KWARTAALBLAD EDP-AUDITING

1993 / 2

KOSTEN- EN BATENPROBLEMATIEK VAN INFORMATIETECHNOLOGIE

ZOMER COMPACT

Compact ®
Jaargang 20, nummer 2
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 RE RA (hoofdredacteur)
drs. R.G.A. Fijneman RE RA
prof. A.W. Neisingh RE RA
drs. P. Veltman RE RA

Redactiesecretariaat
Mw. A.M.F. Hofland, KPMG Klynveld EDP Auditors, K.P. van der Mandelelaan 41, 3062 MB Rotterdam
Tel.: 010 - 453 47 40
Fax : 010 - 453 47 77

Vormgeving
Bureau Karakter, Delft

Aan dit nummer werkten mee
drs. E.W. Berghout
drs.ing. S.R.M. van den Biggelaar
drs. P.P.M.G.G. Brouwers
mw.mr.drs. A.W. Duthler
drs. B.T. Janssen
ir. A. van Kooij
ing. W.J.D. Koot
dr. P.J. van Meel RI
ir. E.J. Mutsaers
prof.dr.ir. R. Paans RE

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

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.

De kosten- en batenproblematiek van informatietechnologie (IT) staat al geruime tijd volop in de belangstelling. Precies een jaar geleden is in Compact (1992/2) uitvoerig aandacht besteed aan de bedrijfseconomische benadering van informatietechnologie. Met name theoretische beschouwingen stonden daarbij centraal, waarbij slechts in beperkte mate praktijkervaringen zijn belicht.

Gezien de voortdurende aandacht voor genoemde problematiek vanuit een theoretische invalshoek lijkt het zinvol vooral eens vast te stellen hoe in de praktijk de kosten en baten van informatietechnologie worden beheerst. Op basis van praktijkervaringen kan desgewenst een theoretische onderbouwing en/of methode worden aangevuld en/of ontwikkeld. Een soort 'state-of-the-art' om inzicht te verkrijgen in de wijze waarop door organisaties pragmatisch invulling wordt gegeven aan het beheersen van bedoelde kosten en baten.

Bij de verdere concretisering bleek dat het onderwerp nog onvoldoende is uitgekristalliseerd om deze 'state-of-the-art' goed te kunnen geven. Hierdoor is niet een themanummer tot stand gekomen dat geheel is gewijd aan praktijkervaringen met betrekking tot het beheer van kosten en baten van informatietechnologie. Misschien zijn managers en EDP-auditors ook in de praktijk te veel op zoek naar kwantitatieve benaderingen om de IT-vraagstukken te kunnen behandelen. Het relatief jonge vakgebied EDP-auditing poogt voor de uit te voeren audits, en dus ook voor kosten/baten-vraagstukken, duidelijke normen te ontwikkelen. Wellicht dat EDP-auditors, evenals de financiële auditors, voor een aantal gebieden tot de conclusie moeten komen dat het 'professional judgement' van doorslaggevend belang is en blijft.

Ondanks bovenstaande overwegingen wordt vanuit een aantal praktijkervaringen toch een tipje van de sluier ten aanzien van het beheersen en beoordelen van de kosten en baten van informatietechnologie opgelicht. Voordat deelproblemen op het gebied van informatietechnologie kunnen worden opgelost, is inzicht in de huidige situatie van het IT-beheer benodigd. In de praktijk blijkt een duidelijke meting van de huidige situatie ten aanzien van het beheer van informatietechnologie toegevoegde waarde op te leveren voor het management. De praktijkervaringen opgedaan met I/T Assessment tonen aan dat beheersingsproblemen in en rondom informatietechnologie niet geïsoleerd kunnen en moeten worden benaderd.

In vele organisaties zijn de middelen zowel qua menscapaciteit als qua financiën schaars, waardoor bij het inrichten en/of vervangen van informatietechnologie steeds sprake is van een keuzeprobleem. Overigens is dit keuzeprobleem niet uniek voor de IT-omgeving. Prioriteiten onderkennen is van belang, waarbij in de praktijk een hulpmiddel is ontwikkeld waarmee de benodigde besluitvorming kan worden gerationaliseerd. Het beoogde effect van de beschreven benadering is om de controverse tussen gelijk hebben en gelijk krijgen bij de besluitvorming te verminderen. Nadat prioriteiten zijn bepaald, dienen concrete investeringsvoorstellen te worden opgesteld. Diverse IT-investeringsaanvragen worden voorzien van oneigenlijke argumenten. Het gelijk krijgen, met andere woorden een goedkeuring van het management verwerven, is daarbij belangrijker dan het gelijk hebben. Met name het inhoudelijk beoordelen van IT-investeringsaanvragen op al hun merites dient verder te worden ontwikkeld. Een beschreven auditaanpak biedt de mogelijkheid om hieraan doelgericht te werken.

Echter, ook bij IT-investeringen kunnen achteraf problemen ontstaan in termen van de hardware levert niet de verwachte performance en/of de software sluit onvoldoende aan bij de gedefinieerde informatiebehoeften. Een belangrijke vraag is dan wie waarvoor verantwoordelijk is en in hoeverre de beroepsaansprakelijkheid voor de automatiseringsbranche hierop is afgestemd. De (toenemende) verwantschap tussen EDP-auditing en Recht, zoals gebleken in eerdere themanummers, wordt ten aanzien van softwarebureaus en automatiseringsadviseurs nogmaals aangetoond.

Zoals reeds gesteld is niet een volledig themanummer tot stand gekomen; een tweetal vreemde eenden is in de bijt opgenomen. In de eerste plaats het onderwerp beveiliging, waarbij het verheugend is te constateren dat niet alleen EDP-auditors maar ook leveranciers zich hiermee bezighouden. Daarnaast is er sprake van een 'achterblijver'. Hiermee wordt geen negatief oordeel over het artikel van Van Kooij uitgesproken, maar wordt slechts gesignaleerd dat dit artikel behoort bij het themanummer van deze lente. Wellicht wordt deze 'vertraging' veroorzaakt door het gebruik van het verkeerde X.400-produkt, waarover u zich na lezing van het artikel zelf een oordeel kunt vormen.

Via de boekbesprekingen in EDP Auditorium komen we weer terug bij het vertrekpunt, namelijk de beheersing van de aspecten kosten en baten van informatietechnologie.

De redactie bedankt de heer P.P. Brouwers voor zijn coördinerende activiteiten ten aanzien van dit Compact-nummer. Wij verwachten dat u als lezer nuttige informatie kunt ontlenen aan de in deze Compact behandelde onderwerpen.

Drs. R.G.A. Fijneman RE RA

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

In de praktijk blijken nog weinig organisaties in staat te zijn de kosten en baten van informatietechnologie op objectieve en voor het management begrijpelijke wijze in kaart te brengen. Op pragmatische wijze wordt een aanpak beschreven op basis waarvan een integrale benadering van kosten en baten mogelijk is.

INLEIDING

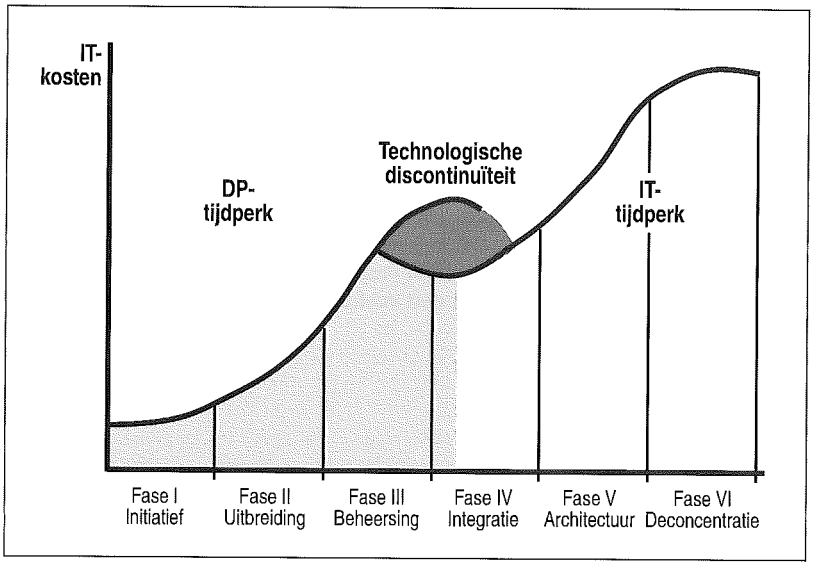
Het gebruik van informatietechnologie (of met een smallere betekenis automatisering) staat in zeer veel organisaties ter discussie. Hoge investeringen in zowel middelen als mensen, langdurige projecten en het achterblijven van de uiteindelijke resultaten bij de veelal zeer hoog gespannen verwachtingen zijn hiervan een belangrijke oorzaak. Er zijn derhalve grote twijfels over de effectiviteit en efficiëntie van de informatieverzorging.
Daarbij komt dat het management onvoldoende inzicht heeft in wat er gebeurt en de IT-manager ook onvoldoende in staat blijkt op objectieve wijze aan te geven hoe de zaken ervoor staan. Een eenduidig begrippenkader en objectief vergelijkingsmateriaal ontbreken, zodat een ieder oordeelt vanuit een subjectieve waarneming van de situatie en op basis daarvan met verbeteringsvoorstellen komt.
In een dergelijke situatie is er grote behoefte aan een objectieve, kwantitatieve en vergelijkende beoordeling van de huidige situatie. De I/T Assessment-methode [Koot89] is een samenhangend geheel van instrumenten waarmee alle aspecten van het gebruik van informatietechnologie kunnen worden gemeten en vergeleken. De resultaten van een I/T Assessment geven voor het management op inzichtelijke wijze weer waar de organisatie als geheel staat, hoe deze positie zich verhoudt ten opzichte van de concurrentie en hoe een en ander kan worden verbeterd.
In dit artikel worden zowel theorie als praktijk rondom de I/T Assessment toegelicht. We zullen ons om praktische redenen moeten beperken tot voorbeelden van analyses en resultaten. De methode biedt een veel breder spectrum aan mogelijkheden.

ACHTERGROND

Om te beginnen wordt de theoretische achtergrond van de I/T Assessment-methode beschreven.

Nolan-fasentheorie

De I/T Assessment is gebaseerd op de Nolan-fasentheorie. De grondslag van deze fasentheorie is het idee dat de ontwikkeling van het gebruik van informatietechnologie bij een organisatie een in fasen te onderscheiden leerproces is. Elke fase kent haar eigen specifieke vraagstukken op het gebied van informatiesystemen, gebruikers, technologie, automatiseringspersoneel en managementinstrumenten. Als gevolg hiervan is de sturing die moet worden gegeven per fase verschillend. Veel hangt dan immers af van de ervaringen die een specifieke organisatie met informatietechnologie heeft opgedaan. De fasentheorie [Nola92] beschrijft zes fasen, gesymboliseerd in twee S-curven. Hierbij geven de S-curven naast het leerproces ook de ontwikkeling van de automatiseringskosten weer (zie figuur 1).



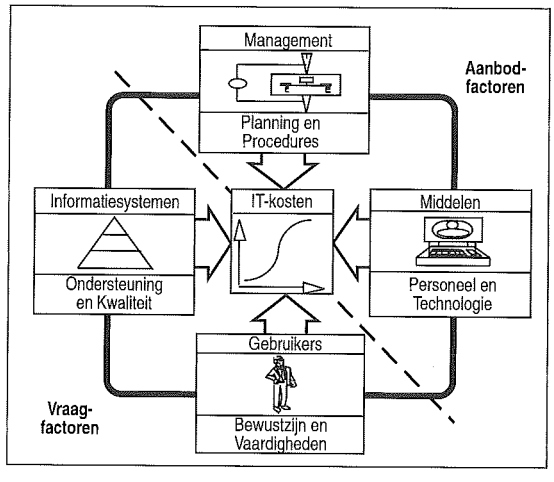
Figuur 1. Nolan-fasen van de ontwikkeling van informatietechnologie.

Aanvankelijk werd informatietechnologie ingezet voor het automatiseren van routinetaken, voornamelijk in de ondersteunende processen, zoals financiën en personeel. Daarmee werden grote efficiëntieslagen gemaakt. Dit was de tijd van de Data Processing. Deze fase was voornamelijk technologiegeoriënteerd. Inmiddels zijn deze taken bij de meeste organisaties met informatietechnologie ondersteund.
Vervolgens is het besef gegroeid dat met informatietechnologie meer mogelijk is dan het automatiseren van routinematige handelingen in ondersteunende processen. Informatietechnologie wordt ingezet om de primaire processen te verbeteren. Persoonlijke ondersteuning en externe ondersteuning van afnemers en leveranciers zijn de belangrijkste kenmerken van deze periode, het IT-tijdperk genaamd. De organisatiedoelstellingen geven expliciet richting aan de toepassing van informatietechnologie. Hiermee is informatietechnologie een strategisch wapen geworden. Uit onderzoek van Nolan, Norton & Co. (NNC) blijkt dat de meeste organisaties in Nederland zich in de eerste fasen van dit tijdperk bevinden. Benadrukt dient te worden dat hiermee geen kwalificatie van goed of slecht wordt gegeven. Deze plaatsbepaling geeft de collectieve leerervaring van de organisatie weer en dient als uitgangspunt voor verdere ontwikkeling te worden gehanteerd.
De meest vooruitstrevende organisaties zijn momenteel bezig het netwerktijdperk te betreden [Nola92]. Dit tijdperk wordt in de fasentheorie gerepresenteerd door een derde S-curve. Het wordt gekenmerkt door het fundamenteel herzien van bedrijfsprocessen. In het netwerktijdperk zullen organisaties opnieuw ontworpen zijn. De processen zullen op basis van de mogelijkheden van de informatietechnologie zijn ingericht. Informatietechnologie is zo niet meer een hulpmiddel maar een hefboom om veranderingen in een organisatie mogelijk te maken [Bate92].

