeft tot gevolg dat vaak op verschillende manieren beveiligingsmaatregelen worden gezocht en getroffen. Na verloop van tijd resulteert dat in ondoorzichtigheid in het in totaliteit getroffen stelsel van beveiligingsmaatregelen en waarschijnlijk in inefficiency ten aanzien van het beheersen van de kosten alsmede onduidelijkheid over de effectiviteit van de getroffen maatregelen.
Dan blijkt geleidelijk dat een meer beleidsmatige aanpak is vereist!

Een goede beveiliging van de informatievoorziening vergt behoorlijke investeringen, waarvan de opbrengsten niet of nauwelijks kunnen worden gemeten.

Een goede beveiliging van de informatievoorziening vergt behoorlijke investeringen, waarvan de opbrengsten niet of nauwelijks kunnen worden gemeten.
Per organisatie zal de inspanning natuurlijk sterk wisselen. Uit verschillende onderzoeken zijn enkele vuistregels te destilleren, die natuurlijk zeer globaal zijn en per branche sterk kunnen verschillen. Met inachtneming van deze beperkingen is een vuistregel dat adequate beveiliging in het algemeen circa één procent van de omzet vergt. Dit betreft dus niet alleen de informatiebeveiliging, maar ook algemene toegangsbeveiliging, inbraakbeveiliging, brandbeveiliging, etc. Wel bleek bij een enquête 85 procent van de ondervraagden de automatisering als één van de meest kritische factoren van beveiliging aan te wijzen. Een andere vuistregel stelt dat IT-beveiliging circa vijf procent van het IT-budget inneemt. Daarbij blijkt dat in de laatste jaren dit percentage toeneemt, met andere woorden de investeringen in IT-beveiliging leggen een grotere druk op het IT-budget.

De hogere investeringen hebben natuurlijk als resultaat dat er keuzes gemaakt moeten worden inzake hoe te beveiligen en met welke diepgang. Vandaar dat door het management uitspraken gedaan moeten worden tegen welke bedreigingen de organisatie zich zal moeten beveiligen en welke middelen daarvoor beschikbaar zijn.

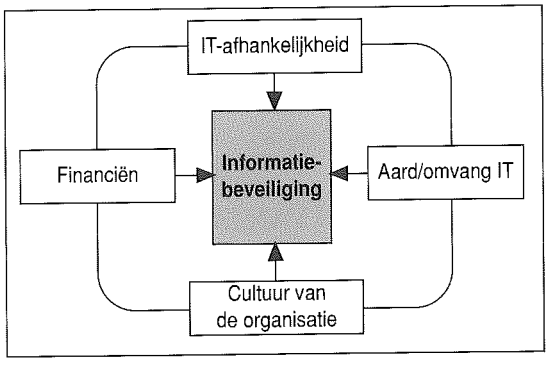
Overigens geldt ook voor dit onderwerp dat een organisatie er naar toe moet groeien. Het is niet realistisch te verwachten dat een organisatie in staat is vanuit een min of meer onbewuste fase, waarin nauwelijks inzicht is in de bedreigingen en beveiligingsmaatregelen, over te gaan tot de fase waarin men zich van de beveiligingsaspecten goed bewust is en een afgewogen beleid invoert. Vaak zal (helaas) eerst een ongewenste gebeurtenis moeten plaatsvinden, waarna men zich op de techniek stort om dergelijke calamiteiten voortaan het hoofd te bieden. Pas in de volgende jaren vindt het bewustwordingsproces plaats, waarin ruimte is voor analyse en beleidsbepaling en waarin een balans gezocht wordt tussen het gewenste beveiligingsniveau en de daarbij horende inspanningen als investeringen, gebruikersmotivatie en -opleiding.

Door de sterkere mate van concentratie van gegevens in bijvoorbeeld geïntegreerde logistiek-financiële systemen is het risico van omvangrijk gegevensverlies toegenomen. Anderzijds zijn door de toename van (gekoppelde) lokale netwerken de gegevensverwerking en -opslag op PC's erg dicht bij de gebruikers gekomen, waardoor de kans op gegevensverlies of misbruik is toegenomen. De gebruikers zelf zijn nog meer dan voorheen medebepalend voor de beveiliging van de opgeslagen gegevens. Een goed bewustzijn van de risico's is derhalve erg belangrijk geworden.
Ook daarom is de behoefte toegenomen om van boven af richtlijnen te geven hoe met de beveiliging van gegevens moet worden omgegaan.

Samenvattend is er een aantal factoren die een duidelijke invloed hebben op de aard en omvang van de beveiliging van de informatievoorziening (zie figuur 1).

INFORMATIEBEVEILIGINGSBELEID: STRATEGISCHE UITGANGSPUNTEN

Informatiebeveiligingsbeleid is niets anders dan een verzameling van strategische uitgangspunten waarin het management van een organisatie dui-

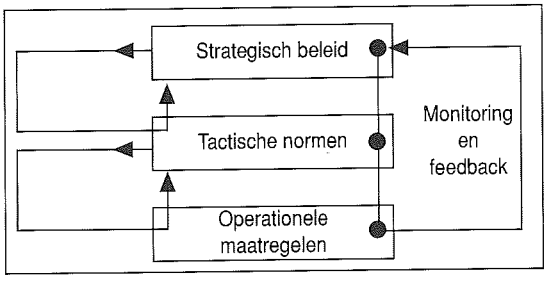


Figuur 1. Factoren van invloed op informatiebeveiliging.

delijk maakt aan het tactisch en operationeel niveau welke gedragslijn de organisatie dient te volgen om te komen tot een adequate informatiebeveiliging. Het beleid vormt daarmee de basis voor het verder uitwerken in normen en (plannen voor) maatregelen.

Uit een recent onderzoek inzake de effectiviteit van kwaliteitskeuring volgens de ISO 9000-standaarden [KPMG93-2] is gebleken, dat het verkrijgen van het certificaat weinig toevoegt aan de werkelijk geleverde kwaliteit, indien niet alle medewerkers van de organisatie zich bewust zijn van de vereiste inspanning. Het door een staforgaan of externe adviseurs laten ontwikkelen van een kwaliteitshandboek mag dan commerciële waarde hebben, zonder de inzet van de medewerkers in de organisatie leidt het niet tot de beoogde kwaliteit! Dit geldt natuurlijk onverminderd voor het opstellen van een beveiligingsbeleidsdocument. Het maken en vaststellen van beveiligingsbeleid is nog geen garantie voor de goede werking. Hiervoor is het nodig dat de uitgangspunten in een informatiebeveiligingsbeleid concreet worden geformuleerd. Door middel van controles op de uitvoering dient het management vast te stellen of de maatregelen werken (monitoring en feedback, zie figuur 2).
Evaluatie van het beleid dient vervolgens plaats te vinden om na te gaan of het beleid nog steeds aansluit op de organisatie en of de juiste maatregelen zijn getroffen.

Figuur 2. Controle op uitvoering.



BEVEILIGINGSNORMEN: UITWERKING OP TACTISCH NIVEAU

Een nadere uitwerking van het beveiligingsbeleid wordt gevormd door normen die op tactisch niveau gesteld worden aan de primaire aandachtsgebieden of processen van de organisatie. Aan de hand van deze normen kunnen beveiligingsmaatregelen worden getroffen, die er samen voor zorgen dat voldaan wordt aan de uitgangspunten van het beveiligingsbeleid.

Overigens hebben de beveiligingsnormen op tactisch niveau vaak uitsluitend betrekking op de normen die gesteld worden aan de informatiebeveiliging. Natuurlijk zijn er binnen een organisatie ook andere risico's te beheersen, in de zin van kwaliteitsvermindering, niet halen van planningen, performanceverlies, onvoldoende personeelsbezetting (zowel kwantitatief als kwalitatief), etc. Deze elementen van risicobeheersing zijn vaak niet in een beveiligingshandboek voor het tactisch niveau uitgewerkt.