De IT-groeiprocessen

Vier groeiprocessen karakteriseren het ontwikkelingsstadium waarin een organisatie zich op het gebied van toepassing van informatietechnologie bevindt. Het Nolan-fasenmodel beschrijft deze ontwikkelingsstadia [Nola92]. De I/T Assessment is gericht op het beoordelen van deze groeiprocessen, onderverdeeld in een vraag- en een aanbodzijde. De vraagzijde heeft betrekking op de ondersteuning van de organisatie door informatiesystemen en de kwaliteit van die systemen alsmede op de kennis en vaardigheden van de gebruikers om informatietechnologie toe te passen. De aanbodzijde heeft te maken met het IT-management (de IT-organisatie, de procedures en dergelijke), de vaardigheden van de automatiseringsdeskundigen en de infrastructuur. Uiteindelijk bepalen deze groeiprocessen hoeveel wordt uitgegeven aan informa-

Figuur 2. IT-groeiprocessen.



tietechnologie. De IT-kosten worden daarmee een afgeleide (zie figuur 2).

Kwantificeren en vergelijken

De I/T Assessment-methode kenmerkt zich door alle aspecten van de groeiprocessen op uniforme wijze te kwantificeren. Daardoor wordt het mogelijk organisaties met elkaar te vergelijken. Vooral vergelijking met organisaties in dezelfde branche biedt het management waardevolle inzichten in de status van de eigen IT-activiteiten. Hierdoor ontstaat management-informatie zoals deze ook voor andere aspecten van organisaties gangbaar is. Zo wordt de financiële situatie van een organisatie beoordeeld door vergelijking van bijvoorbeeld de 'solvabiliteit' met andere, soortgelijke organisaties. Door de jaren heen zijn voor dergelijke ratio's min of meer objectieve normen ontstaan, waarmee de financiële status van een organisatie wordt aangegeven. Voor de status van het gebruik van informatietechnologie zijn door een groot aantal I/T Assessment-onderzoeken ook dergelijke normen, benchmarks genaamd, ontwikkeld. Daar waar mogelijk en zinvol, zijn deze benchmarks branchespecifiek, dan wel Nolan-fase-specifiek. In dit laatste geval speelt een rol in welke fase de organisatie geacht wordt te zijn, gerelateerd aan de organisatiedoelstellingen en de positie van soortgelijke organisaties (bijvoorbeeld concurrenten). De vergelijking vindt plaats op basis van een verwachting ten aanzien van de ontwikkelingsfase. Voor alle benchmarks gelden branche-gemiddelden en bandbreedten die een 'gezonde' ontwikkeling aangeven.
Afwijkingen van de benchmarks hoeven niet zorgwekkend te zijn, maar kunnen bewuste beleidsmatige keuzes weerspiegelen. Door confrontatie met (de afwijkingen van) de benchmarks wordt het management wel met de neus op de feiten gedrukt. Dat noopt tot een gezonde (her)bezinning.

VISIE OP EFFECTIVITEIT EN EFFICIENTIE

Zoals uit de voorgaande paragraaf blijkt beziet de I/T Assessment-methode het gebruik van informatietechnologie vanuit management-perspectief. Aan het management wordt een objectief referentiekader gegeven waarmee de effectiviteit en de efficiëntie van het gebruik van informatietechnologie kunnen worden gemeten. De meetresultaten worden op twee niveaus geïnterpreteerd.

Enerzijds worden op basis van de meetresultaten uitspraken gedaan over de huidige situatie op zich. Volgens de fasentheorie is het niet zozeer van belang in welke fase een organisatie zich bevindt, maar wel dat de groeiprocessen in evenwicht zijn en dat effectief en efficiënt met de beschikbare middelen wordt omgegaan. Zeer hoogwaardige technologie met onervaren gebruikers leidt bijvoorbeeld nooit tot de gewenste resultaten.

Anderzijds wordt bezien of de toepassing van informatietechnologie aansluit bij de strategische richting van de organisatie. Er ontstaat derhalve een beeld van de effectiviteit en efficiëntie vanuit strategisch perspectief. Zo zien we niet zelden dat organisaties bezig zijn met het ontwikkelen van het vierde grootboekpakket, terwijl voor strategisch belangrijke bedrijfsprocessen nog nagenoeg geen ondersteuning aanwezig is.
Uit onderzoek blijkt dat het management de informatietechnologie veelal als een blok aan het been beschouwt [VSB92]. Dit wordt veelal ingegeven door het ontbreken van het bovengenoemde, objectieve referentiekader en van kennis van de mogelijkheden van informatietechnologie. Het door een I/T Assessment verkregen referentiekader stelt het management in staat gefundeerde IT-gerelateerde beslissingen te nemen.

DE PRAKTIJK

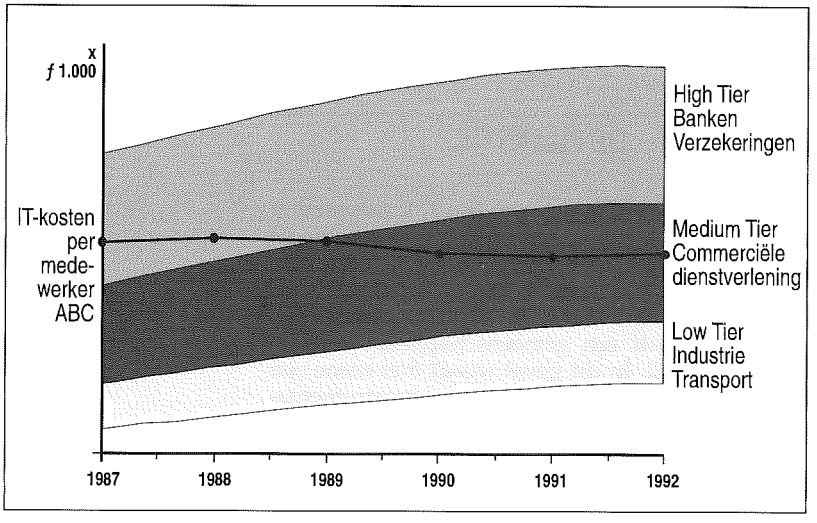
Eén van de aanleidingen voor een I/T Assessment vormen fusies en overnames, waarbij de IT-situatie van alle partijen wordt onderzocht. Doelstelling van de assessment is dan te komen tot een optimale IT-omgeving voor de nieuwe organisatie. Hierdoor wordt een gemeenschappelijk vertrekpunt gecreëerd. In dit geval wordt met name een beroep gedaan op het objectieve meetinstrumentarium.
De onduidelijkheid over kosten en opbrengsten van informatietechnologie is echter de meest voorkomende aanleiding. Zo ook bij een internationale verzekeringsmaatschappij, die we voor het gemak ABC-verzekeringen zullen noemen. ABC bevond zich in een situatie met teruglopende marges, toenemende concurrentie en een marktaandeel dat onder druk stond. Zoals bij zoveel bedrijven werd veel gedaan om de kosten te drukken. Ook de IT-manager werd hiermee (voor het eerst in zijn lange loopbaan) geconfronteerd. Zijn pogingen het management ervan te overtuigen dat op het IT-budget niet kon worden gekort, leidden niet tot het gewenste resultaat. De reden hiervoor was dat onvoldoende duidelijk was waar het geld aan werd uitgegeven, wat het opleverde en of de IT-kosten ten opzichte van de concurrentie niet erg hoog lagen. De marges stonden immers al onder druk. Om op deze managementvragen een antwoord te krijgen werd besloten een I/T Assessment te laten uitvoeren.

Samengevat dienden dus de volgende, veel voorkomende vragen te worden beantwoord:
- Geven we niet te veel uit?
- Levert het wel genoeg op?
- Geven we het aan de goede dingen uit?

Bij deze vraagstelling ligt de nadruk op het creëren van een objectief referentiekader. Hiervoor is uiteraard een objectief meetinstrumentarium een voorwaarde.
In de volgende subparagrafen zullen de vragen van de kosten/opbrengsten-problematiek vanuit onze praktijkervaring, aan de hand van het voorbeeld van ABC, worden uitgewerkt. De fusie/overname-vragen zijn veelal onderdeel van deze problematiek.

Geven we niet te veel uit?

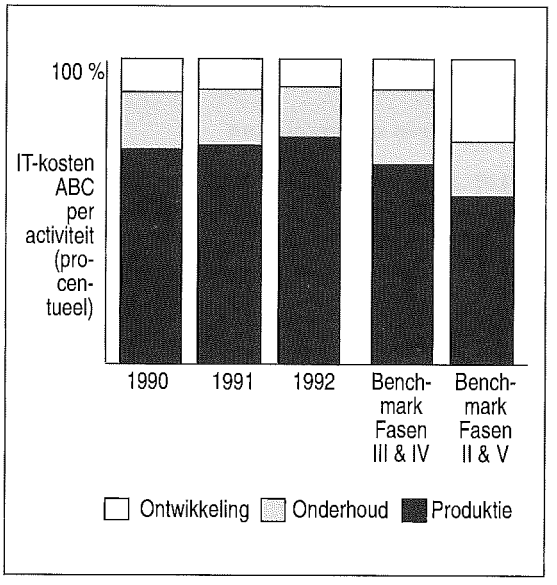
De eerste invalshoek voor deze vraag van het management van ABC is het absolute kostenniveau. Vergelijkbare cijfers worden verkregen door de totale IT-kosten uit te drukken in IT-kosten per medewerker, als percentage van de omzet of als percentage van de totale kosten. Door eenvoudigweg dit soort benchmarks te vergelijken is er over het kostenniveau een uitspraak te doen (cijfers van het CPB geven ook al een eerste indicatie).
In figuur 3 staat het voorbeeld van ABC, waarvan de IT-kosten per medewerker in de loop der tijd buiten de verwachte bandbreedte terecht kwamen.



Figuur 3. IT-kosten per medewerker bij ABC.

Vergelijking van deze financiële benchmarks alleen gaat echter nog steeds voorbij aan de wijze waarop de middelen worden aangewend. Beantwoording van deze vraag in absolute zin is dan ook van beperkte waarde. Mogelijke verklaringen voor de geconstateerde afwijkingen in figuur 3 zijn bijvoorbeeld:
- een onevenredige toename in het personeelsbestand;
- boven gemiddeld efficiënte aanwending van middelen;
- achterblijvende bestedingen door bijvoorbeeld geringe ontwikkeling;
- beleidsmatige overwegingen de kosten te beperken.

Veelal zal het echter een combinatie van verschillende factoren zijn.
Een verdere verdieping van het inzicht in de efficiëntie wordt verkregen door de opbouw naar een tweetal verschillende invalshoeken te analyseren. Enerzijds wordt onderzocht aan welke middelen geld wordt uitgegeven (technologie, personeel en overig). Anderzijds wordt onderzocht aan welke activiteiten de middelen worden besteed (ontwikkeling, onderhoud en produktie van applicaties). De onderlinge verhoudingen en vergelijking met de benchmarks leveren belangrijke inzichten op. Zo blijkt uit figuur 4 dat de produktiekosten van ABC relatief hoog waren en dat er met name weinig overbleef voor ontwikkeling van nieuwe systemen.



Figuur 4. IT-kosten van ABC onderverdeeld naar activiteiten.

Een gedegen beoordeling van het kostenniveau kan echter pas worden gegeven zodra ook de groeiprocessen zijn onderzocht, want daarmee wordt ook inzicht verschaft in de opbrengsten. Dit brengt ons meteen bij de volgende vraag.

Levert het wel genoeg op?

Feitelijk wordt hiermee gevraagd of de gemaakte IT-kosten ook gerechtvaardigd zijn. Zoals reeds eerder aangegeven zijn de groeiprocessen de drijvende kracht achter het totale kostenniveau. Een hoog kostenniveau met beperkt ontwikkelde groeiprocessen duidt immers veelal op een inefficiënt en/of ineffectief gebruik van de beschikbare middelen. De reeds beschreven balans tussen de groeiprocessen speelt hierbij een belangrijke rol.

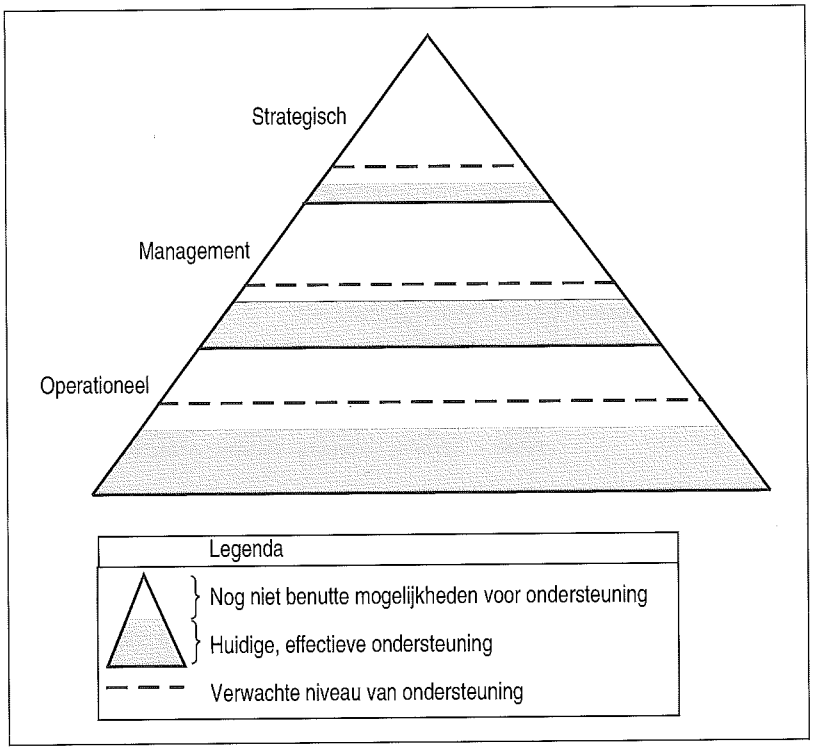
Vraagfactoren
De opbrengsten van de toepassing van informatietechnologie moeten uiteraard worden gezocht in de gebruikersorganisatie. De (kwantitatieve) graadmeter die hiervoor in de I/T Assessment wordt gebruikt, is de mate waarin gebruikers daadwerkelijk bij hun werkzaamheden door informatietechnologie worden ondersteund. De groeiprocessen aan de vraagzijde, te weten 'informatiesystemen' en 'gebruikers', zijn hiervoor gezamenlijk bepalend. De informatiesystemen leveren een potentieel aan ondersteuning dat afhankelijk is van de geboden functionaliteit en gebruikskwaliteit.
De vaardigheden van de gebruikers in de omgang met informatietechnologie bepalen de mate waarin dit potentieel ook benut wordt (de effectieve ondersteuning). Zo zullen geavanceerde, kwalitatief goede systemen niet renderen als de gebruikers onvoldoende zijn opgeleid om de systemen te gebruiken en vice versa. Hiermee is het belang aan-

getoond van de balans tussen informatiesystemen en gebruikers.
De gekwantificeerde mate van effectieve ondersteuning kan vervolgens worden vergeleken met benchmarks. Deze benchmarks zijn branche-specifiek.
Bij ABC (zie figuur 5) bleek dat de effectieve ondersteuning, net als de IT-kosten, beneden het niveau van de concurrentie lag. De resultaten van de financiële analyse, met name de lage uitgaven aan ontwikkeling, hadden hiervoor al een indicatie gegeven. Nu is ook van belang dat de ontwikkelinspanning niet zou leiden tot een significante uitbreiding van de ondersteuning. De kosten én baten waren dus lager dan verwacht; de verhouding was daardoor echter wel conform de verwachting.

Uit het onderzoek naar de gebruikersorganisatie bleek dat dit lage niveau van ondersteuning mede werd veroorzaakt door een laag bewustzijn van de mogelijkheden om de werkzaamheden met informatietechnologie te ondersteunen. Dit had namelijk tot gevolg dat er informatiesystemen werden ontwikkeld die slechts de zeer eenvoudige, routinematige activiteiten ondersteunden.
Een beperkt bewustzijn van de gebruikers kan dus verdergaande ondersteuning tegenhouden. De groeiprocessen aan de vraagzijde zijn daardoor weliswaar in balans (efficiënt), maar blijven achter bij de verwachtingen (niet effectief).
Zoals gezegd wordt de potentiële ondersteuning onder meer bepaald door de gebruikskwaliteit (functionele kwaliteit) van de systemen. Door de functionele kwaliteit te combineren met de technische kwaliteit (structuur, onderhoudbaarheid en gedrag in de produktie-omgeving), wordt inzicht verkregen in de acties die kunnen worden ondernomen om de effectieve ondersteuning te verbeteren. Zo kunnen systemen die van goede technische kwaliteit zijn, maar onvoldoende aan de gebruikerswensen voldoen, door functionele aanpassingen worden verbeterd. Als de technische kwaliteit echter ook veel te wensen overlaat, is vervanging het overwegen waard. Bij ABC (zie figuur 6) bleek dat voor een groot aantal systemen, met name in het primaire proces, functionele aanpassingen (onderhoud) nodig waren. Het hypothekensysteem zou een technische renovatie moeten ondergaan.

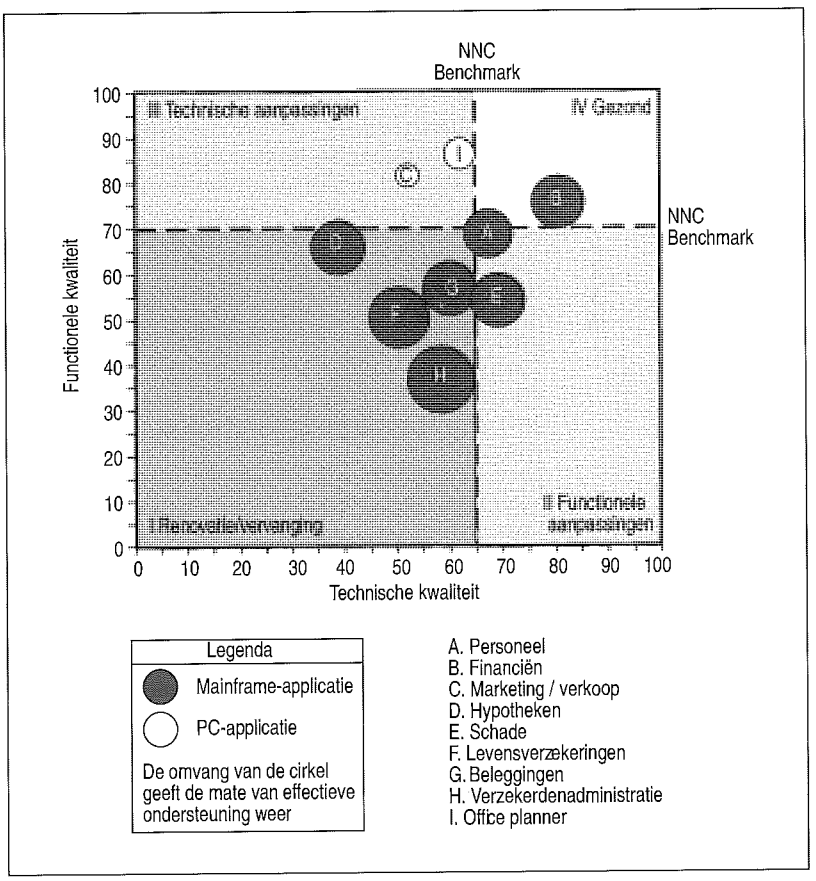
Aanbodfactoren
De opbrengsten aan de vraagzijde komen tot stand aan de aanbodzijde door aansturing en aanwending van de beschikbare mensen en middelen. De effectiviteit en efficiëntie worden daarbij bepaald door het 'IT-management' ofwel het beheersinstrumentarium en de kwaliteit en kwantiteit van de 'mensen en middelen'.

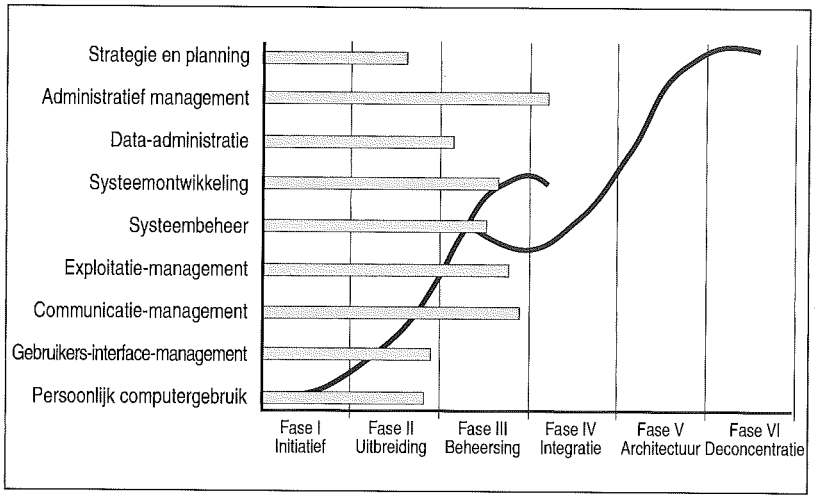
Ten aanzien van het IT-management wordt onderzocht welke beheersinstrumenten op welke wijze worden gehanteerd om de activiteiten van de IT-organisatie in goede banen te leiden. De analyse is erop gericht te achterhalen of het gehanteerde instrumentarium past bij de fase waarin de organisatie zich bevindt. Dit betekent dat een zeer uitgebreide en stringente toepassing van kwalitatief goede beheersinstrumenten, niet in alle situaties is gewenst. In het voorbeeld van ABC (zie figuur 7)



Figuur 5. Opbrengsten; effectieve ondersteuning bij ABC.

Figuur 6. Kwaliteit van informatiesystemen bij ABC.

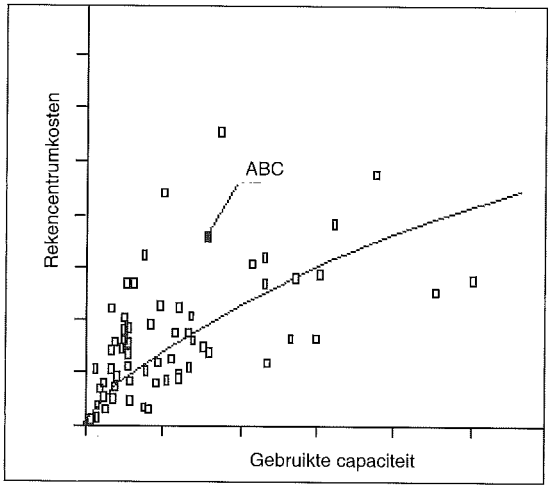




Figuur 7. IT-beheersinstrumentarium bij ABC.

was het beheersinstrumentarium op zich vrij ver ontwikkeld en geformaliseerd. Gezien de eerdere bevindingen bij de analyse van de ondersteuning, waaruit bleek dat deze achterbleef bij de verwachting en dus nog een aanzienlijke groei moet doormaken, gaf dit een onbalans te zien.
In een dergelijke situatie zouden de gebruikers moeten worden gestimuleerd tot het nemen van initiatieven, het experimenteren met hulpmiddelen en het nadenken over mogelijkheden voor het gebruik van informatietechnologie. Het formele, procedurele instrumentarium heeft daarop een negatieve invloed en werkt uitbreiding van de ondersteuning eerder tegen.
Aan de mens/middelen-kant wordt beoordeeld of deze in kwalitatief en kwantitatief opzicht in staat is de gewenste taken uit te voeren en of dit efficiënt gebeurt.
De IT-medewerkers worden daarom op een fors aantal vaardigheidsgebieden beoordeeld. In combinatie met hun ervaringsprofielen wordt bekeken of de huidige bezetting in staat mag worden geacht de haar toebedeelde taken de komende jaren uit te voeren. De ervaringsprofielen bieden bovendien inzicht in het loopbaan- en doorstroombeleid. Bij ABC bleek bijvoorbeeld dat de gemiddelde tijd die medewerkers van de ontwikkelafdeling in één functie zaten, slechts anderhalf jaar was. Dit had tot gevolg dat in een bepaalde functie gemiddeld weinig functie-specifieke ervaring voorhanden was.
De resultaten van de financiële analyse kunnen aanleiding zijn de produktiviteit van de ontwikkelaars aan een nadere analyse te onderwerpen. In financieel opzicht zullen ontwikkelinspanningen immers moeten leiden tot nieuwe systemen en daarmee tot onderhouds- en produktiekosten, tenzij slechts systemen worden vervangen. Vergelijking met de benchmarks gaf bij ABC geen afwijking te zien die vroeg om een nadere analyse van de produktiviteit van systeemontwikkeling.

De technische infrastructuur wordt enerzijds beoordeeld op de geschiktheid van de typen technologie voor het ondersteunen van de gebruikers. Hierbij kan eenvoudigweg al worden gedacht aan de mate van werkplekintegratie (één werkstation voor alle doeleinden), uniformiteit en beschikbaarheid. Anderzijds kunnen de telecommunicatie- en rekencentrumfaciliteiten op efficiëntie worden doorgelicht. Bij ABC leidde deze doorlichting tot de conclusie dat de kosten relatief hoog waren voor een rekencentrum met een dergelijk werkaanbod (zie figuur 8). Deze conclusie werd ook onderbouwd door de financiële analyse (zie figuur 4), waaruit bleek dat de produktiekosten relatief hoog waren.



Figuur 8. Rekencentrumkosten.

De capaciteit bleek te zijn afgestemd op de piekbelasting die aanzienlijk hoger lag dan de gemiddelde bezetting. Dit leidde tot een grote overcapaciteit buiten de piekuren. Door tijdens piekuren batchprocessen te voorkomen hoefde de capaciteit niet te worden uitgebreid en nam de servicegraad naar gebruikers toe.
Bovengenoemde analyses geven een goed inzicht in de efficiëntie en de mogelijkheden om deze te verbeteren. Wederom moet echter ook de balans tussen de groeiprocessen in ogenschouw worden genomen. Zo zullen zeer vaardige en ervaren IT-medewerkers weinig opleveren bij een gebrekkige, verouderde infrastructuur. Maar ook in de relatie met de groeiprocessen aan de vraagzijde kan sprake zijn van onbalans.
De groeiprocessen aan de aanbodzijde bleken bij ABC goed ontwikkeld. Mede door de gebrekkige IT-kennis en -ervaring bij de gebruikersorganisatie en de formele IT-beheersinstrumenten was de organisatie echter onvoldoende in staat voldoende effectieve ondersteuning te realiseren. De IT-organisatie kwam daardoor in een expertmatige, IT-inhoudelijke rol terecht. In deze situatie bleek het alleen mogelijk traditionele, functiegeoriënteerde systemen op te leveren, die onvoldoende aansloten bij de bedrijfsdoelstellingen. Hiermee komen we meteen bij de volgende vraag.

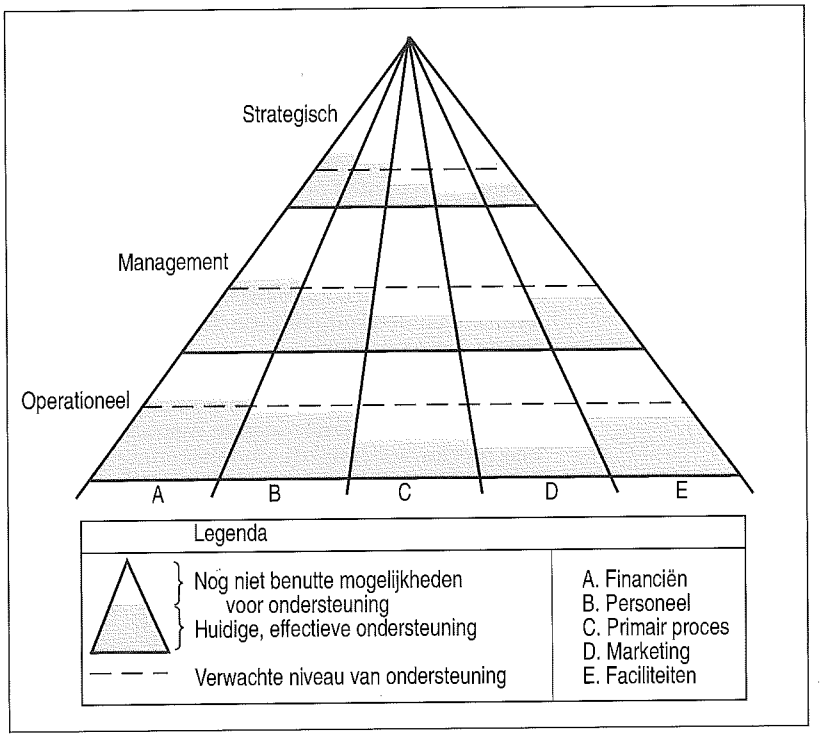
Geven we het aan de goede dingen uit?