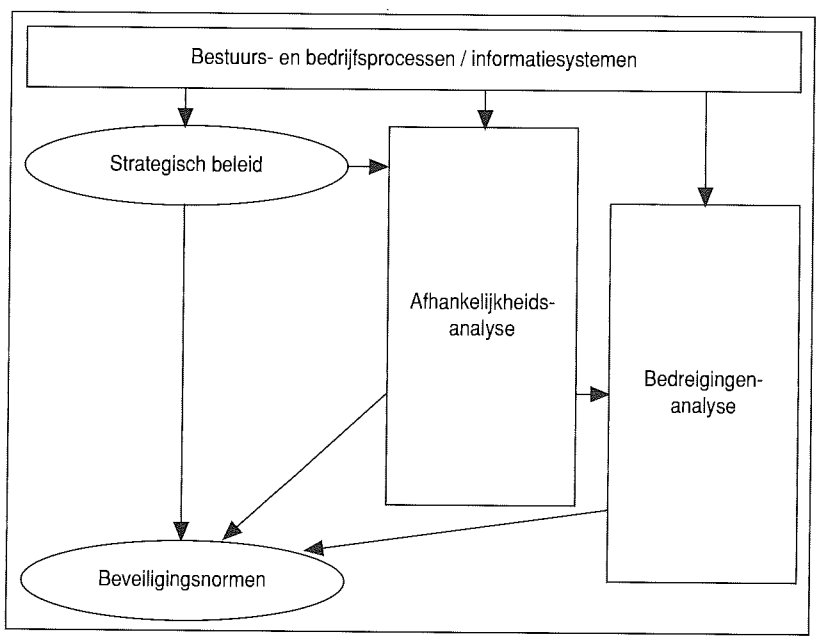
De kloof tussen min of meer abstract beleid en concrete maatregelen is groot. Maatregelen zijn meestal opgenomen in procedurebeschrijvingen en worden derhalve regelmatig gewijzigd. Ook de organisatie verandert regelmatig, waardoor de procedures weer veranderen, echter zonder dat het beleid zich wijzigt. Daarom is een meer stabiele beleidsvertaling gewenst, die vorm heeft gekregen in een opsomming van tactische normen (eisen).
Naast de onderhoudbaarheid speelt hierbij de acceptatie een belangrijke rol. Zoals eerder aangegeven is beveiligingsbeleid vaak abstract, terwijl de uitwerking daarvan in maatregelen vaak als onvriendelijk en soms als onbegrijpelijk overkomt. De overgang is gewoon te groot, waarbij het maar al te vaak voorkomt dat de maatregelen door mensen worden opgesteld die niet direct bij de processen in de organisatie betrokken zijn. Dat draagt niet bij tot een makkelijke acceptatie en bewustwording.

Door eerst concretere normen te definiëren kan afstemming in de organisatie plaatsvinden inzake de redelijkheid van de normen, uitgaande van het abstractere beveiligingsbeleid. In de praktijk blijkt het eenvoudiger te zijn consensus te krijgen over een normenstelsel dan over een stelsel van maatregelen. Een voorstel dat tot op maatregelniveau is uitgewerkt, wordt als bedreigend ervaren. Een voorstel echter waarin normen staan opgenomen, nodigt uit tot meedenken hoe op de meest efficiënte wijze aan die normen kan worden voldaan. Door dat denkproces begrijpt men beter waartoe bepaalde maatregelen bijdragen en is men derhalve beter gemotiveerd om die maatregelen adequaat toe te passen.
Die zelfde motivatie is vereist om tijdig te signaleren dat door verandering van processen bepaalde maatregelen inefficiënt of ineffectief worden dan wel zelfs ontbreken. Dan is begrip voor de achtergrond nodig om te kunnen handelen in de geest van het beveiligingsbeleid en de daarvan afgeleide beveiligingsnormen.

Het afzonderlijk vastleggen van de normen kan ook een goede voorlichtingsfunctie hebben, bijvoorbeeld voor derden die van de kwaliteit van de organisatie afhankelijk zijn. Steeds meer organisaties gebruiken kwaliteit als marketinginstrument, zoals bij het ISO-9000-certificaat. Het toenemend belang van informatiebeveiliging blijkt uit het verschijnen van advertenties waarin automatiseringsorganisaties wijzen op de goede kwaliteit van de beveiligingsorganisatie. Beveiliging wordt steeds belangrijker in verband met de netwerkkoppelingen en datacommunicatieverbindingen tussen de organisaties. Het is wel aardig om via EDI-afspraken een just-in-time delivery system aan te houden, maar dan moet je er wel van kunnen uitgaan dat de handelspartner over een goed beveiligde automatiseringsinfrastructuur beschikt. Met name de aspecten betrouwbaarheid en continuïteit zijn dan van groot belang. Dan is het aantoonbaar hebben van kwaliteit volgens een goed normenstelsel geen overbodige luxe.

Ook andere mensen kunnen belang hebben bij de kwaliteit van de beveiliging van de informatievoorziening van een organisatie. In dat kader kan bijvoorbeeld de accountant worden genoemd, die een controle-aanpak hanteert die verschilt naarmate de kwaliteit van de informatievoorziening verschilt. Steeds meer verschuift de gewenste aanpak naar het steunen op maatregelen die de organisatie zelf al heeft getroffen, waardoor de accountant minder cijfermatig te werk hoeft te gaan en meer de werking van de organisatie kan toetsen aan 'redelijkerwijs te stellen eisen'. Niets is zo efficiënt als wanneer de organisatie zelf kan aangeven wat zij redelijke normen acht en zich ook bereid toont daarnaar te handelen. Doordat de accountant de toereikendheid van de geformuleerde normen zal beoordelen en de naleving van de getroffen maatregelen zal toetsen, kan hij een belangrijke toegevoegde waarde hebben. De accountant zal zich daarbij meestal laten bijstaan door een EDP-auditor.

Figuur 3. Samenhang tussen beleid, normen en analyses.



OPSTELLEN VAN DE NORMEN

Het beveiligingsbeleid vormt het uitgangspunt voor het treffen van een evenwichtig stelsel van beveiligingsnormen. Om tot dat evenwichtig stelsel te komen zijn de volgende analyses van belang:
- afhankelijkheidsanalyse;
- bedreigingenanalyse.

De samenhang hiertussen is schematisch in figuur 3 weergegeven.

Afhankelijkheidsanalyse

Een afhankelijkheidsanalyse, ook wel gevoeligheidsanalyse genoemd [Jans91], houdt in dat vastgesteld wordt in hoeverre de door de informatiesystemen ondersteunde bedrijfsprocessen afhankelijk zijn van kwaliteitskenmerken als betrouwbaarheid en beschikbaarheid van de informatievoorziening en welke schaden kunnen optreden als gevolg van verstoringen in de informatievoorziening. Het resultaat van een afhankelijkheidsanalyse is:
- inzicht in de bedrijfsdoelstellingen en de bedrijfsprocessen;
- inzicht in de relatie tussen informatiesystemen en bedrijfsprocessen;
- inzicht in de relatie tussen de informatiesystemen onderling en tussen de verschillende componenten van die informatiesystemen;
- inzicht in de maximaal toelaatbare directe of indirecte schade als gevolg van het optreden van ongewenste gebeurtenissen.

Natuurlijk is het moeilijk om de maximaal toelaatbare schade te bepalen. Daarom is het veel praktischer om dit niet te kwantificeren, maar meer te rubriceren in de zin van laag, gemiddeld of hoog.

Een afhankelijkheidsanalyse kan op verschillende niveaus worden uitgevoerd. Zo zal (vaak impliciet) op strategisch niveau een uitspraak worden gedaan over algemeen commercieel, bedrijfseconomisch of maatschappelijk belang van bepaalde categorieën van informatievoorziening. Daar spelen elementen een rol als beschikbaarheid van de infrastructuur van de informatievoorziening in verband met commerciële snelheid van handelen. Zo zal een vluchtreserveringssysteem een veel hogere beschikbaarheid eisen van de IT-componenten dan het voorraadbeheersingssysteem van een tapijtgroothandel.

In het algemeen kan worden gesteld dat logistieke en besturingssystemen veel hogere beschikbaarheidseisen stellen dan boekhoudkundige systemen, maar dat aan de andere kant de laatste systemen hogere eisen stellen aan de toegangsbeveiliging (bijvoorbeeld ten behoeve van betaaltoepassingen). Ook wettelijke regelingen spelen daarbij

mogelijk een rol, bijvoorbeeld bescherming van persoonsgegevens.
Op tactisch niveau kan een analyse plaatsvinden van de afhankelijkheid van één informatiesysteem op grond waarvan concrete normen zijn te formuleren, of kunnen clusters van afhankelijke componenten worden geïdentificeerd op grond waarvan concrete normen zijn vast te stellen. Daarbij kan gedacht worden aan componenten in een rekencentrum die door meerdere informatiesystemen worden gebruikt bij de verwerking, en waarvoor het het meest praktisch is afzonderlijk normen op te stellen.

Bedreigingenanalyse

De volgende stap is de bedreigingenanalyse, waarbij geanalyseerd wordt aan welke bedreigingen een informatiesysteem en IT-componenten bloot staan. In deze fase wordt nog geabstraheerd van de reeds getroffen maatregelen. Het resultaat van een bedreigingenanalyse is een overzicht van bedreigingen waartegen de organisatie zich wenst te beveiligen en bedreigingen waartegen de organisatie zich niet wenst te beveiligen. Een vaak gehoorde zin in dit kader is dat een organisatie zich wenst te beveiligen tegen het kwaad van alle dag (en misschien iets meer). Daarbij wordt het treffen van maatregelen tegen bijvoorbeeld actiegroepen of bomaanslagen dan uitgesloten.

In theorie zijn verschillende risico-analysemethoden ontwikkeld en hebben verschillende organisaties praktische programma-tools ontwikkeld. Meestal bestaan deze tools uit geautomatiseerde checklists, al dan niet voorzien van aan te passen wegingsfactoren en risico-inschattingen. Echter, in de praktijk is steeds gebleken dat aan alle methoden bezwaren kleven, waarvan de belangrijkste zijn:
- de moeilijkheid van het inschatten van de kans op het optreden van een ongewenste gebeurtenis;
- de wijze waarop de kansen geaggregeerd moeten worden om vervolgens de effectiviteit van specifieke maatregelen te wegen;
- de vereiste deskundigheid voor het uitvoeren van de risico-analyses; en
- de lange doorlooptijd (en hoge kosten) die dergelijke onderzoeken vergen.

Daarom is het verstandiger zeker in de eerste opzet geen uitgebreide risico-analyse uit te voeren. Maar dat wil natuurlijk ook niet zeggen dat volledig aan de mogelijke bedreigingen voorbij moet worden gegaan. Zonder aan cijfermatige analyses te beginnen zijn de meeste betrokken medewerkers heel goed in staat aan te geven welke bedreigingen relevant zijn. Relevant wil in dat geval zeggen dat het manifest worden van een bedreiging aannemelijk is en voor de organisatie een zodanige schade oplevert dat het verantwoord is daar maatregelen tegen te treffen. Dit vereist natuurlijk wel medewerkers die enerzijds op de hoogte zijn van het belang van de bedrijfsprocessen en anderzijds van de gevolgen van het optreden van ongewenste gebeurtenissen. In dat kader kan het opstellen van scenario's hulp bieden. Een scenario is een beschrijving van een hypothetische gebeurtenis. Door in scenario's te denken kan men dialogen tussen de verschillende disciplines op gang brengen, gevoel krijgen voor voorwaarden waaraan voldaan moet zijn om iets te laten gebeuren of om aannames ter discussie te stellen.

Pas als in een later stadium de beveiligingsmaatregelen zijn gedefinieerd en zijn geïmplementeerd, zal de meer globale bedreigingenanalyse kunnen worden uitgebreid tot een volledige risico-analyse. Dan kunnen namelijk via gerichte (deel)onderzoeken bedreigingen, getroffen maatregelen, restrisico's en kosten van verder te treffen maatregelen tegen elkaar worden afgewogen.

Het opstellen van de normen zelf

Het opstellen van de normen zelf vindt plaats aan de hand van de resultaten van de afhankelijkheids- en bedreigingenanalyses. De afhankelijksheidsanalyse vormt met name de basis voor de kwaliteitseisen die in de normen zijn weergegeven, terwijl de bedreigingenanalyse vooral de beveiligingsnormen aandraagt. Het interpreteren van de analyses voor de vertaalslag naar de normen vergt een goed inzicht in de flexibiliteit van de organisatie met betrekking tot het kunnen omzetten van normen naar maatregelen. Het normenstelsel kan eenvoudig opsommend zijn indien de organisatie reeds een hoge beveiligingsgraad heeft en de medewerkers gemotiveerd zijn, terwijl een meer toelichtende beschrijving van de normen op zijn plaats is bij een organisatie waarbij nog maar beperkt met beveiliging rekening is gehouden.

Goede ervaringen zijn opgedaan met het laten opstellen van de normen door een 'neutrale' interne of externe deskundige.

De opgestelde normen dienen eenduidig te zijn, zodat degenen die vervolgens maatregelen dienen te treffen, de normen ook eenvoudig kunnen hanteren. Soms is het haast onmogelijk normen anders te formuleren dan in termen van maatregelen. Indien je dit wilt voorkomen, zal de norm meestal zo globaal moeten worden gedefinieerd dat de eenduidigheid in het gedrang komt en degenen die er later mee moeten werken er zich veel te weinig bij voor kunnen stellen.

Goede ervaringen zijn opgedaan met het laten opstellen van de normen door een 'neutrale' interne of externe deskundige, die zorgt dat voortdurend wordt afgestemd met de betrokken verantwoordelijken in de organisatie.. Daardoor wordt de voortgang erin gehouden en vindt een evenwichtige invulling plaats. Daarbij zijn verrassend goede resultaten behaald door beperkte afhankelijkheids- en bedreigingenanalyses onafhankelijk te laten uit-

accountants. Zoals eerder is aangegeven, kan deze toezichtfunctie op termijn worden uitgevoerd met behulp van een gedegen risico-analyse.

Overigens is op het terrein van de informatiebeveiliging mogelijkerwijs ook indirect een Quality Assurance-functie actief, met name voor het definiëren van verschillende richtlijnen voor documentatie en werkwijzen bij systeemontwikkeling. Door goed onderling overleg wordt uniformiteit in de uitvoering van werkzaamheden verkregen, hetgeen de kwaliteit van de produkten ten goede komt.

Ten slotte onderhoudt de security officer externe contacten en volgt ontwikkelingen die voor het beleid en de uitwerking daarvan van belang kunnen zijn.

Het *lijnmanagement* draagt in eerste instantie zorg voor de vertaling van het beleid naar de normen voor de eigen afdeling. Zoals eerder is aangegeven, gebeurt dit in nauw overleg met de security officer. Nadat de normen door het management zijn geaccepteerd, zal de lijnmanager met zijn medewerkers overgaan tot het definiëren van een werkbaar stelsel van maatregelen die de normen afdekken. Door daarbij de medewerkers te betrekken zal de motivatie voor de naleving sterk toenemen.

Controlemaatregelen zijn het meest effectief wanneer zij in de organisatie zijn verankerd, bijvoorbeeld door functiescheidingen.

Nadat de maatregelen zijn ingevoerd, ziet het lijnmanagement erop toe dat de medewerkers handelen in overeenstemming met de getroffen maatregelen. Eventueel kan deze toezichtfunctie worden uitgevoerd door een verbijzonderde interne-controlefunctie. Zeker in het kader van bijzondere deskundigheid (bijvoorbeeld binnen een rekencentrum) kan een EDP-auditor doeltreffend worden ingezet.

CONTROLE

Voor beveiliging geldt in sterke mate dat de doeltreffendheid mede afhangt van de discipline waarmee maatregelen worden nageleefd. Aangezien beveiliging vaak als gebruikersonvriendelijk of (door onwetendheid) ondoelmatig wordt ervaren, is er soms de neiging minder alert de voorschriften na te leven. Dit is natuurlijk funest voor de beveiliging als geheel. Daarom is voortdurende controle op de naleving essentieel, waardoor zo nodig bijsturing tijdig kan plaatsvinden, maar vooral steeds weer kan worden ingespeeld op de verantwoordelijkheid en motivatie van de individuele medewerkers.

De behoefte aan inzicht in de mate van naleving is vooral aanwezig bij het lijnmanagement, dat verantwoordelijk is voor de naleving van de maatregelen in de eigen afdeling. Controlemaatregelen zijn het meest effectief wanneer zij in de organisatie zijn verankerd, bijvoorbeeld door functiescheidingen. Indien om welke reden dan ook een proces hapert, zal dat een andere functie in het proces opvallen en derhalve een signalerende functie hebben, waardoor tijdig correctieve acties kunnen worden ondernomen.

Ook bij de directie die eindverantwoordelijk is voor het stelsel van beveiliging bestaat behoefte aan inzicht in de opzet en uitvoering van de beveiligingsmaatregelen. Naast de taak van de security officer op dit punt, wordt controle namens de directie vaak uitgevoerd door een verbijzonderd controle-orgaan, de interne accountantsdienst (IAD), waarin vaak ook EDP-auditing is vertegenwoordigd.
Het zal duidelijk zijn dat voor een efficiënte uitvoering van de verschillende controle-activiteiten een goede afstemming tussen de controlerende instanties zinvol is. Daardoor kunnen doublures worden voorkomen. Indien binnen de lijnorganisatie een (interne-) controlefunctie voorkomt zal de IAD met de interne-controlefunctie en de security officer nauwe contacten onderhouden.