Bij het beantwoorden van de twee eerste vragen lag de nadruk op de op specifieke aspecten gerich-

te analyses, de balans tussen de groeiprocessen en de relaties tussen de groeiprocessen en de financiën. Het referentiekader dat nodig is om hierop te kunnen antwoorden ligt met name in de relevante omgeving. Gesteld echter dat er niet te veel wordt uitgegeven en dat de kosten/baten-verhouding acceptabel is, dan is het nog steeds de vraag of het geld wel aan de goede dingen wordt uitgegeven. Het antwoord op deze vraag is afhankelijk van de strategische doelstellingen van de eigen organisatie.
De strategische doelstellingen worden vertaald naar de consequenties voor de toepassing van informatietechnologie. Zo heeft de doelstelling 'klantgeoriënteerd werken in plaats van produktgericht' als consequentie dat de 'front-office'-systemen dit werkproces moeten kunnen ondersteunen. De oude, produktgerichte systemen voldoen dan niet meer. De doelstelling 'iedere agent moet bij de klant meteen betrouwbare levertijden kunnen afgeven' impliceert dat die agent over online-voorraadgegevens moet kunnen beschikken. De toepassingen en infrastructuur zullen dus aan bepaalde voorwaarden moeten voldoen.
Dit betekent dat het geld aan de goede dingen wordt uitgegeven als de strategisch belangrijke gebieden met informatietechnologie worden ondersteund. Om hier inzicht in te krijgen kan bijvoorbeeld niet worden volstaan met 'de gemiddelde ondersteuning', maar is een analyse naar bedrijfsgebieden noodzakelijk, waarbij uiteraard ook wordt gekeken naar de mate van integratie van systemen tussen bedrijfsgebieden.
Een dergelijke analyse bij ABC gaf te zien dat de gemiddelde ondersteuning al aan de lage kant was. Bij nadere beschouwing van de als strategisch aangemerkte gebieden marketing en afhandelen van aanvragen (primair proces), bleek de ondersteuning hier ver beneden de verwachting te liggen (zie figuur 9). Met name de lage ondersteuning in het primaire proces is in de verzekeringsbranche verwonderlijk en zorgwekkend.

Een belangrijke oorzaak hiervan was het onvermogen om de kennis van het primaire proces te vertalen naar IT-oplossingen. Dit onvermogen kon worden verklaard uit het gebrek aan kennis en ervaring bij de gebruikers en de expertmatige houding van de IT-organisatie. Uit de vaardigheidsanalyse van de IT-medewerkers bleek dan ook dat IT-kennis goed ontwikkeld was, maar business-kennis achterbleef.

Zoals de strategische richting van de organisatie consequenties heeft voor de focus van ontwikkel- en onderhoudsinspanningen, zo kunnen er ook consequenties voor bijvoorbeeld de technische infrastructuur of de ontwikkelafdeling zijn. Als uit de doelstellingen blijkt dat de systemen 24 uur per dag met grote betrouwbaarheid beschikbaar moeten zijn (bijvoorbeeld in kerncentrales), dan heeft dit consequenties voor de infrastructuur en de beheersing daarvan. Als blijkt dat er zeer snel systemen moeten kunnen worden ontwikkeld, dan heeft dit consequenties voor de ontwikkelomgeving (hulpmiddelen) en voor de benodigde vaardigheden van de IT-medewerkers.



Figuur 9. Effectieve ondersteuning per werkgebied bij ABC.

De resultaten

Bij ABC leidde de I/T Assessment tot onderstaande resultaten.

Belangrijkste constateringen:

- Ten opzichte van de concurrentie en de eigen doelstellingen blijft ABC achter in de toepassing van informatietechnologie, met name in het primaire proces.

- De ondersteuning van de ondersteunende processen is zowel kwalitatief als kwantitatief goed.

- Bij het bestaande, ten opzichte van de concurrentie lage IT-kostenniveau wordt het merendeel van de middelen opgeslokt door de hoge produktiekosten en het onderhoud. Dit heeft tot gevolg dat er nagenoeg geen nieuwe systemen worden ontwikkeld.

- Door de communicatiekloof tussen gebruikers en IT-organisatie en de daardoor ontbrekende kennis, blijkt het bovendien niet mogelijk de ondersteuning in het primaire proces substantieel te verbeteren.

- De rekencentrumkosten zijn aan de hoge kant doordat de capaciteit is afgestemd op een piekbelasting.

- Met de huidige benadering zal ABC dus niet in staat zijn tot de nodige substantiële verbeteringen te komen.

Oplossingsrichtingen:

- Om in het primaire proces de ondersteuning snel substantieel te verhogen zal een (standaard) pakket moeten worden aangeschaft. Met een dergelijke oplossing zal de ondersteuning weliswaar niet op alle punten optimaal zijn, maar wel wordt de nodige ervaring opgedaan met toepassing van informatietechnologie in het primaire proces.

- Overbrug de communicatiekloof tussen de gebruikers en de IT-organisatie door opleiding, overleg en samenwerking.

- Breng de onderhoudsinspanning gericht op systemen van ondersteunende functies terug naar een niveau waarmee de ondersteuning wordt geconsolideerd. Hiermee wordt capaciteit vrijgemaakt ten behoeve van ondersteuning van het primaire proces.

- De piekbelasting kan eenvoudig worden teruggebracht door batch-verwerking buiten de piekuren te laten plaatsvinden en de prioriteitenstelling hierop aan te passen. Op termijn zal dit leiden tot betere benutting van de beschikbare capaciteit en daarmee tot kostenbesparing.

De waarde van een I/T Assessment is echter niet alleen gelegen in de eenmalig verkregen resultaten en de daaruit voortvloeiende verbeteringen, maar ook in het feit dat het onderzoek het bewustzijn van gebruikers en management prikkelt en er bewuster met informatietechnologie wordt omgegaan. De methoden en technieken worden veelal ook na het onderzoek door de organisatie gehanteerd en worden dan tot een 'tool of management'. Besturing vindt dan plaats op basis van informatie die volgens de I/T Assessment-methode wordt verzameld.

PRAGMATISCHE TOEPASSING I/T ASSESSMENT

Zoals al eerder aangegeven biedt de I/T Assessment-methode een breed spectrum aan mogelijkheden. De concrete aanpak is afhankelijk van aanleiding, vraagstelling en randvoorwaarden.

Klantgedreven aanpak

De vragen van de klant staan bij de uitvoering van I/T Assessment-onderzoeken centraal. Dit betekent dat het uitvoeren van een volledige I/T Assessment niet altijd noodzakelijk hoeft te zijn. Afhankelijk van de vragen wordt een samenhangende set instrumenten gebruikt om de specifieke vragen te beantwoorden.
Zo was het voor een produktie-organisatie cruciaal het bewustzijn en kennisniveau bij gebruikers en gebruikersmanagement te verhogen en tevens inzicht te krijgen in de wijze waarop de huidige ondersteuning plaatsvond. De IT-organisatie had namelijk de opdracht een strategisch IT-plan te maken en vond bij de gebruikersorganisatie onvoldoende basis hierop verder te bouwen. Hiervoor werd dan ook een project gedefinieerd waarin alleen de vraagzijde werd onderzocht. Intensieve participatie van gebruikers en management bracht een duidelijke verbetering teweeg in de wijze waarop met informatietechnologie werd omgegaan.
In een ander geval werd ervoor gekozen eerst een snelle 'scan' uit te voeren, gericht op de gebruikersorganisatie en de financiën. Op basis van deze resultaten werd vervolgens een toegesneden instrumentarium samengesteld om bepaalde gebieden verder uit te diepen.

Doorlooptijd en kosten

Een belangrijk aspect van doorlichtingen is veelal de doorlooptijd. Organisaties worden niet zelden opgezadeld met zeer langdurige trajecten, waardoor het momentum in de loop van het traject verloren gaat. Bovendien staan de ontwikkelingen binnen de organisatie niet stil, waardoor het beeld bij een te lange doorlooptijd al is achterhaald als het onderzoek wordt afgerond. Er wordt dan ook naar gestreefd I/T Assessments ook in grote organisaties zeer snel uit te voeren. Voor een organisatie met 20.000 werknemers en 700 IT-medewerkers is bijvoorbeeld binnen drie maanden een volledige I/T Assessment uitgevoerd.
Als vuistregel voor de kosten van een volledige I/T Assessment kan één procent van het totale IT-budget worden aangehouden. De werkelijke kosten zijn uiteraard afhankelijk van de gekozen diepgang van het uit te voeren onderzoek.

I/T Assessment en Business Process Redesign

Momenteel zijn veel organisaties hun werkprocessen fundamenteel aan het heroverwegen. Termen als 'Business Process Redesign' en 'Business Reengineering' zijn aan de orde van de dag [Bate92]. Dergelijke heroverwegingen worden mede ingegeven vanuit de (toegenomen) mogelijkheden van de toepassing van informatietechnologie.
Vaak resulteren deze herontwerpen in fundamentele veranderingen in de werkprocessen en bijbehorende rol van informatietechnologie [Bate91]. Dit brengt met zich mee dat een groeipad gedefinieerd moet worden waarmee het mogelijk wordt deze verandering beheerst tot stand te brengen. De I/T Assessment kan worden gebruikt om het vertrekpunt te bepalen op het gebied van de toepassing van informatietechnologie. Inzicht in de efficiëntie en effectiviteit zijn dan niet het primaire doel. Het doel is het creëren van een stabiele uitgangssituatie om het veranderingstraject op te baseren. Een stabiele situatie betekent dat de groeiprocessen in evenwicht zijn. Dit is meteen de eerste stap in het veranderingstraject op het gebied van informatietechnologie. Door de I/T Assessment wordt duidelijk welke acties moeten worden ondernomen om dit te realiseren. Op de korte termijn leveren deze acties verhoogde effectiviteit en efficiëntie op, op de langere termijn de stabiele uitgangssituatie voor het veranderingstraject.

TOT SLOT

Effectiviteit en efficiëntie van de informatievoorziening zijn van strategisch belang. Niet alleen vanwege de hoge kosten, tegenwoordig bij veel informatie-intensieve organisaties tussen de vijftien en vijfentwintig procent van de totale kosten, maar zeker ook vanuit het gegeven dat informatietechnologie een belangrijke factor is in het realiseren van de strategische doelstellingen van een organisatie [Koot92].
In de praktijk blijken nog weinig organisaties in staat te zijn de kosten en baten van toepassing van informatietechnologie op objectieve en voor het management begrijpelijke wijze in kaart te brengen. Het IT-budget biedt vaak maar een beperkt inzicht in de werkelijke totale IT-kosten (gemiddeld vijfendertig procent hoger dan het IT-budget), kostensoorten en kostenplaatsen. De baten worden veelal in nog veel vagere termen weergegeven. Het management ziet dus met name kosten(overschrijdingen) en heeft onvoldoende inzicht in de (strategische) baten.
De I/T Assessment is een objectieve, kwantitatieve en vergelijkende beoordeling van de effectiviteit en efficiëntie van de informatievoorziening. De resultaten van een I/T Assessment geven voor het management op inzichtelijke wijze weer waar de organisatie als geheel staat, hoe deze positie zich verhoudt ten opzichte van de concurrentie en hoe een en ander kan worden verbeterd. Bovendien wordt een handvat gecreëerd waarmee in de toekomst de vinger aan de pols kan worden gehouden.
Immers:
'If you can measure it, you can manage it ...'

LITERATUUR

[Bate91] M.V. Batelaan en P. van Doorn, *Informatietechnologie van Plateau tot Plateau: Een strategie voor de implementatie,* Harvard Holland Review, 91/27.

[Bate92] M.V. Batelaan en R.F.M. Vrolijk, *Proces herontwerp met informatietechnologie als hefboom,* Holland Management Review, 92/29.

[Koot89] W.J.D. Koot en J.T.M. van der Zee, *I/T Assessment, Een kwalitatieve en kwantitatieve evaluatie van de informatieverzorging vanuit een strategisch perspectief,* Informatie, jaargang 31, 89/12.

[Koot92] W.J.D. Koot, *Kosten en baten van informatietechnologie,* Bedrijfskundig vakblad B&ID, december 1992.

[Nola92] R.L. Nolan en W.J.D. Koot, *De actualisering van de Nolan-fasentheorie,* Holland Management Review, 92/31.

[VSB92] Vereniging voor Strategische Beleidsvorming en Nolan, Norton & Co., *Rapport van een onderzoeksprogramma 'Ondernemingsstrategie en Informatie Technologie'*, januari 1992.

Drs. B.T. Janssen
Studeerde Bestuurlijke Informatiekunde aan de Katholieke Universiteit Brabant. Hij is sinds 1988 werkzaam bij Nolan, Norton & Co., waar hij een groot aantal opdrachten heeft uitgevoerd op het gebied van het strategisch gebruik van informatietechnologie. Een belangrijk deel van zijn ervaring bestaat uit I/T Assessments.

Ing. W.J.D. Koot
Is als senior organisatie-adviseur werkzaam bij Nolan, Norton & Co. en auteur van vele artikelen op het gebied van informatie-management, strategisch gebruik van informatietechnologie en I/T Assessment.

Ir. E.J. Mutsaers
Studeerde Technische bedrijfskunde aan de Technische Universiteit Eindhoven en is sinds 1989 werkzaam als organisatie-adviseur bij Nolan, Norton & Co. Hij heeft een groot aantal opdrachten uitgevoerd op het gebied van het strategisch managen en toepassen van informatietechnologie.

Nolan, Norton & Co. is een wereldwijd adviesbureau inzake het management en de strategische toepassing van informatietechnologie, en maakt in Nederland deel uit van KPMG Klynveld Management Consultants.

Prioriteitenstelling met Decision

Dr. P.J. van Meel RI

Gezien de veelal schaarse middelen wordt het management regelmatig geconfronteerd met het bepalen van prioriteiten bij het nemen van besluiten. Veelal hebben hierbij subjectieve overwegingen de overhand.
Door Van Meel wordt een hulpmiddel geïntroduceerd dat ondersteuning biedt bij het rationaliseren van het besluitvormingsproces.