Ook de externe accountant kan in dit geheel een rol vervullen. Indien de accountant een controle-aanpak volgt die erop is gericht primair de interne kwaliteitsorganisatie te toetsen (waarbij inbegrepen de geautomatiseerde gegevensverwerking), dan zal hij zijn bevindingen met betrekking tot de beveiliging van de automatisering volgens de Wet computercriminaliteit aan de directie en Raad van Commissarissen kenbaar moeten maken. Hoewel de bevindingen zeker niet het gehele terrein van de beveiliging van de informatievoorziening betreffen, zal het management toch een indicatie ontvangen over de toereikendheid van de opzet en uitvoering van de beveiligingsmaatregelen. Om niet een verkeerd verwachtingspatroon te krijgen, is het noodzakelijk dat het management goed op de hoogte is van de reikwijdte van het onderzoek van de accountant.

SAMENVATTING

De tijd is rijp voor het beleidsmatig aandacht schenken aan informatiebeveiliging. Iedereen is zich bewust van het belang van een betrouwbaar en continu proces van de informatievoorziening. Echter, iedereen lost dat op zijn manier op of gaat ervan uit dat anderen in de organisatie dat wel gedaan zullen hebben. Sommigen willen wel graag, maar weten niet wat ze moeten beveiligen of waar ze rekening mee moeten houden (bijvoorbeeld in het informatiesysteem of in de systeemsoftware). Resultaat is een ondoorzichtig vangnet van beveili-

gingsmaatregelen, waarvan het moeilijk is vast te stellen of het effectief en efficiënt is.
Daarom is het beleidsmatig omgaan met informatiebeveiliging een must geworden.

Indien meerdere functies bij de implementatie zijn betrokken, is het effectief niet direct in maatregelen af te dalen, maar een normenstelsel te ontwikkelen op grond waarvan te treffen beveiligingsmaatregelen worden vastgesteld. Daardoor ligt er een referentieboekwerk voor (bijna) alle situaties waarin informatiebeveiliging een rol speelt. Ook kan dat normenstelsel een goede rol spelen tussen (interne of externe) accountant en de organisatie. Soms krijgen accountants het verwijt dat ze niet duidelijk overbrengen wat hun normen zijn. Door acceptatie van de normen door de accountant weten de medewerkers gelijk aan welke normen zij zich dienen te houden.

Het uitvoeren van omvangrijke, kwantitatieve risico-analyses is meestal weinig effectief gebleken, door praktische en methodische problemen. Via directe baseline controls zijn snel acceptabele resultaten te behalen, omdat dan beperkt rekening behoeft te worden gehouden met de specifieke karakteristieken van de eigen organisatie. Een goede oplossing voor een aanpak waarbij de eigen organisatie wél wordt betrokken, zowel inhoudelijk als uitvoerend, wordt gevormd door het uitvoeren van de analyses ten aanzien van de afhankelijkheid, bedreigingen en kwetsbaarheid.

LITERATUUR

[BSI93] British Standards Institution, *A Code of Practice for Information Security Management*, 1993.

[Jans91] Mw. D. Jansen Heijtmajer, *Beveiligingsbeleid geautomatiseerde informatievoorziening*, Compact 1991/3.

[KPMG93-1] KPMG Klynveld, *Inbraak of doorbraak?, Analyse van de Wet computercriminaliteit*, mei 1993.

[KPMG93-2] KPMG Klynveld Management Consultants, *Certificering en kwaliteitszorg, Een gespannen relatie*, oktober 1993.

[s'Jac93] R.A. s'Jacob, *Syllabus Cursus Informatiebeveiliging*, KPMG Klynveld EDP Auditors, 1993.

[NGI92] Nederlands Genootschap voor Informatica, Afdeling beveiliging, *Beveiligingsbeleid en beveiligingsplan*, Kluwer bedrijfswetenschappen, 1992.

Drs. H.G.Th. van Gils RE RA
Is als senior manager werkzaam bij KPMG Klynveld EDP Auditors en doceert EDP-auditing in het kader van de post-doctorale Accountantsopleiding aan de Universiteit van Amsterdam. Hij heeft met name onderzoeken verricht naar de betrouwbaarheid van informatiesystemen en de kwaliteit van computercentra.

Het beoordelen van het testen van systemen

P. van Berge

De traditionele wijze van testen, waarbij de gebruiker tijdens de acceptatietest voor het eerst wordt geconfronteerd met het nieuw gebouwde, werkende systeem, is tijdrovend, arbeidsintensief en inefficiënt voor de betrokken disciplines.
Vanuit zijn praktijkervaringen bij de Kas-Associatie gaat Van Berge in op de voordelen van een werkwijze waarbij de gebruiker in een eerder stadium bij het testen wordt betrokken. De EDP-auditor kan zich bij deze testmethodiek een beter gefundeerd oordeel vormen over de kwaliteit van het testen dan bij de traditionele testwijze, mits aan een aantal voorwaarden is voldaan.

INLEIDING

Tijdens de ontwikkeling van een informatiesysteem leveren vele specialisten een bijdrage: de materiedeskundige, de informatie-analist, de functioneel en technisch ontwerper, de data(base) administrator, de programmeur, etc. Al deze disciplines werken op basis van systeemspecificaties. Elke bijdrage moet worden getest of getoetst. In de loop van het ontwikkeltraject dienen deze individuele bijdragen geïntegreerd te worden tot grotere eenheden. Uiteindelijk ontstaat zo het nieuwe systeem.

In de praktijk blijkt het bouwen van foutloos werkende systemen een utopie te zijn. In veel ontwikkelde applicaties worden vroeg of laat nog fouten geconstateerd. Deze fouten kunnen variëren van 'onbelangrijk' tot 'ernstig'. Een onbelangrijke fout is bijvoorbeeld een rubriek welke wordt afgedrukt op een andere plaats dan de gebruiker zou willen. Ernstige fouten zijn fouten die het programma doen stoppen of een onjuiste verwerking veroorzaken met alle gevolgen van dien: geldverlies, schadeclaims of zelfs verlies van mensenlevens.

In dit artikel worden de problemen behandeld waarmee systeemontwikkelaars, gebruikers en auditors bij de traditionele wijze van testen worden geconfronteerd. In een alternatieve wijze van testen wordt ingegaan op een aantal essentiële elementen van een gestructureerde testmethodiek en de gevolgen hiervan voor de auditor.

BEGRIPSBEPALING

Voor de begripsvorming wordt nader ingegaan op de begrippen systemen, testen en fouten.

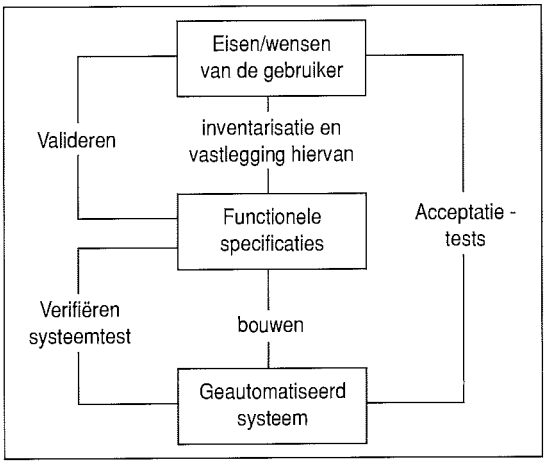
Systemen

Evenals natuurlijke systemen maken ook de door mensen ontwikkelde geautomatiseerde systemen deel uit van een groter systeem. Zo zal in de bancaire wereld een geldsysteem deel uitmaken van een cliëntensysteem dat op zijn beurt weer deel uitmaakt van de totale bedrijfsorganisatie (in feite ook een systeem). Ook al lijken systemen heel verschillend, zij vertonen toch een groot aantal overeenkomsten. Er bestaan gemeenschappelijke uitgangspunten, theorieën die op alle soorten systemen toegepast kunnen worden. We kunnen datgene wat technici en wetenschappers geleerd hebben over andere systemen ook toepassen op geautomatiseerde systemen. Zo is een belangrijk systeemprincipe uit de biologie de specialisatiewet: hoe meer een organisme aan zijn omgeving is aangepast, des te moeilijker is het voor dat organisme zich aan een andere omgeving aan te passen.
Als we dit vertalen naar automatisering: als een systeem optimaal aan een bepaalde CPU, programmeertaal of DBMS wordt aangepast, treden problemen op als een andere CPU of DBMS wordt aangeschaft. Of ook: als een informatiesysteem wordt ontwikkeld op basis van een bestaande gebruikerstoepassing zal het moeilijk zijn dit systeem aan te passen als de gebruikerseisen veranderen en evolueren. Kennis van de systeemtheorie kan informatici dus helpen geautomatiseerde informatiesystemen te begrijpen om daarmee stabiele, betrouwbare systemen te ontwikkelen.

Als we ons beperken tot de automatiseringswereld en de vraag 'Wat is een systeem?' stellen aan de specialisten, dan is het antwoord verschillend: de systeemprogrammeur verstaat hieronder de hardware, de programmeur noemt de software, de adviseur administratieve organisatie noemt de administratieve procedures, de boekhouder bedoelt de financiële administratie, terwijl voor de accountant het systeem 'alles' omvat. Dit artikel beperkt zicht tot de ontwikkelde software.

Testen

Testen is een belangrijk onderdeel van de kwaliteitsbeheersing bij de ontwikkeling van informatiesystemen. De vraag hierbij is of de kwaliteit van een systeem hetzelfde is als het foutvrij zijn van een systeem. Kwaliteit is meer dan het ontbreken van fouten. Aan de andere kant is het ontbreken van fouten een kwaliteitseis. Elke discipline bekijkt de kwaliteit (en ook het testen) vanuit zijn invalshoek: de gebruiker, de ontwerper, de database administrator.
We kunnen testen onderscheiden in valideren en verifiëren. Alvorens de functionele specificaties goed te keuren moet de gebruiker de juistheid en volledigheid ervan *valideren*. De technisch ontwerper moet de specificaties *verifiëren* vanuit zijn (technische) verantwoordelijkheid. Zowel gebruikers als de technisch ontwerpers voeren dus tijdens en na het ontwerpstadium een controle uit op de kwaliteit van het systeem. Bij communicatie- en interpretatieverschillen kan vroegtijdig worden ingegrepen. De samenhang tussen valideren en verifiëren kan schematisch worden weergegeven als in figuur 1.



Figuur 1. Samenhang tussen valideren en verifiëren.

Zodra de eerste programma's door de programmeur zijn opgeleverd, kan gecontroleerd worden of deze voldoen aan de specificaties. De volgende stadia kunnen worden onderscheiden: de programmatest, de systeemtest en de acceptatietest.

Fouten

Ervan uitgaand dat de functionele specificaties gevalideerd zijn door de gebruiker kunnen fouten in het systeem als volgt worden geformuleerd: het systeem reageert anders dan de specificaties aangeven of het systeem doet meer of minder dan de specificaties vereisen. Dit type fouten is goed te testen. De specificaties vormen immers een juist uitgangspunt bij de beantwoording van de vraag: goed of fout. Maar voor gebruikers zijn nog meer zaken als 'fout' aan te merken: bijvoorbeeld het niet gebruiken van functietoetsen met een standaardbetekenis (helpfunctie, terugbladeren, vooruitbladeren en dergelijke) of het ontbreken van standaarden voor print- en schermontwerp.

Uitgaande van de situatie dat fouten gemaakt worden moeten we, voor het bepalen van de testaanpak, antwoord geven op de vraag hoeveel fouten we ons in het eindprodukt kunnen veroorloven en welke investeringen in het testen nog economisch verantwoord zijn. Zo zal de programmeur van de besturing van een modern verkeersvliegtuig zich minder fouten kunnen permitteren (en dus langer testen) dan een programmeur die een overzicht van alle cliënten moet vervaardigen. Deze afweging is van invloed op de omvang en diepgang van de testactiviteiten, maar voor beiden geldt dat een

volledigheidstest van honderd procent een illusie is. Zo is uit onderzoek gebleken dat in het besturingssysteem van IBM (MVS) na negen jaar intensief gebruik nog steeds fouten werden geconstateerd. Ondanks deze fouten blijken organisaties toch uitstekend met dit besturingssysteem te kunnen werken. Met andere woorden: systemen behoeven niet volledig foutvrij te zijn om toch in de praktijk goed te functioneren. Als het in de praktijk onmogelijk is alle mogelijke situaties uit te testen betekent dit dat wij bij het testen selectief te werk moeten gaan. Dus alleen tests uitvoeren die een redelijk grote kans hebben een onacceptabele fout op te sporen.

Systemen behoeven niet volledig foutvrij te zijn om toch in de praktijk goed te functioneren.

TRADITIONELE WIJZE VAN TESTEN EN DE AUDIT

De traditionele fasering van testen is de volgende: na de programmatest door de programmeur, test de ontwerper het systeem. Na deze systeemtest voert de gebruiker een acceptatietest uit. Hierbij kan de gebruiker vaststellen dat aan zijn wensen en eisen, zoals vastgelegd in het functioneel ontwerp, is voldaan. De beslissing om tot invoering over te gaan is afhankelijk van de resultaten van de acceptatietest. Na akkoord van de gebruikersorganisatie wordt het systeem in produktie genomen.

In de praktijk levert deze wijze van testen problemen op voor de gebruikersorganisatie, de systeemontwikkelaar en de auditor. Zo wordt de gebruiker pas in de acceptatiefase met 'zijn' systeem geconfronteerd om de functionaliteiten en de gebruikersvriendelijkheid van het systeem te testen. Als de gebruiker in deze fase 'fouten' constateert moet het programma worden teruggeplaatst naar test, worden aangepast, overgedragen en opnieuw door de gebruiker worden getest.
Deze procedure herhaalt zich totdat de gebruiker geen fouten meer constateert. Het gevolg is dat de gebruiker onder grote tijdsdruk komt te staan om het systeem voor de geplande inproduktiename te accepteren. Door deze druk bestaat bij hem de neiging de acceptatietest minder zorgvuldig uit te voeren. Kortom, een inefficiënte wijze van testen welke tijdrovend, arbeidsintensief en voor de betrokkenen frustrerend is. Bovendien bestaat een grote kans dat de tests van de gebruiker en de systeemontwikkelaar elkaar overlappen.

Rol auditor

In NIvRA-geschrift 43 [NivR88] wordt onder 4.7 'Voorbereiden van de acceptatietest' gesteld dat de gebruiker bij de test de juistheid en volledigheid van het functioneren van het systeem moet vaststellen. De auditor moet kunnen beoordelen of aan deze eis is voldaan. Hij moet kunnen beoordelen of alle mogelijkheden zijn getest. Vragen moeten worden beantwoord als: is er een 'beoordeelbaar' testdossier aanwezig, zijn er uitvoervoorspellingen gemaakt, zijn alle mogelijke testsituaties (ook bij online-systemen) opgenomen in het testdossier.

In de praktijk blijkt dat systeemontwikkelaars en gebruikers aanvankelijk alle geteste situaties wel opnemen in het testdossier. Maar gaandeweg wordt hier minder aandacht aan besteed. Als het management aan de auditor een oordeel vraagt over de kwaliteit van de test van het ontwikkelde systeem kan de auditor rapporteren dat niet alle testsituaties in het dossier zijn aangetroffen. Maar een concreet antwoord op de vraag of in voldoende mate is getest kan, op basis van het dossier, niet worden gegeven. Als de auditor een objectief oordeel wil geven zal hij een grote mate van creativiteit aan de dag moeten leggen: hij zal zelfstandig alle mogelijke functionele en systeemtechnische testgevallen moeten bedenken, vastleggen en vergelijken met de door de systeemontwikkelaar/gebruiker opgestelde testgevallen. Dit vereist van de auditor niet alleen gedetailleerde kennis van de applicatie maar het legt eveneens een groot beslag op diens tijd. Waarbij het maar de vraag is of dit voor het bedrijf economisch verantwoord is.

Samengevat: De traditionele wijze van testen en beoordelen levert voor alle disciplines problemen op. Hieronder wordt daarom ingegaan op een andere wijze van testen en de beoordeling ervan. De accenten liggen hierbij met name op de systeemtest en op de aanwezigheid van een gestructureerde testmethodiek.

EEN ALTERNATIEVE WIJZE VAN TESTEN EN DE AUDIT

Bij de alternatieve wijze van testen gelden de volgende uitgangspunten:

Uitgangspunt 1:
Systeemontwikkelaars en gebruikers moeten rekening houden met de aanwezigheid van fouten in het systeem. Met andere woorden, het ontbreken van fouten is een uitzondering, fouten zijn 'normaal'.

Uitgangspunt 2:
In de traditionele systeemtest worden systeemfuncties geïntegreerd en wordt het volledige systeem aan een grote 'integratietest' onderworpen. Deze manier van testen (de 'big bang-test') blijkt in de praktijk niet efficiënt en moeilijk beheersbaar en bestuurbaar te zijn. Deze problemen heeft de organisatie niet als gekozen wordt voor een vorm van

'incremental testing'. In plaats van één grote 'stortvloed' van problemen te creëren worden de fouten hanteerbaar gemaakt. De projectleider heeft meer grip op de voortgang van de test.

Uitgangspunt 3:
In tegenstelling tot de traditionele wijze van testen vindt tijdens de systeemtest zowel de test van de systeemontwikkelaar als van de gebruiker plaats. De systeemtest vindt plaats in een separate systeemtestomgeving. Dit is een beveiligde omgeving waarin zich een verzameling op elkaar afgestemde testsets en programma's bevindt. De gebruiker kan in een 'proeftuin' het ontwikkelde systeem leren kennen en uitproberen. Hij wordt dan automatisch getraind in het gebruik van het later in produktie te nemen systeem.