INLEIDING

Het stellen van prioriteiten is een universeel probleem, zowel bij toepassing van informatietechnologie als daarbuiten. Iedere organisatie wordt ermee geconfronteerd. Met name als de besluitvorming door meer dan één persoon moet worden verricht, is dit een onderwerp dat steeds opnieuw tot gecompliceerde besluitvormingssituaties leidt. Het gebeurt nogal eens dat hierdoor conflicten ontstaan die schadelijk zijn voor de organisatie. In veel gevallen leidt de gangbare manier waarop de prioriteiten worden gesteld tot een beleid dat niet optimaal is. Dit heeft weer ten gevolge dat de organisatie minder effectief en efficiënt functioneert dan mogelijk is. In dit artikel wordt op dit probleem ingegaan. Met een automatiseringsafdeling als voorbeeld wordt een methodiek geschetst die tevens vertaald is in een concreet werkend en effectief middel, 'Decision'. Dit maakt het mogelijk met subjectieve meningen rationeler om te gaan, vooral in een complexe omgeving.

Deze oplossing vindt haar oorsprong in de prioriteitenstelling bij toepassing van informatietechnologie, maar de methodiek is verder ontwikkeld tot een algemeen organisatorisch hulpmiddel. Door dit hulpmiddel bij het stellen van prioriteiten te gebruiken kan men de IT-organisatie zo goed mogelijk besturen. De EDP-auditor kan hetzelfde hulpmiddel gebruiken om de kwaliteit van de IT-organisatie te beoordelen en om ermee tot adviezen voor verbetering te komen.

Het artikel bestaat uit drie onderdelen:
1. de gewenste oplossing met als voorbeeld een automatiseringsomgeving;
2. de werking van de methodiek voor prioriteitenstelling Decision;
3. praktijkervaringen en de toegevoegde waarde.

DE GEWENSTE OPLOSSING

Aan de hand van een voorbeeld in de automatiseringsomgeving wordt de gewenste oplossing toegelicht.

Het voorbeeld

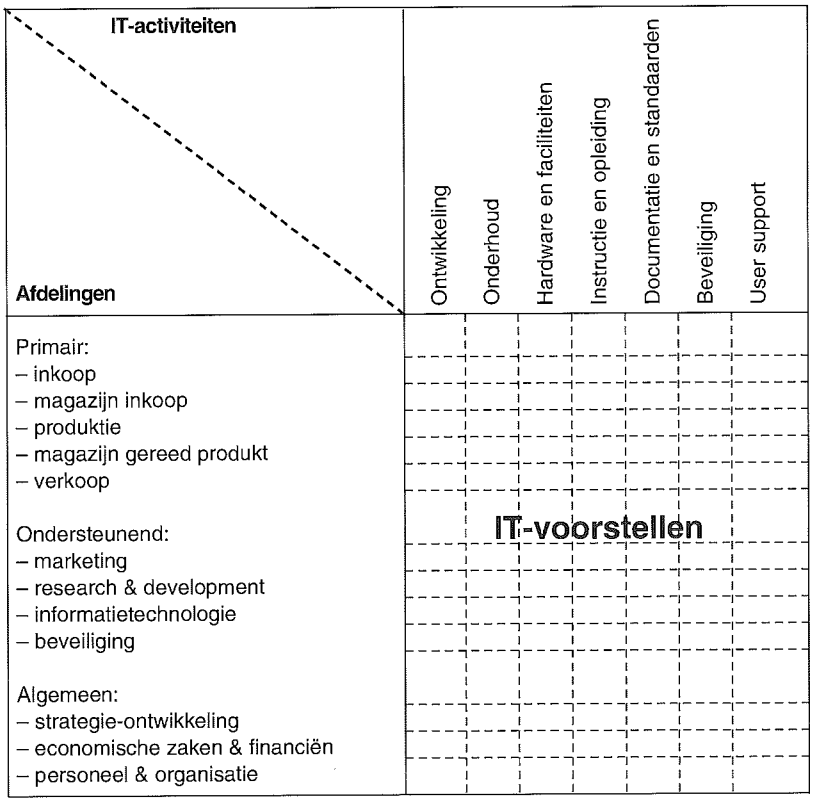
Als voorbeeld nemen we de produktie-organisatie Infotron, waarbinnen een automatiseringsafdeling de taak heeft voor de gehele organisatie het aspect informatietechnologie te behartigen. Bij Infotron wordt een aantal afdelingen onderscheiden. Deze zijn verdeeld in drie groepen: primaire produktieafdelingen, ondersteunende afdelingen en algemene afdelingen. In het geval van dit voorbeeld valt de automatiseringsafdeling onder de ondersteunende afdelingen en draagt de naam 'Informatie Technologie', afgekort als IT.
Bij Infotron werken vijfhonderd mensen en bij de afdeling IT dertig. Deze dertig mensen vervullen alle functies die bij Infotron op IT-gebied nodig zijn. Aan het hoofd van de afdeling staat een IT-manager. Hij heeft de verantwoording voor het operationeel houden van alle informatiesystemen binnen Infotron. Daarnaast moet hij voor het informatiebeleid en de automatiseringsplanning zorgen. Er is een stuurgroep IT waarin hij deelneemt. Andere leden zijn de managers van de andere afdelingen bij Infotron en de directie.

De IT-manager heeft vooral in twee opzichten te maken met het probleem van het stellen van prioriteiten: bij de dagelijkse besluitvorming en bij de beleidsvorming op de langere termijn. In beide opzichten is er een groot aantal wensen op IT-gebied. Dagelijks wordt hij bestookt met een groot aantal noodkreten en alarmeringen. Periodiek wordt hij ter verantwoording geroepen over de kosten die zijn afdeling maakt. In de stuurgroep wordt de voortgang van lopende projecten besproken (en wel vooral het gebrek aan voortgang). Daarnaast richt hij zich, als hij de tijd daarvoor kan vinden, op de inrichting van een informatieplan en ontdekt daarbij dat er meerdere witte vlekken en zwakke plekken binnen zijn aandachtsgebied voorkomen. Hij gaat met Decision werken om de besluitvorming te ondersteunen. Zijn EDP-auditor staat hem hierbij ter zijde.

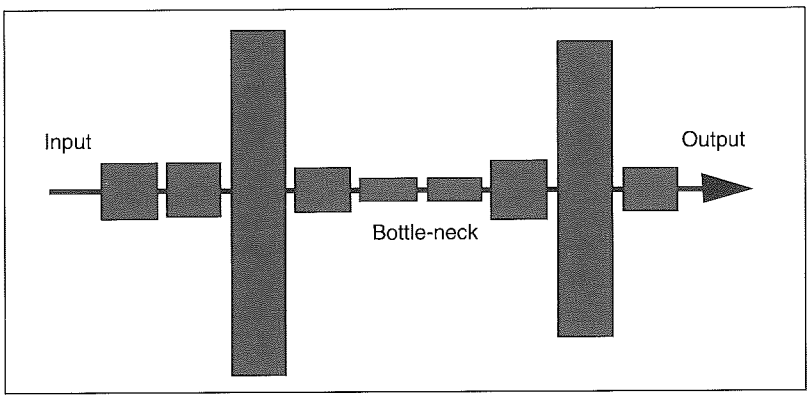
Om tot een ordening van dit alles te komen heeft de IT-manager een schema gemaakt (zie figuur 1). In figuur 1 staan verticaal de afdelingen van Infotron en horizontaal de IT-activiteiten van zijn afdeling. Alle wensen en voorstellen die op de korte termijn betrekking hebben vinden er een plaats. Ook de tekortkomingen die op de langere termijn betrekking hebben en de wensen op strategisch gebied staan erop.

Het evenwicht als het algemene uitgangspunt

Bij het toekennen van middelen aan taken en aan systemen binnen het IT-aandachtsveld is het van zeer groot belang dat er een evenwicht bewaakt wordt. Voordat de IT-manager in de stuurgroep



Figuur 1. Inventarisatie van IT-voorstellen bij Infotron.



Figuur 2. Een bottle-neck.

dit moeilijke onderwerp uitwerkt, behandelt hij een eenvoudige tekening (zie figuur 2).

Met deze tekening wordt een rivier bedoeld. Door deze rivier stroomt een hoeveelheid water bij de monding naar buiten. De hoeveelheid wordt bepaald door het gedeelte van de rivier dat de kleinste doorvoercapaciteit heeft. De capaciteiten van de andere stukken van de rivier hebben geen of nauwelijks invloed op de uitvoer. Alleen de bottleneck is van belang voor de totale prestatiecapaciteit van het riviersysteem. Als de beheerder van de rivier de capaciteit van een bottle-neck kan vergroten met tien procent, vergroot hij tegelijk de capaciteit van de hele rivier met tien procent. Zolang dit

de enige bottle-neck is, kan hij met een beperkte inspanning veel bereiken. Daarom zal hij zijn prioriteiten juist op die plaats richten.

Dit principe staat bij het werken met Decision centraal. De werkelijkheid van Infotron is niet zo eenvoudig als het zuiver lineaire en seriële verband van de rivier en dit is één van de kernproblemen die met Decision worden opgelost.

Het evenwicht tussen gelijk hebben en gelijk krijgen

De kwaliteit van een organisatie hangt grotendeels af van de bereidheid tot samenwerking tussen mensen. Deze bereidheid wordt minder als zij jaloers op elkaar zijn, als er een hevige competitie is en als zij elkaar vliegen afvangen. Natuurlijk zijn mensen nergens gelijk en een gezonde competitie is een prikkel die meestal voor de organisatie als geheel een goede zaak is. Men moet dus zoeken naar een optimum.

Gelijk krijgen
Voor de besluitvorming bij het stellen van prioriteiten is een motivering van ieder voorstel nodig om ervoor te zorgen dat een voorstel wordt aangenomen. Als men een stuk uit de taart van schaarste wil krijgen, zijn er echter meestal ook nog andere zaken nodig. Om *gelijk te krijgen* kan het heel dienstig zijn als men een persoonlijk krediet heeft opgebouwd. Dit verkrijgt men bijvoorbeeld door te wijzen op persoonlijke successen in het verleden. Ook kan het belangrijk zijn dat men een imago heeft met een bijbehorende uitstraling die alle weerstand en oppositie al bij voorbaat ontmoedigt. Gelijk krijgen behoeft niet altijd alleen gebaseerd te zijn op argumenten. Een goede argumentatie is nuttig, maar een flexibele en genuanceerde opstelling in een team kan wonderen doen. Een starre houding die niet open staat voor compromissen, is niet bevorderlijk als men gelijk wil krijgen. Het is ook vaak noodzakelijk om op een punt te geven om op een ander punt te kunnen nemen. Het is dikwijls het samenspel van deze vrij irrationele factoren dat bepaalt of een voorstel wordt aangenomen en of men gelijk krijgt. Als het via deze factoren niet wil lukken, kan de hiërarchische positie altijd nog de doorslag geven.

Een goede balans tussen 'gelijk krijgen' en 'gelijk hebben' is één van de doelstellingen die ten grondslag liggen aan Decision.

Gelijk hebben
In principe *heeft men gelijk* als men een voorstel doet dat een maximaal verschil oplevert tussen de toename van het nut en het beslag op schaarse middelen. Zo'n voorstel moet de hoogste prioriteit krijgen. Nut is in dit kader de effectiviteit gerelateerd aan het belang dat het desbetreffende onderwerp voor de organisatie heeft. In dat geval heeft men gelijk en zou men ook gelijk moeten krijgen. Dit is de meer rationele benadering.

Een goede balans tussen 'gelijk krijgen' en 'gelijk hebben' is één van de doelstellingen die ten grondslag liggen aan Decision. Een te groot verschil tussen beide is nadelig en leidt tot te grote wrijvingen. Decision lost de tegenstelling op tussen de mensen die vooral gelijk hebben en de anderen die vaak op andere gronden gelijk krijgen, door hen op een 'derde punt' te richten. Hiermee wordt een gemeenschappelijk doel bedoeld dat in de toekomst ligt. Door een zekere graad van abstractie en door de rationaliteit van Decision worden gevoeligheden tussen teamleden verminderd. Een gemeenschappelijk doel is een bindmiddel en vermindert fricties tussen mensen.

Specialisatie

Een andere factor die hierbij meespeelt is de mate van specialisatie. Een specialisme heeft zo zijn voor- en nadelen. Een nadeel ervan is dat bijvoorbeeld de hardware-specialist van de IT-afdeling wel eens meer gericht kan zijn op de specifieke ontwikkelingen op zijn eigen vakgebied dan op de zaken die voor Infotron als geheel gelden.
Hierdoor zal de specialist eerder zijn eigen belangen verdedigen en minder vanuit een 'helikoptergezichtspunt' het evenwicht van de gehele organisatie behartigen. Bij de te hanteren methode van prioriteitenstelling wordt zowel dit specialistische belang als het belang van de totale organisatie behartigd.

Het rationaliseren van de besluitvorming

De getalsverhoudingen die in de praktijk kunnen voorkomen, worden het beste verduidelijkt aan de hand van het voorbeeld. De IT-manager bij Infotron heeft vastgesteld dat er sprake is van circa vijfhonderd voorstellen op automatiseringsgebied per jaar, variërend van specialistische datacommunicatie-apparatuur tot datakluizen en meubilair, van bouwkundige voorzieningen tot een nieuw tekstverwerkingssysteem en van onderhoud aan een programma tot een aangepast informatieplan.

Deze voorstellen worden periodiek behandeld in de stuurgroep IT-investeringen die bestaat uit twaalf personen. Zonder een goede methodiek kunnen nu alle ingrediënten voor een suboptimale besluitvorming aanwezig zijn. Ieder voorstel wordt immers goed gemotiveerd en door de indiener verdedigd en hij (of zij) zal het belang of de noodzaak ervan aantonen. Andere leden van de stuurgroep hebben te weinig kennis van zaken om ieder specifiek voorstel goed te kunnen beoordelen of zij hebben meer oog en begrip voor andere noden. Het machtsspel dat hieruit volgt zal gespeeld worden en een rationele besluitvorming zonder compromissen is niet mogelijk, met alle nadelige gevolgen van dien.