Na akkoord van de testresultaten van de gebruiker worden de programma's, JCL en parameters overgedragen aan het rekencentrum. Het rekencentrum is, als beheerder van de technische infrastructuur, met name geïnteresseerd in de technische implicaties welke de uitvoering van de programma's met zich meebrengt.

Om de continuïteit in de verwerking te kunnen garanderen moeten de programma's voldoen aan een aantal criteria. Voordat een programma in produktie wordt genomen, moet dit programma getoetst worden aan deze criteria. Dit gebeurt dan in een separate 'semi-produktie-omgeving'. De acceptatietest is dus veeleer een 'technische acceptatietest' om de overgedragen programmatuur te toetsen aan de gestelde eisen: controle op het overdrachtsdossier en het beoordelen van de performanceaspecten. Het grote voordeel van deze werkwijze is dat aan de eerder genoemde bezwaren tegemoet wordt gekomen.
De verschillen tussen de traditionele en de alternatieve wijze van testen zijn schematisch weergegeven in figuur 2.

Soort test	Conventioneel	Alternatief
Systeem-test	a. Functionele test systeem-ontwikkelaar	a. Functionele test systeem-ontwikkelaar b. Functionele test gebruiker
Acceptatie-test	a. Functionele acceptatie-test gebruiker b. Technische acceptatietest Rekencentrum	a. Technische acceptatietest Rekencentrum

Figuur 2. Conventionele en alternatieve teststrategie.

De concrete invulling van de teststadia is dan als volgt:

Programmatest

Hierbij worden afzonderlijke programma's getest in relatie tot de programmaspecificaties zoals deze in het technisch ontwerp zijn opgenomen. De meest gebruikte aanpak hierbij is dat de programmeur het door hem geschreven programma test. Dit houdt allereerst in het 'debuggen', dat wil zeggen draaiend maken van een programma.

Systeemtest

In deze fase wordt het systeem voor het desbetreffende increment getest. Deze test wordt in eerste instantie gedaan door de systeemontwerper. Hierna wordt de gebruiker bij de systeemtest betrokken. Door de gebruiker er nu reeds bij te betrekken raakt deze vertrouwd met zijn systeem en kan hij eventuele tekortkomingen die niet tijdens de validatie van het functioneel ontwerp naar voren zijn gekomen, signaleren. De accenten bij de test van de gebruiker liggen dus met name op het gebruikersgemak van het ontwikkelde systeem en het praktische werken ermee. Het functioneren van het systeem conform de specificatie is de verantwoordelijkheid van de systeemontwikkelaar. De doorlooptijd van de gebruikerstest kan hierdoor aanzienlijk worden verkort.

Acceptatietest

Om aan de eisen van betrouwbaarheid, tijdigheid, beschikbaarheid en efficiency te kunnen blijven voldoen zullen er vanuit de technische infrastructuur eisen worden gesteld aan de ontwikkelde systemen. Het rekencentrum zal eisen en standaarden formuleren met betrekking tot de ter acceptatie aangeboden programma's. Deze eisen kunnen betrekking hebben op de hardware (bijvoorbeeld applicaties moeten gebruik maken van de aanwezige technische infrastructuur) en op de verwerking (bijvoorbeeld programma's mogen niet vastlopen op 'foutieve' records in juiste invoerbestanden of op lege invoerbestanden).

Uitgangspunt 4:
Het vierde en laatste uitgangspunt is de aanwezigheid van een testmethodiek. Bij een testmethodiek wordt gestructureerde aandacht besteed aan de volgende aspecten:

Functiescheiding

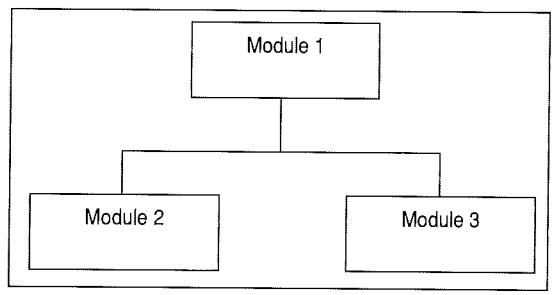
Onderscheid kan worden gemaakt in de functiescheiding binnen de afdeling Systeemontwikkeling (programmeur en ontwerper) en tussen de systeemontwikkelafdeling en de gebruikersorganisatie. Op deze aspecten wordt hieronder nader ingegaan.
Onderscheiden worden de 'white box-test' (WBT) en de 'black box-test' (BBT). De WBT controleert de eigenschappen van het programma zoals de pro-

grammeur deze heeft beschreven. Als deze test wordt uitgevoerd door de programmeur zelf is deze test relatief onbetrouwbaar omdat interpretatiefouten er niet uit worden gehaald. Beter is deze test door een collega-programmeur te laten uitvoeren. Deze test is in staat de zwakheden in de structuur van het programma bloot te leggen. Met name de stabiliteit van het geschreven programma moet worden aangetoond: raakt het programma niet in een loop, breekt het programma niet voortijdig af.

De technisch ontwerper controleert met behulp van de BBT of het programma doet wat het volgens de specificaties moet doen. Indien de programmeur de BBT zou uitvoeren bestaat het gevaar dat deze niet objectief staat ten opzichte van de specificaties. De BBT moet inzicht geven of het programma geen ongewenste eigenschappen heeft. Het resultaat hiervan kan zijn:

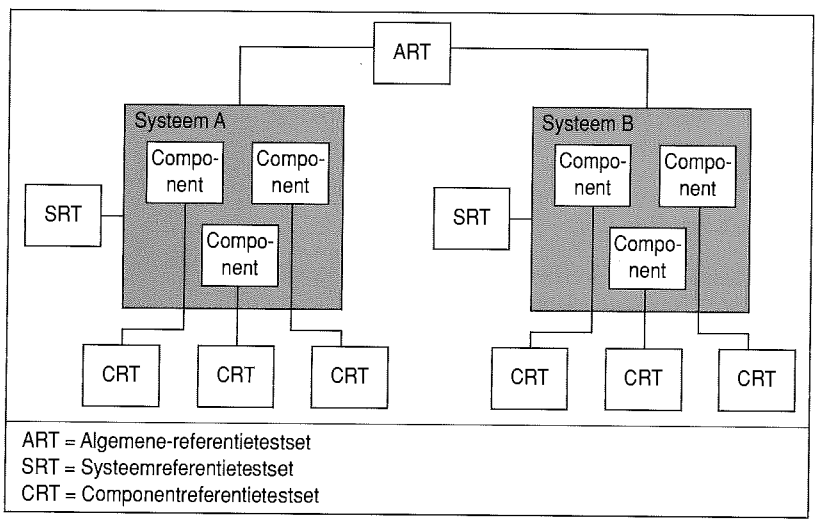
- de specificaties zijn weliswaar onduidelijk maar het programma werkt toch goed;
- de specificaties zijn juist maar het programma werkt onjuist; het programma moet dus worden aangepast;
- de specificaties zijn onduidelijk en het programma werkt onjuist: beide moeten worden aangepast.

Bij de genoemde alternatieve wijze van testen vindt in de systeemtestomgeving zowel de test van de systeemontwikkelaar als de gebruikerstest plaats. Van een door automatisering ondersteunde functiescheiding (aparte acceptatie-omgeving) tussen gebruikers en systeemontwikkelaars is geen sprake meer: de systeemtest en de gebruikerstest zijn de gemeenschappelijke verantwoordelijkheid van het projectteam.



Figuur 3. Modulaire opbouw van de test.

Figuur 4. Classificatie van testgegevens.



Modulariteit

Het systeem moet qua structuur zodanig gebouwd zijn dat het mogelijk is ook de test modulair op te zetten (zie figuur 3).

Bij een modulaire opbouw moet het mogelijk zijn de modules 2 en 3 afzonderlijk te testen. Vervolgens kan module 1 getest worden inclusief de relatie van module 1 naar module 2 en de relatie van module 1 naar module 3 zonder de modules 2 en 3 opnieuw te testen.

Herhaalbaarheid

Een test moet herhaald kunnen worden en daarbij identieke resultaten geven. Hierbij doet zich een aantal praktische problemen voor: technisch bijvoorbeeld om vergelijkbare testresultaten te reproduceren, organisatorisch bijvoorbeeld het reproduceren van de beginsituatie. Voor de technische problemen zijn er technische oplossingen in de vorm van programmatuur om testgegevens te kunnen vergelijken en om bestanden weer in hun beginstand te kunnen terugplaatsen. Organisatorische problemen zijn: het beheer van de testbestanden, het beheer van de testresultaten en de registratie van de testlog. Een hulpmiddel hierbij is het classificeren van de testgegevens. Onderscheiden kunnen worden de 'algemene-referentietestsets', de 'systeemreferentietestsets' en de 'componentreferentietestsets'.

Een algemene-referentietestset is een gegevensverzameling die door meerdere systemen wordt gebruikt. Hiervan is maar één versie in omloop. Voorbeelden hiervan in de bancaire wereld zijn de cliëntgegevens (cliënten-database) en de fondsgegevens (fondsen-database).

De systeemreferentietestset is een gegevensverzameling waaraan door maar één systeem wordt gerefereerd. Vaak zal de inhoud van een dergelijke testset gerelateerd zijn aan een algemene-referentietestset. Een voorbeeld hiervan zijn de stuknummers van een fonds. De fondsen die hierin voorkomen komen ook voor in de fondsen-database.
De componentreferentietestset is een gegevensverzameling die wordt gebruikt om een component te testen. Een component is een te testen eenheid die bestaat uit één of meer programma's die zowel logisch als technisch met elkaar verbonden zijn. Een batch-testcomponent is gelijk aan een job. De samenhang tussen de verschillende klassen van testgegevens is schematisch weergegeven in figuur 4.

Meetbaarheid/controleerbaarheid

De specificaties van het te testen systeemdeel moeten exact zijn gedefinieerd. Slechts dan kan de uit-

komst van de test beoordeeld worden. De volgende vormen van meetbaarheid kunnen worden onderscheiden:
- de testresultaten, om een juiste vergelijking met de in de specificaties voorkomende eisen mogelijk te maken;
- de testactiviteiten, om vast te stellen welke systeemfuncties door een test worden gedekt;
- de testeffectiviteit, om te bepalen hoe volledig bepaalde systeemfuncties met een test worden gedekt.

Efficiency

Aan een vorm van efficiency is reeds aandacht besteed door een vroegtijdige inschakeling van de gebruiker bij de systeemtest (proeftuin). Hiermee kan de gebruiker op een praktische wijze met het systeem leren omgaan en wordt een inefficiënte wijze van overdragen van de test voorkomen.

Indien er bij het bepalen van testgevallen naar gestreefd wordt om alle in de praktijk mogelijke situaties te testen zal de testset een oneindig grote omvang aannemen. De uitvoering en de beoordeling van de resultaten zullen een fors tijdsbeslag leggen op de afdeling Systeemontwikkeling, de gebruikersorganisatie en de auditor. Uit het oogpunt van test-efficiency mag de test derhalve niet te omvangrijk zijn, maar moet hij wel 'doeltreffend' zijn. De volgende criteria zijn hiervoor aan te geven:

Equivalentieklasse
Bij het samenstellen van de test moeten beperkingen worden opgelegd. Het doel moet zijn een 'eindige' verzameling testgevallen die een zo groot mogelijke kans heeft om eventueel aanwezige fouten op te sporen. Er is derhalve geen tweede testgeval aanwezig dat een vergelijkbare invoerconditie test.

Bijvoorbeeld: de waarde van een opdrachtsoort mag liggen tussen de 100 en de 200. Het is niet efficiënt testgevallen te maken met de waarden 125, 130, 150 en 180. Het is doeltreffender dit zelfde veld te testen op de waarden 50, 150 en 250. Hierbij worden dus alle gebieden waarin de boven- en ondergrens de mogelijkheden van het veld verdelen een keer geraakt. Als een testgeval in een bepaalde equivalentieklasse een fout op het spoor komt, dan is het aannemelijk dat alle andere testgevallen uit de klasse dezelfde fout op het spoor komen. Uiteraard zijn deze veronderstellingen niet honderd procent zeker, maar in elk geval zijn drie testgevallen, elk uit een verschillende equivalentieklasse, beter dan drie testgevallen uit dezelfde klasse.

Grenswaarde-analyse
Grenswaarden zijn die waarden van invoer- en uitvoervelden die precies op, juist onder of juist boven de grenzen van de equivalentieklassen liggen. In plaats van het nemen van zo maar een waarde uit een equivalentieklasse nemen we één of meer waarden die ervoor zorgen dat de grens van de equivalentieklasse door de test wordt gecontroleerd. Bijvoorbeeld: werk de dispositieruimte bij als de effectieve waarde groter is dan 10.000. We kunnen dan testgevallen uitschrijven voor: 9.999, 10.000 en 10.001.

'Genoeg' volledigheid

Om niet te veel fouten achter te laten moet de test volledig genoeg zijn. Het combineren van alle in een systeem te testen vraagstellingen levert meestal een onmetelijk groot aantal benodigde testgevallen op. Om dit probleem te voorkomen zijn criteria te definiëren die 'genoeg' volledigheid kunnen garanderen:
- statement coverage;
- decision coverage;
- condition coverage.

Van statement coverage is sprake als elke in de specificaties voorkomende actie ten minste één keer door een testgeval wordt geraakt; in feite is dit een minimumtesteis voor alle programmatuur.

Bij decision coverage en condition coverage wordt elke gespecificeerde beslissing respectievelijk vraagstelling volledig door de test geraakt en wel zodanig dat alle mogelijke antwoorden op de beslissing/vraagstelling minimaal één keer in het resultaat voorkomen.

CONCLUSIE

Traditioneel test de gebruiker in de acceptatietest de functionaliteiten en de gebruikersvriendelijkheid van 'zijn' systeem. Bij 'fouten' moet de programmatuur worden teruggeplaatst naar test, worden gecorrigeerd, overgedragen en opnieuw worden getest door de gebruiker. Deze procedure wordt herhaald totdat geen fouten meer worden gevonden. Deze wijze van testen is tijdrovend, arbeidsintensief en inefficiënt voor de betrokken disciplines.

Een alternatief voor deze werkwijze is de gebruiker eerder te betrekken bij de test: in een beveiligde systeemtest-omgeving wordt zowel de test van de systeemontwikkelaar als de test van de gebruiker uitgevoerd. Ervan uitgaand dat het functioneel ontwerp door de gebruiker reeds is gevalideerd, kan de gebruikerstest een relatief eenvoudige test zijn met een korte doorlooptijd. Een incrementele wijze van testen bevordert dit proces nog. Van een door automatisering ondersteunde functiescheiding (aparte acceptatie-omgeving) is dan geen sprake meer: de systeemtest en de gebruikerstest zijn de gemeenschappelijke verantwoordelijkheid van het projectteam.

De accenten van de test liggen grotendeels op de test van de systeemontwikkelaar. Deze moet hierin worden ondersteund door een gestructureerde testmethodiek waarin een aantal principes wordt gehanteerd. De acceptatietest wordt beperkt tot een test van het rekencentrum om te toetsen of aan de gestelde eisen is voldaan.

P. van Berge
Is sedert medio 1978 in dienst bij de Kas-Associatie. Tot 1987 is hij werkzaam geweest bij de afdeling Systeemontwikkeling, als systeemontwerper en informatie-analist. Tevens heeft hij enige tijd gefunctioneerd als teamleider onderhoud van de systeemgroep Effecten. Halverwege 1987 is hij overgestapt naar de Interne Accountants Dienst/EDP audit. Hij is op dit moment werkzaam als senior system EDP-auditor met als belangrijkste werkvelden de applicatieve systemen in ontwikkeling en het onderhoud hiervan.
Met betrekking tot het eerste veld participeert hij in een groot aantal projecten met interne controle en beveiliging als aandachtsgebied.

Het uitgangspunt dat de test van de gebruiker juist en volledig moet zijn, is praktisch onmogelijk te realiseren. Aanvaard moet worden dat fouten aanwezig zijn. Maar een probleem is dat we niet weten welke fouten dit zijn. Een gestructureerde testmethodiek is een belangrijke bijdrage om fouten tot op een 'aanvaardbaar' niveau terug te dringen. Voorwaarde hierbij is dat in deze methodiek een aantal principes wordt gedefinieerd met betrekking tot functiescheiding, modulariteit, herhaalbaarheid, meetbaarheid, efficiency en 'volledigheid'. De rol van de auditor verplaatst zich dan van het per systeem afzonderlijk 'toetsen van het dossier' naar het 'toetsen van de testmethodiek' en op het gebruik ervan. De auditor kan dan een beter gefundeerd oordeel geven over de kwaliteit van het testen.

LITERATUUR

[NIvR88] NIvRA, *Automatisering en controle; Deel V. Organisatorische maatregelen en controletechnieken voor de ontwikkeling van geautomatiseerde informatiesystemen*, NIvRA-geschrift 43, Kluwer, 1988.

[Mors91] N.P.M. Mors en E.A.P. Diemer, *Testen van informatiesystemen*, Cap Gemini, 1991.