Daar komt bij dat de algemene directie het globale belang wel inziet en vaak wel kan beoordelen of een voorstel past in het beleid van Infotron. Zij heeft echter vaak geen weerwoord op technische argumenten. Ook de gebruikers hebben dit weerwoord niet, maar zij zullen de nadruk leggen op de gevolgen voor de gebruikersorganisatie, iets waar de IT-mensen weer minder of geen inzicht in hebben. De IT-mensen staan vaak (en stonden vooral in het verleden) met hun technische en specialistische argumenten het sterkst.

Eisen aan de methodiek

De eisen die de IT-manager aan de te gebruiken methodiek en het daarbij gebruikte systeem stelt zijn de volgende:
- zij moeten vooral de besluitvorming ondersteunen die te maken heeft met de planning (het wat, wie en wanneer) en niet met inhoudelijke aspecten (het hoe);
- zij moeten een concreet hulpmiddel zijn en niet alleen een theorie;
- zij moeten een minimale drempel vormen voor de deelnemers en niet met moeilijke nieuwe begrippen komen;
- eenvoud en toegankelijkheid gaat boven complexiteit en verfijning;
- het hulpmiddel moet 'fool-proof' zijn.

DE WERKING VAN DECISION

In organisaties van uiteenlopende aard is met het systeem voor de ondersteuning van de prioriteitenstelling Decision gewerkt. Zoals dat in deze tijd behoort is deze methodiek in de vorm van een computertoepassing gegoten. Aan de huidige produktieversie zijn uitgebreide praktijktests voorafgegaan. De opmerkingen van de gebruikers en de opgedane ervaringen zijn verwerkt in het systeem. Bij de verdere beschrijving gaan we ervan uit dat de IT-manager de coördinator is bij het gebruik van Decision. Hij coördineert hierbij de volgende vier stappen: definitie, beoordeling, consolidatie en iteratie.

1. De definitiefase

Aan het begin moet de IT-manager de volgende zaken definiëren:

- Wat is het onderwerp van beschouwing? Hij kiest voor het IT-aspect binnen het gehele bedrijf Infotron, maar hij zou ook het bedrijf als geheel hebben kunnen kiezen.

- Wat zijn de te onderscheiden functies binnen Infotron? Hij gebruikt hiertoe een analysemethode die gebaseerd is op de procesbenadering.

- Wat is het beslissings- of beoordelingsprobleem? De wijze waarop de investeringen in zijn IT-sector moeten worden gedaan, is van strategisch belang. Daarom kiest hij voor dit onderwerp. Hij richt zich hierbij zowel op de korte termijn als op de langere termijn.

- Wat is de bijbehorende schaarstefactor? Hij kiest voor de beschikbare geldmiddelen, maar bij een andere probleemstelling zou hij bijvoorbeeld ook de ontwikkelingscapaciteit als schaarstefactor hebben kunnen kiezen.

- Welke veranderingsvoorstellen zijn er? Na inventarisatie vindt hij dat hij vierhonderd voorstellen voor de besluitvorming moet opnemen.

- Wie zijn de deelnemers aan de besluitvorming? Dit is bij dit voorbeeld de gehele IT-stuurgroep van Infotron.

Nadat de IT-manager het antwoord op al deze vragen heeft gegeven, kan hij het systeem met deze gegevens voeden. Hierbij komt hij nog meer problemen tegen. Zo moet hij voor een verdeling in afdelingen kiezen. Hij moet er daarbij rekening mee houden dat het latere evenwichtsbeeld zo significant mogelijk moet zijn. Als hij namelijk voor een stuk van de organisatie een te fijne of een te grove verdeling toepast, kan de analyse van het evenwichtsdiagram worden beperkt. De ervaring van de EDP-auditor helpt hem hierbij. Een ander probleem is dat ieder voorstel 'één op één' aan een taak binnen een afdeling moet zijn gekoppeld. Voor dit probleem zijn binnen Decision meerdere oplossingen voorhanden. Als al deze stappen gezet zijn, kan hij aan de volgende fase beginnen.

2. De beoordelingsfase

De IT-manager maakt per deelnemer formulieren, waarop laatstgenoemde zijn oordeel naar enkele gezichtspunten vastlegt. Zo geeft de deelnemer aan hoe belangrijk hij het IT-aspect en de automatiseringsinfrastructuur voor iedere afdeling vindt (BIF) [Bede85]. Hij drukt zich uit in een schaal van 0 tot 10 en richt zich daarbij naar zogenaamde 'normzinnen' (zie figuur 3 voor een kort voorbeeld). Dit zijn formuleringen per rapportcijfer die aangeven welke betekenis bij iedere waarde hoort.

BIF	=	Belangrijkheid van de Informatietechnologie voor de betrokken Functie/afdeling
10	=	Absoluut noodzakelijk.
7	=	Van groot belang voor het operationeel ondersteunen van de functie/afdeling.
4	=	Ondersteunend, maar het bereiken van de strategische doelstellingen hangt er niet van af.
1	=	Weinig of geen bijdrage tot het bereiken van de strategische doelstellingen.

Figuur 3. Een voorbeeld van een set normzinnen.

Iedere deelnemer geeft in een 'deskundigheidsindex' per afdeling ook op in welke mate hij zich deskundig acht en op de hoogte is van de achtergronden om uitspraken te kunnen doen.

Daarnaast geeft hij aan hoe belangrijk hij de verschillende afdelingen binnen zijn bedrijf vindt.
Van ieder voorstel, wens of investeringsobject geeft de deelnemer aan hoe effectief de desbetreffende taak op dit moment wordt uitgeoefend (dit is in figuur 4 aangeduid met ETF). Daarnaast geeft hij aan hoe effectief dit aspect zal zijn na honorering van de wens of na realisatie van het voorstel (ETF-plus). Hij geeft ook aan hoe belangrijk die taak is voor de functie waar die taak onder valt (BTF). Hierbij drukt hij zich eveneens uit in rapportcijfers en geeft daarbij zijn totaaloordeel of -impressie van ieder aspect. Voor ieder beoordelingspunt zorgt een set normzinnen voor ondersteuning. Als hij ergens geen mening over heeft kan hij dat punt vrijelijk overslaan.

Een fictief voorbeeld van deze beoordelingen staat in figuur 4. De kolommen ETF, ETF-plus en BTF geven de zojuist genoemde beoordelingscriteria van effectiviteit en belangrijkheid van voorstellen weer.

Deelnemer:	Datum:		Tijd:	
INFOTRON Omschrijving	ETF	ETF-plus	BTF	Kosten
Inkoop				1.284
1 Datacommunicatie-apparatuur	5	7	5	1.200
2 Meubilair operating	5	6	4	34
3 Tekstverwerkingsapparatuur	4	7	6	25
4 DECISION	2	8	8	25
5 ...				...
Magazijn inkoop				125
6 Aanleg kabelgoten	5	5,5	5	13
7 Instructiehandboek voorraad	5	7	8	32
8 Barcode-lezers	4	7	9	24
9 Aansluiting op het netwerk	4	4,3	4	56
10 ...				...
Produktie				427
11 IR-registratiepunten	4	6	5	5
12 Card key sloten (3x)	4	7	7	27
13 Datakluizen	3	5	4	35
.. ...				...

Figuur 4. Een ingevuld beoordelingsformulier.

Dit zijn tot dusver beoordelingen op het niveau van afdelingen en voorstellen. Op het niveau van de gehele organisatie worden ook beoordelingen van de deelnemers gevraagd. Deze hebben onder andere betrekking op de mening van iedere deelnemer over de doelstelling van Infotron.

Bij de kwantiteiten van dit voorbeeld geeft iedere deelnemer circa duizend beoordelingen. De IT-manager ervaart dat iedere deelnemer toch maar betrekkelijk weinig tijd nodig heeft. De cijfertoekenning komt immers niet in de plaats van de oordeelsvorming maar is er de neerslag van. Daarnaast blijkt het dat de methode snel went, omdat het bijna een natuurlijk proces is om je in rapportcijfers uit te drukken.

Van iedere deelnemer maakt hij een invoerverslag. Tegelijk maakt hij ook voor iedere deelnemer individuele uitvoerverslagen. Deze analyseert hij samen met zijn EDP-auditor. Waar de EDP-auditor minder logische zaken constateert wijst de IT-manager de deelnemer daarop. De deelnemers stellen hun beoordelingen bij totdat zij zich daar geheel in kunnen vinden. Op basis hiervan worden voor iedere deelnemer zijn persoonlijke prioriteitenlijst en een persoonlijk evenwichtsdiagram vervaardigd en aan hem voorgelegd (de verklaring hiervan volgt later bij figuur 8). In figuur 5 is een voorbeeld van de prioriteitenlijst getoond.

Deelnemer:	Datum:	Tijd:	
INFOTRON persoonlijke proioriteitenlijst			
Omschrijving	Score	Beslag	Cumul.
Meubilair operating	84	34	34
Aanleg kabelgoten	79	13	47
DECISION	77	25	72
Instructiehandboek voorraad	65	32	104
Card key sloten (3x)	45	27	131
Datakluizen	42	35	166
Bestedingslimiet	180		
Barcode lezers	32	24	190
IR-registratiepunten	31	5	195
Datacommunicatie-apparatuur	29	1.200	1.395
Tekstverwerkingsapparatuur	28	25	1.420
Aansluiting op het netwerk	26	56	1.476
...			

Figuur 5. Een persoonlijke prioriteitenlijst.

In dit overzicht staat in de kolom 'Score' de waarde die het desbetreffende voorstel heeft op basis van de ingegeven beoordelingen. De kolom 'Beslag' geeft het beslag op schaarse middelen van ieder voorstel weer. In de kolom 'Cumul.' worden deze bedragen gecumuleerd.

3. De consolidatiefase

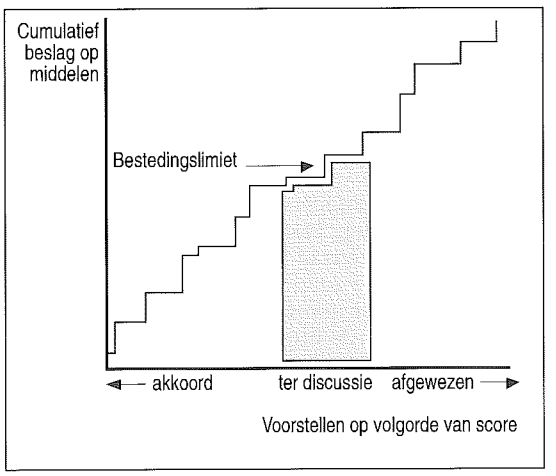
Nadat alle deelnemers het eens zijn met de uitvoer die op hun eigen beoordelingen is gebaseerd, voegt de IT-manager de beoordelingen van alle deelnemers samen. Er zijn controle- en correctieprocedures in Decision opgenomen die ervoor zorgen dat dit verantwoord gebeurt.
Nadat de gegevens op een vergelijkbare leest zijn geschoeid, kan hij de resultaten van de groep afdrukken. Dit is onder andere een geconsolideerde prioriteitenlijst. Op deze lijst is ook de bestedingslimiet aangegeven, zodat iedereen kan zien welke zaken in principe kunnen worden uitgevoerd en welke wensen men niet kan honoreren.

Figuur 6 geeft een verkort voorbeeld van de geconsolideerde prioriteitenlijst met fictieve getallen.
Dit overzicht omvat verticaal alle vierhonderd voorstellen en horizontaal staan alle twaalf deelne-

Omschrijving	Score van groep	Beslag	Cumul. beslag	Consensus indicator	Deelnemer A	B	C	D
Meubilair operating	75	34	34	2,6	100	10	90	100
DECISION	72,5	25	59	40	70	75	75	70
Aanleg kabelgoten	66,2	13	72	24,4	70	65	60	70
Instructiehandboek voorraad	65	32	104	20	60	70	60	70
Datakluizen	65	35	139	19	59	71	60	70
Barcode-lezers	53,7	24	163	24,4	50	50	60	55
Bestedingslimiet		180						
Datacommunicatie-apparatuur	45	1.200	1.363	3,4	35	95	20	30
Card key sloten (3x)	...	...	...	...	...	...	...	...
IR-registratiepunten								
Tekstverwerkingsapparatuur								
Aansluiting op het netwerk								
...								

Figuur 6. De geconsolideerde prioriteitenlijst.

mers, namelijk de twaalf leden van de IT-stuurgroep, naast elkaar (in figuur 6 vier deelnemers, te weten A, B, C en D). Dit is een onoverzichtelijk groot overzicht en daarom is de 'consensus-indicator' een effectief hulpmiddel. Deze 'consensus-indicator' is een getal per voorstel dat aangeeft in welke mate alle deelnemers een gelijkluidende mening hebben over een voorstel. Als deze indicator een lage waarde heeft is er een geringe overeenstemming over het voorstel in kwestie. Door middel van de 'consensus-indicator' kan de discussie van de IT-stuurgroep gericht worden op de voorstellen die onder een bepaalde waarde van deze indicator komen. Voor die voorstellen is er namelijk binnen de stuurgroep een geringe overeenstemming en dus ligt het voor de hand eerst daarover te praten.

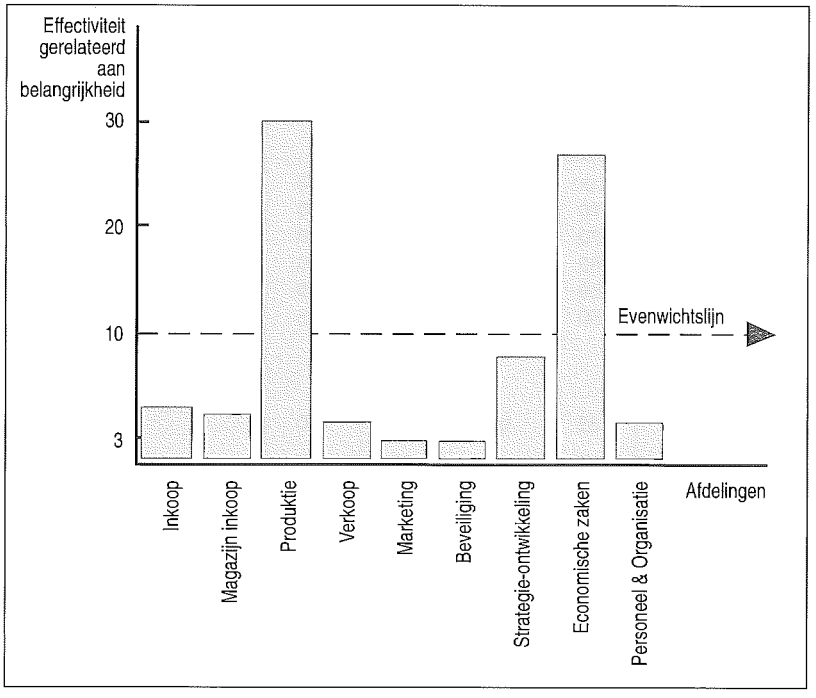


Figuur 7. De prioriteitenlijst in beeld.

De prioriteitenlijst wordt ook in een grafiek visueel gemaakt (zie figuur 7). Het beslag op schaarse middelen van de voorstellen wordt hier in een grafiek uitgezet. De lijn geeft het cumulatieve verloop aan van dit beslag op schaarse middelen. Deze lijn heeft een snijpunt met de bestedingslimiet van de schaarstefactor. Voorbij dat snijpunt moeten de voorstellen in principe worden afgewezen. Zo wordt duidelijk dat de stuurgroep zich vooral zou kunnen concentreren op het gearceerde gebied. De voorstellen die links van dat gebied liggen hebben immers een hoge score. Daarom hoeven deze niet meer intensief te worden besproken en hoeven de indieners deze niet meer met veel argumenten aan te bevelen. Lange discussies over zaken die duidelijk moeten worden afgekeurd (rechts van het gearceerde gebied), zullen daardoor nu ook eerder kunnen worden vermeden.

Hiervóór is steeds met opzet gesproken over het 'beslag op schaarse middelen' en niet over de 'kosten' van een voorstel. De schaarstefactor is bij Decision namelijk niet gedefinieerd. Daardoor kan men bij de definitiefase vrijelijk voor iedere soort schaarstefactor kiezen. Te denken valt aan investeringsruimte, bezuinigingsbedrag, meters kantoorruimte, hectares grond, machine-uren, ontwikkelcapaciteit.

Eén van de belangrijkste produkten van Decision is het evenwichtsdiagram (zie figuur 8). Dit evenwichtsdiagram is door zijn opbouw vergelijkbaar met de rivier in figuur 2. Men kan in figuur 2 een bovenaanzicht van een rivier zien. Figuur 8 kan men zich vervolgens voorstellen als een zij-aanzicht van dezelfde rivier.
Dit diagram is het hulpmiddel van Decision voor de algemene strategiebepaling. Het ondersteunt de besluitvorming die betrekking heeft op de langere termijn. Het prioriteitenoverzicht sluit hierop geheel aan en geeft aan welke beslissingen voor de korte termijn kunnen worden genomen. Op basis van het evenwichtsdiagram kan de IT-manager zwakke plaatsen bij Infotron (ten aanzien van het



Figuur 8. Het evenwichtsdiagram.

IT-aspect) duidelijk onderkennen en daarop plannen baseren of initiëren.
In dit diagram staan deafdelingen van Infotron op de horizontale as. Op de verticale as staat de mate waarin deze afdelingen kunnen presteren en ertoe bijdragen dat het IT-aspect bij Infotron aan de doelstelling beantwoordt. Dit wordt gedefinieerd als effectiviteit. Er is een verschil in de mate waarin iedere afdeling van belang is voor het bereiken van het doel door het gehele bedrijf. Daarom wordt op de verticale as de prestatiecapaciteit in een relatief getal uitgedrukt: de verhouding tussen effectiviteit en belangrijkheid.

Door het evenwichtsdiagram op deze manier in te richten geeft de hoogte van de kolommen in het diagram aan in hoeverre een afdeling een zwakke plek vormt. De laagste kolommen (in het diagram de afdelingen Marketing en Beveiliging) vormen voor Infotron bottle-necks. De mate waarin Infotron haar doel bereikt wordt voornamelijk door deze afdelingen bepaald. In het diagram ligt dit op het niveau met de waarde 3. Deze afdelingen zijn het meest beperkend voor het gehele bedrijf en daarom moeten daar de hoogste prioriteiten worden gelegd.

Het bedrijf functioneert (wat betreft het IT-aspect) door deze bottle-necks op een lager niveau dan mogelijk zou zijn. Het gemiddelde van alle kolommen is de evenwichtslijn, en deze ligt op een niveau 10. Als alle middelen optimaal aan de afdelingen zouden zijn toebedeeld, zouden alle kolommen op het niveau van deze evenwichtslijn uitkomen. In theorie zou de organisatie bij dit voorbeeld op het niveau 10 kunnen functioneren.

Doordat het diagram de verhoudingen visueel maakt kan de IT-manager nu doelgerichte beleidsmaatregelen afleiden. Hij kan aan de afdelingen Marketing en Beveiliging vragen welke extra voorstellen zij kunnen bedenken voor verbetering van de effectiviteit. Ook kan hij nagaan of er misschien IT-middelen van de afdelingen Produktie en Economische zaken intensiever kunnen worden benut. Als deze benutting of bezetting niet kan worden gewijzigd, kan hij nagaan of IT-middelen uit die afdelingen misschien beter elders kunnen worden ingezet.

Het evenwichtsdiagram geeft aan welke beleidsmaatregelen getroffen kunnen gaan worden. Het geeft de richting voor nadere analyse aan. Dit heeft effect op wat langere termijn. De prioriteitenlijst geeft aan wat op korte termijn concreet kan gaan worden gedaan.
Het evenwichtsdiagram geeft ook een *kwaliteitsindicatie* aan. Als er immers een groot verschil is tussen de bottle-neck en de evenwichtslijn, wordt de IT-functie bij Infotron niet optimaal vervuld.

4. De iteratiefase

Door herhaald gebruik wordt het nuttig effect van Decision groter. De geconsolideerde uitvoer wordt in de stuurgroep besproken en ondersteunt de meningsvorming. De groep kan op basis hiervan de beoordelingen bijstellen en nieuwe aangepaste uitvoer opvragen. Zij kan de methode ook afwisselend toepassen op het totale organisatieniveau (ten aanzien van alle aspecten) en op een lager niveau (alleen het IT-aspect).

De directie van Infotron kan met Decision als maatstaf ook komen tot een gefundeerde budgettoekenning, waarbij het evenwicht over de gehele organisatie heen wordt bevorderd. Een budget is dan niets anders dan een aantal clusters van voorstellen en wensen.

Men kan ten slotte ook binnen een afdeling of op het niveau van de gehele organisatie aspectmatig tot prioriteitenstelling komen, door afwisselend voor een ander onderwerp van besluitvorming te kiezen (investeringen, ruimteverdeling, onderzoekscapaciteit, opleidingen).

De globale doelstelling

Het is mogelijk dat men kiest voor een strikt economische benadering. Het beslag op schaarse middelen van iedere wens of ieder projectvoorstel wordt dan bepaald door zowel het investeringsbedrag als de bijbehorende exploitatielasten te ramen. De vermeerdering van de effectiviteit wordt gerelateerd aan dit beslag op schaarse middelen, en de berekende score is een uitgangspunt voor de prioriteitenstelling.
Er zijn echter ook situaties waarbij men bijvoorbeeld de kwaliteit van de produkten, de servicegraad aan de klanten of een andere doelstelling van groot belang acht, en daarbij het beslag op schaarse middelen minder doorslaggevend wil laten zijn.

Daarom is het systeem Decision dubbel uitgevoerd

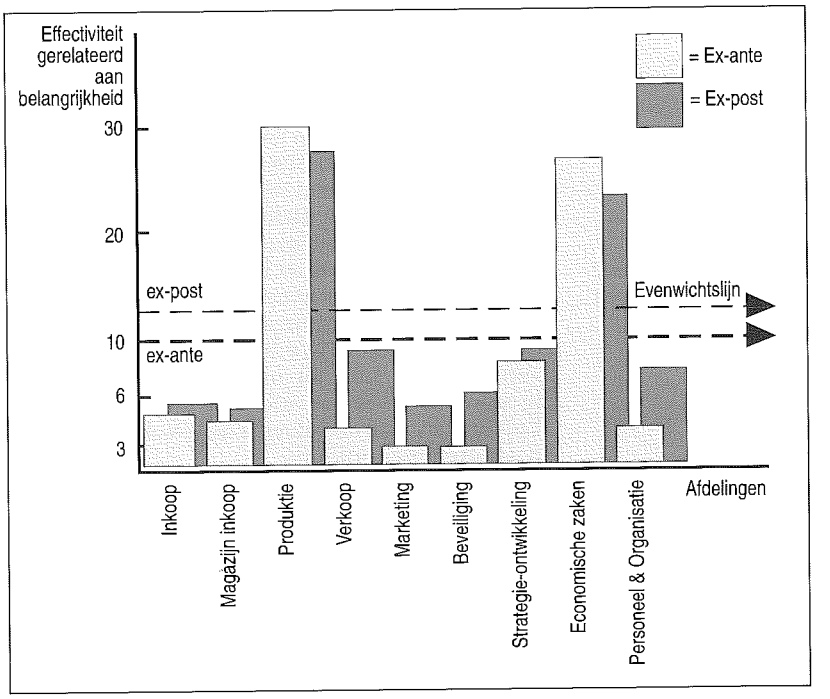
en zo kan men vanuit beide gezichtshoeken over de uitvoer beschikken. Men kan zodoende zien wat het verschil in de resultaten is tussen de beide invalshoeken. Men ziet zo wat het effect van een andere visie omtrent de 'globale doelstelling' is op de besluitvorming of de te ondernemen strategie.

De 'globale doelstelling' kan iedere deelnemer naar believen instellen door voor een mix tussen beide extreme invalshoeken te kiezen. Op deze wijze kan men ook een gevoeligheidsanalyse verrichten en zichtbaar maken wat de effecten van andere beleidsuitgangspunten zijn.

Het evenwicht ex-post en ex-ante

Het evenwichtsdiagram kan naar twee gezichtspunten worden bepaald. Het evenwichtsdiagram ex-ante geeft de situatie weer voordat er één voorstel is uitgevoerd. Het systeem beschikt echter over alle gegevens om ook een ex-postsituatie te kunnen bepalen. Daarbij gaat het van de hypothese uit dat de prioriteitenlijst conform de berekende scores zou worden gerealiseerd. In figuur 9 is dit weergegeven. Het evenwichtsdiagram van figuur 8 was het evenwichtsbeeld ex-ante. Dat beeld is in figuur 9 herhaald in de lichte kolommen. In de erachter staande donkere kolommen is weergegeven hoe het evenwicht ex-post eruit ziet. Dit levert een uitermate krachtige analysemogelijkheid op. We kunnen nu immers zien wat het eindresultaat zou zijn als alle beoogde voorstellen precies volgens de berekeningen van Decision zouden worden uitgevoerd. Het prestatieniveau van de IT-functie lag in de ex-antesituatie op het niveau van de bottle-neck (met als waarde 3) en bevindt zich in de ex-postsituatie op een niveau 6. Als de geproduceerde prioriteitenlijst precies wordt opgevolgd, zal het prestatieniveau dus verdubbelen. De prioriteitenlijst en het evenwichtsdiagram zijn namelijk volledig op elkaar afgestemd.
De evenwichtslijn ex-ante is lager dan de evenwichtslijn ex-post. Door de voorstellen uit te voeren worden namelijk middelen toegevoegd waarvan men een effectiviteitsverhoging verwacht.

Het is overigens ook mogelijk dat men gaat bezuinigen. Dan zal Decision bij voorkeur middelen onttrekken aan de hoogste kolommen. De evenwichtslijn, die het theoretisch optimale prestatieniveau weergeeft, zal dalen. Het werkelijke prestatieniveau ligt echter op het niveau van de bottle-neck. Dit niveau zal wellicht niet worden aangetast. Bij de bezuinigingsvoorstellen kunnen ook voorstellen zitten die een herverdeling van middelen of capaciteiten betreffen. Deze kunnen een verlaging van de hoogste kolommen tot gevolg hebben en een verhoging van de kolom van de bottle-neck. Het is goed mogelijk dat door op deze manier met bezuinigingsvoorstellen om te gaan per saldo de werkelijke prestatiecapaciteit niet wordt aangetast, maar zelfs wordt verhoogd!
Deze stijging kunnen we nu visueel maken. We kunnen nu zelfs kwantitatief in procenten benaderen wat het totaaleffect voor de effectiviteit van de gehele IT-functie is.



Figuur 9. Het evenwichtsdiagram ex-ante en ex-post.

PRAKTIJKERVARINGEN EN DE TOEGEVOEGDE WAARDE

De toegevoegde waarde van de methode valt te ontlenen aan een aantal praktijkervaringen.

Kwaliteit van de besluitvorming

Bij meerdere gelegenheden is een test in de praktijk uitgevoerd. Hierbij is de besluitvorming zoals die al eerder was gedaan door een management-team opnieuw verricht. De eerdere besluitenlijst is naast de uitkomsten van de testsituatie gelegd, en het team achtte de tweede lijst als de juiste. Beide lijsten bevatten dezelfde voorstellen. Een aantal voorstellen op de eerste lijst was akkoord verklaard en op de tweede lijst ook. Eveneens is een aantal voorstellen op de eerste lijst afgewezen en op de tweede lijst ook. Het aantal voorstellen dat in *beide* gevallen tot dezelfde beslissing leidde (akkoord of afgewezen), was circa 65 procent. Tussen beide lijstuitkomsten lag dus een verschil van circa 35 procent.