[Turn90] W.S. Turner, R.P. Langerhorst, G.F. Hice, H.B. Eilers, A.A. Uijttenbroek, *SDM System Development Methodology*, Cap Gemini Publishing, 1990.

EDP AUDITORIUM

BOEKBESPREKING

Post-doctorale opleiding EDP-Auditing referatenbundel 1

R. Barends

Inleiding

De afsluiting van de post-doctorale EDP-Auditingopleiding aan de Erasmus Universiteit wordt gevormd door een door de student op te stellen en te verdedigen referaat. Mede gezien het aantal positieve reacties en de duidelijk aanwezige vraag naar reeds beschikbare referaten, is besloten selecties van referaten te bundelen en periodiek te publiceren. Als belangrijkste criteria voor selectie gelden:
- de lezenswaardigheid van het referaat voor een brede en professionele lezersgroep;
- de aard en de verscheidenheid van onderwerpen;
- de toegevoegde waarde voor de EDP-Auditingopleiding en het vakgebied.

Inmiddels is het eerste nummer in de reeks verschenen. De referaten die zijn opgenomen in deze bundel hebben alle betrekking op de verwerkingsorganisatie.
Achtereenvolgens zijn referaten over de volgende onderwerpen opgenomen:
- Service-level Management, L.M.C. Jaspers;
- Controleerbaarheid van de COSSO-beveiligingschecklist, H.F. van der Horst;
- Water en Vuur, J.F. Kuperus en G.H.M. Meijer;
- Effectiviteit van logging, R. Wasman.

De referaten handelen primair over de toepassing van het vakgebied EDP-auditing op verschillende specifieke deelgebieden. In de eerste bundel zijn geen artikelen opgenomen die zich richten op de meer theoretische/fundamentele aspecten van het vakgebied.

Service-level Management
Het accent van dit referaat ligt duidelijk op de analyse van de kenmerken van service level agreements en de organisatie voor het beheer, het zogenaamde service level management.
Hoewel ook aandacht wordt besteed aan EDP-auditingaspecten op dit terrein, geldt dat deze zich voornamelijk beperkt tot een opsomming van de aandachtsgebieden. Het belang voor de EDP-auditor is vooral gelegen in de analyse van de inhoud van de service level agreements. Met name door de opname van enkele modelcontracten wordt de lezer een goede mogelijkheid geboden de gedachtengang die geleid heeft tot de geformuleerde conclusies en aanbevelingen te volgen. Hoewel geen modelaanpak is opgenomen, biedt de uitgevoerde analyse wel een groot aantal aanknopingspunten voor de EDP-auditor die betrokken is bij het opstellen of controleren van service level agreements.

Controleerbaarheid van de COSSO-beveiligingschecklist
Ook dit artikel moet worden gezien als een kritische analyse. Binnen het referaat worden op een heldere wijze de tekortkomingen op het gebied van de controleerbaarheid van de COSSO-beveiligingschecklist geschetst. Aangezien de checklist te veel ruimte laat om tot een eenduidig oordeel te kunnen komen wordt beargumenteerd dat een controleprogramma noodzakelijk is om de tekortkomingen te ondervangen.
Voor een EDP-auditor die betrokken raakt bij de invulling van de checklist zeker een aanrader. Echter, door recente ontwikkelingen op dit terrein (ISO 9000-certificering) is het belang van de COSSO-beveiligingschecklist, althans in de vorm zoals behandeld in het referaat, in betekenis afgenomen.

Water en Vuur
De voornaamste doelstelling van dit artikel is de lezer in te wijden en meer inzicht te geven in het begrip brand. Niet de organisatorische aspecten worden behandeld, maar de bouwkundige punten die relevant zijn in relatie met het uitbreken van brand worden nader uitgewerkt.
Na een inwijding in de bouwkundige/technische terminologie worden de aandachtsgebieden voor de EDP-auditor aangegeven. Het merendeel van de EDP-auditors zal hier echter in de praktijk niet of nauwelijks mee geconfronteerd (willen) worden. Opmerkelijk in dit verband is zeker ook een deel van de conclusie van het referaat. Hierin wordt namelijk gesteld dat de specialistische kennis die nodig is voor het beoordelen van de preventieve en repressieve technische maatregelen doorgaans niet van een EDP-auditor kan worden verwacht. Hierdoor lijkt het erop dat het referaat een onderwerp behandelt dat niet tot het terrein van de EDP-auditing kan worden gerekend.

Effectiviteit van logging
Het laatste referaat geeft een gestructureerd overzicht van de diverse aspecten rond logging in een MVS-omgeving. Hoewel het gekozen onderwerp dit niet direct doet verwachten, is het mede door de heldere formulering en opbouw een zeer lezenswaardig referaat. De gekozen systematiek, waarbij aan de hand van het OSI management framework de 'Soll-positie' per systeemcomponent wordt afgestemd met de 'Ist-positie' van de specifieke subsystemen in een MVS-omgeving, spreekt tot de verbeelding.
Voor wie zich niet laat afschrikken door het gebruikte IBM-jargon een must indien snel inzicht moet worden verkregen in de mogelijkheden en de onmogelijkheden van logging.

De bundel is verkrijgbaar via het secretariaat van de opleiding EDP-Auditing, Vakgroep ACAB, Erasmus Universiteit Rotterdam, tel. 010-4081508.

CUMULATIEF

Overzicht van eerder verschenen artikelen in Compact
Een compilatie van artikelen over informatica en recht die in eerdere Compacts zijn verschenen, is, aangevuld met actuele bijdragen over dit onderwerp, opgenomen in *Twintig over Informatietechnologie en recht*. Twintig auteurs behandelen een breed spectrum van aspecten van de raakvlakken van informatietechnologie en recht op voor EDP-auditor, manager, adviseur, jurist en accountant toegankelijke wijze.
Het boek is verkrijgbaar via de boekhandel onder nummer: ISBN 90 14 04634 0.

1 20e jaargang 93/1 lente 1993

Netwerkmanagement, de organisatorische opzet en financiële beheersing
ir. E.J. Evelo

Akzo en telecommunicatie, de organisatorische ontwikkeling
H. Reijn

SURFnet, beveiliging in een open netwerk
E. Zegwaart

Beveiliging van digitale kieslijnen
drs.ing. D. Brouwer

Secure Cash Management; an audit perspective
M. Kennett BA

Nieuwe ontwikkelingen in de cryptografie: Kerberos en Digital Signature Standard
drs. T.P. de Vries

Beveiligingsperikelen rondom Novell NetWare
J.L. Ramos Najera

2 20e jaargang 93/2 zomer 1993

Informatietechnologie duur? I/T Assessment: een beproefde methode voor het beoordelen van effectiviteit en efficiëntie van de informatieverzorging
drs. B.T. Janssen, ing. W.J.D. Koot en ir. E.J. Mutsaers

Prioriteitenstelling met Decision
dr. P.J. van Meel RI

De audit van een IT-investeringsaanvraag
drs.ing. S.R.M. van den Biggelaar en drs. P.P.M.G.G. Brouwers

Verzekerbaarheid van automatiseringsrisico's
mw.mr.drs. A.W. Duthler

Beveiligingsstandaard voor informatiesystemen
prof.dr.ir. R. Paans RE

Global electronic mail: integratie van elektronische post met X.400
ir. A. van Kooij

3 20e jaargang 93/3 herfst 1993

De toegevoegde waarde van EDP-auditing bij systeemontwikkeling
ir. J.A. Verstelle

Normenstelsels voor systeemontwikkeling: hoe bruikbaar zijn deze?
mw.drs. C.D.M. van der Veen

Projectbeheersing en -audit: contingency-benadering vereist
ir. B.A.W.M. Bruns

De toegevoegde waarde van inspectietechnieken tijdens het ontwikkeltraject
B. Rooth

Invoering van informatiesystemen
drs. Th.H. van Hesteren

Twintig vuistregels voor 'foutloos' onderhoud
E. Bergler

4 20e jaargang 93/4 winter 1993

Ontwikkelingen in de accountantscontrole in een geautomatiseerde omgeving
drs. R.G.A. Fijneman RE RA

Aandacht voor interne controle tijdens systeemontwikkeling
drs. J.J. van Beek RE RA

Audit automation
drs. L.H. Dam RA en drs. P. Veltman RE RA

Operational auditing en EDP-auditing; is hier sprake van een begripsverwarring?
J.C. Boer RE RA

Accountant, EDP-auditor en jurist: een multidisciplinaire samenwerking
mw. mr. drs. A.W. Duthler

Automatiseringsrisico's, verzekeringen en de rol van de accountant
drs. G.J.W.C. Vankan

Geautomatiseerde betalingen
drs. R. Oudega en drs. P. Veltman RE RA