Genoemd verschil hield in dat ten minste 35 procent van alle eerder genomen beslissingen zou leiden tot een suboptimale situatie en dus in feite fout was. Dit verschil is aanzienlijk, maar dit is toch niet verwonderlijk. Als men zonder een ondersteunend systeem dezelfde genuanceerde afwegingen wil doen, moet men in staat zijn zeer veel gegevens en beoordelingscijfers onderling met elkaar in verband te brengen. Bij Infotron hebben twaalf deelnemers ieder circa duizend beoordelingscijfers gegeven. Door Decision werden dus twaalfduizend getallen met elkaar in verband gebracht om tot de

conclusies voor Infotron te komen. Met de gecombineerde kracht van een computer en de strakke logica van Decisionis dit mogelijk; een mens alleen zonder deze hulpmiddelen kan dit niet.
Een ander gevolg van Decision is dat men zich concentreert op wat relevant is. Door het systeem immers wordt ook een visueel beeld gegeven van de werkelijke prioriteitenlijst (zie figuur 7). Hierdoor concentreert men zich in de discussies op datgene wat haalbaar en relevant is. De efficiëntie van het vergaderen wordt daardoor sterk bevorderd. Het besluitvormingsproces, binnen én buiten de vergaderruimte, wordt tevens minder duur en vermoeiend en leidt tot minder irritaties. Het gehele proces levert een aanzienlijke tijdsbesparing op. Ook ervoeren de deelnemers de te volgen procedure als prettig en efficiënt.

Het evenwicht in de praktijk

Bij het gebruik van Decision in de praktijk (bij een andere organisatie dan in ons voorbeeld van Infotron) zijn frappante constateringen gedaan. Zo bleek in enkele situaties dat er een grote spreiding is in de gevonden waarden van het evenwichtsdiagram. Dit kan verkort worden weergegeven in tabel 1.

Primaire afdelingen	6
Ondersteunende afdelingen	16
Algemene afdelingen	18
Gemiddelde van de organisatie	12

Tabel 1.Spreiding waarden van het evenwichtsdiagram.

Alle functies in een organisatie zijn hierbij teruggebracht tot drie groepen van functies of afdelingen. De evenwichtslijn van de betrokken organisatie lag op een niveau 12. De primaire functies en primaire processen scoorden samen gemiddeld een niveau 6 en de ondersteunende en algemene afdelingen kwamen op een niveau 16 en 18 uit. Dit gebrek aan evenwicht werd door velen beschouwd als een bevestiging van hun eigen mening (!).

Het is de primaire afdelingen in deze organisatie jaar in jaar uit onvoldoende gelukt middelen toegekend te krijgen. Door een cumulatie gedurende jaren is hun prestatiecapaciteit ten opzichte van het belang van hun functie slechts eenderde geworden van die van de meest bevoorrechte andere afdelingen en functies.

De IT-manager en de EDP-auditor

Als definitie van EDP-auditing geeft een NIVRA-commissie:

'EDP-auditing is het door een onpartijdig deskundige kritisch beoordelen van en adviseren over de kwaliteit van de organisatie van de automatisering, de automatiseringsorganisaties en de te automatiseren c.q. geautomatiseerde informatiesystemen.'

Als aspecten van het begrip kwaliteit kan men kiezen voor betrouwbaarheid, doeltreffendheid en doelmatigheid.

De IT-afdeling heeft een taak die met deze definities veel gemeen heeft. In het hier geschetste voorbeeld van de IT-afdeling binnen Infotron is de IT-manager verantwoordelijk voor de kwaliteit van de automatiseringssystemen. Hij maakt deel uit van een stuurgroep die (bijvoorbeeld) beslissingen neemt over voorgestelde IT-investeringen. De problematiek die daarbij aan de orde is kunnen we als volgt formuleren:

'Het IT-management en de IT-stuurgroep moeten een beleid vormen en doen uitvoeren dat binnen het raamwerk van de mogelijkheden en middelen tot een maximale kwaliteit leidt van de organisatie van de automatisering, de automatiseringsorganisaties en de te automatiseren c.q. geautomatiseerde informatiesystemen.'

In de beschrijving die hiervóór van Decision is gegeven, blijkt dat deze methode op een belangrijk deel van deze opdracht van toepassing is. Uit die beschrijving van de methode blijkt ook dat vooral het evenwichtsdiagram en de daarbij behorende analysemogelijkheden voor de EDP-auditor een krachtig middel zijn om zijn taak van 'kritische beoordeling en advies' uit te oefenen.

Twee functies (de IT-manager en de EDP-auditor) kunnen dus een belangrijke ondersteuning bij hun werk vinden in Decision. De een kan gebruik maken van het werk en de resultaten van de ander. Met name in de eerste fase kan een samenwerking tussen beiden nuttig zijn.
Op basis van de uitvoer van Decision kunnen de EDP-auditor en/of de IT-manager komen tot expliciete adviezen. Zij kunnen door middel van het evenwichtsdiagram ex-ante en ex-post zelfs aangeven welke verandering in kwaliteit mag worden verwacht als hun adviezen worden opgevolgd.

Aantal deelnemers

In de meeste besluitvormingssituaties wordt de omvang van de groep deelnemers beperkt gehouden. De stuurgroep van twaalf personen bij Infotron heeft een gangbare omvang. De reden hiervan is dat de efficiëntie en de effectiviteit van het overleg bij een grotere omvang snel dalen. Een computer wordt echter helemaal niet gehinderd door aantallen.

Als de IT-manager een groot aantal gebruikers wil laten deelnemen, naast de stuurgroepleden, dan is daartegen geen bezwaar. Zij hebben misschien een minder brede visie, maar zij hebben vaak wel meer kennis van de concrete omstandigheden. Met deze minder brede visie kan rekening worden gehouden door met name de deskundigheidsindex te gebruiken. Het systeem is erop berekend met grote aantallen deelnemers om te gaan. Een groter aantal deelnemers kan de waarde van de uitvoer vermeerderen. Het neveneffect is dat er een grotere betrokkenheid van de mensen bij Infotron ontstaat zonder dat het nadeel van een onbeheerste inspraak behoeft op te treden.

De vaststelling van de functies en de proces-onderdelen

Bij de definitiefase dient de indeling in functies te worden vastgesteld waarmee vervolgens wordt gewerkt. Dit op zich kan al een onderwerp zijn van veel discussie. Ook hier is in de praktijk gebleken dat de kwaliteit van het eindprodukt afhangt van de inspanning die men zich voor deze schijnbaar eenvoudige taak getroost.

De motivering van de voorstellen

In een traditioneel besluitvormingsproces is de verbale toelichting in combinatie met de fenomenen die bij 'gelijk krijgen' spelen vaak voldoende. Als men Decision gebruikt, wordt het aspect 'gelijk hebben' bevorderd. Het overtuigen en bewerken van mensen in een groep wordt nu echter voor een deel vervangen door de schriftelijke motivering van het voorstel. We zien nu in de praktijk dat voorstellen zónder een schriftelijke motivering minder stemmen kunnen gaan scoren. Decision bewerkstelligt hierdoor dat de voorstellen van een betere en expliciete motivering worden voorzien.

De 'sponsor' en het systeembeheer

Zoals bij iedere IT-toepassing geldt ook voor Decision dat er ten minste twee zaken geregeld moeten zijn om tot goede resultaten te komen. Er is een systeembeheerder nodig om de applicatie te beheren, de procedures te doen volgen en de formulieren te beheren. Daarnaast is er ook een 'sponsor' nodig, zoals de IT-manager van Infotron. Hij beschikt over de positie, de overtuigingskracht, het overzicht en de kennis om de deelnemers te motiveren. Hij beschikt ook over het inzicht de uitvoer te kunnen analyseren en op basis van de uitvoer conclusies te trekken. Op basis hiervan kan hij de initiator van nieuw beleid zijn.

CONCLUSIES

De methode leidt tot een besluitvorming die veel betrouwbaarder en genuanceerder kan zijn dan anders mogelijk zou zijn. Knelpunten en zwakke punten ten aanzien van de prioriteitenstelling in de organisatie worden zichtbaar. Het blijkt voor de deelnemers een methodiek te zijn waar men snel aan gewend is. Zij beoordelen het als erg positief dat ieders mening even hard kan doorklinken en een juist gewicht kan krijgen. Zij vinden dat de oordeelsvorming door ondersteuning van zo'n methode veel systematischer en volledíger wordt. Zo'n systeem brengt de indieners van een voorstel tot een betere motivering van de voorstellen en leidt bij de besluitvormers tot een meer expliciete beoordeling. De kwaliteit van de organisatie kan er in sterke mate positief door worden beïnvloed.
De IT-manager en de EDP-auditor vinden in Decision een krachtig hulpmiddel bij hun werk. De IT-manager wordt gesteund bij zijn beslissingen betreffende de prioriteiten en hij krijgt een hulpmiddel voor strategische beleidsvorming. De EDP-auditor kan het hulpmiddel hanteren bij zijn beoordeling van de kwaliteit en ter ondersteuning van zijn adviezen.

LITERATUUR

[Bede85] E.F. Bedell, *The Computer Solution Strategies for the Information Age*, Irwin, Illinois, 1985.

Dr. P.J. van Meel RI
Is directeur van Van Meel Associates BV te Kaatsheuvel, dat als motto heeft: "matching economics and informatics". Daarvóór was hij bij enkele middelgrote ondernemingen verantwoordelijk voor economische zaken en informatietechnologie. Gedurende twaalf jaar vervulde hij deze functie ook bij één van de grootste AA-organisaties, en werkte hij vanuit die positie mee aan de landelijke informatiemodellen voor de agrarische sector. Tijdens deze periode promoveerde hij aan de KUB op het onderwerp "Een optimalisatiemodel voor automatisering bij AA-organisaties".

De audit van een IT-investeringsaanvraag

Drs.ing. S.R.M. van den Biggelaar en drs. P.P.M.G.G. Brouwers

Het beoordelen van IT-investeringsaanvragen moet volgens een gestructureerde aanpak plaatsvinden. Bij deze beoordeling dienen zowel formele als inhoudelijke aspecten een rol te spelen. Hoewel in dit artikel niet een totaaloplossing wordt geboden, wordt wel een structuur voor het uitvoeren van een hierop gerichte audit beschreven. Op basis van deze structuur is het mogelijk verdere invulling te geven aan de inhoudelijke beoordelingsaspecten van een dergelijke audit.

INLEIDING

Investeringen in informatietechnologie bezorgen het management nog steeds of zelfs in toenemende mate problemen. Via diverse bedrijfseconomische methoden wordt getracht de kosten en baten van IT-investeringen inzichtelijk te maken, zodat het management op verantwoorde wijze besluiten kan nemen. In het themanummer 1992/2 van Compact is door Swinkels en Van Irsel bij deze problematiek al uitgebreid stilgestaan. Hoewel diverse bedrijfseconomische methoden zijn onderkend, voorzien van een theoretische onderbouwing, blijkt het management nog géén of onvoldoende grip te hebben op IT-investeringen.

Het management blijft informatietechnologie nog te veel als een bijzonder aspect in de bedrijfsvoering beschouwen, waarbij men zich tevreden stelt met globale beloften omtrent de gunstige effecten van informatietechnologie of zich zelfs in het geheel niet bewust is van de kosten en baten van informatietechnologie. Zelfs in organisaties die op allerlei terreinen forse bezuinigingen doorvoeren blijkt dat op het gebied van informatietechnologie het geld als het ware over de balk wordt gesmeten. Indien hierover discussies met het management worden opgestart, blijkt veelal het management hiervoor niet ontvankelijk te zijn. Wellicht heeft men zich al tevreden laten stellen door IT-beheerders en automatiseerders met argumenten over alle 'ongrijpbare' voordelen van het toekomstige informatiesysteem en/of de verbeterde infrastructuur.
Automatisering en informatietechnologie worden nog te veel als tovermiddel gehanteerd voor het oplossen van vooral organisatorische problemen, hoewel in de praktijk het tegendeel toch genoegzaam wordt bewezen. Met vallen en opstaan leren of door schade en schande wijzer worden lijkt op het gebied van informatietechnologie wel vergaand te zijn doorgevoerd. Het management, dat al jarenlang vertrouwd is met tal van investeringsbeslissingen, lijkt IT-investeringen of voorstellen daartoe echter nog te weinig gestructureerd te benaderen.

Zonder theoretische beschouwingen als oplossing voor dit vraagstuk te introduceren, wordt in dit artikel eerst een aantal van de huidige problemen ontleend aan de praktijk behandeld. Daarna worden, aan de hand van een tweetal casussen, praktijksituaties beschreven van de wijze waarop het management omgaat met IT-investeringsaanvragen. Vervolgens wordt een gestructureerde aanpak beschreven waarmee een IT-investeringsaanvraag kan worden beoordeeld. Ten slotte wordt aan de hand van de beschreven casusposities de toegevoegde waarde van de IT-investeringsaudit toegelicht.
Dit artikel pretendeert niet de oplossing, als die al bestaat, voor alle problemen ten aanzien van het beheersen van IT-investeringen te bieden. Wel wordt een structuur beschreven, waarmee het mogelijk is omissies op basis van gericht onderzoek te reduceren. Zowel voor auditors als voor het management wellicht een uitdaging om hieraan een actieve bijdrage te leveren.

PROBLEMEN TEN AANZIEN VAN IT-KOSTEN EN -BATEN

In praktijksituaties wordt regelmatig een aantal problemen op het gebied van de beheersing van kosten en baten van informatietechnologie onderkend. Een aantal problemen is onderstaand samengevat:

- Een integraal IT-budget of integrale IT-taakstelling ontbreekt veelal. Hierdoor is het niet mogelijk het effect van IT-investeringen op het totale kostenniveau en ten opzichte van andere investeringen te bepalen.

- Investeringsaanvragen worden onderbouwd door technische experts, die geen of onvoldoende kennis hebben van bedrijfseconomische methoden.

- De indirecte kosten van informatietechnologie (bijvoorbeeld beheeractiviteiten in de gebruikersorganisatie) zijn moeilijk te identificeren en kwantificeren.

- De IT-kosten in de infrastructuur en de IT-toepassingen worden onvoldoende duidelijk onderscheiden.

Met betrekking tot de IT-baten zijn als probleemgebieden te noemen:

- Er zijn geen objectieve parameters om het effect van informatietechnologie te meten.

- Informatietechnologie is sterk geïntegreerd in de organisatie, waardoor het moeilijk is aan te geven welke baten aan welk deel van de informatietechnologie dienen te worden toegekend.

- Evenals bij de kostenbepaling of zelfs in versterkte vorm geven de bedrijfseconomische methoden onvoldoende antwoord op het bepalen van de baten.

- De baten omvatten vele kwalitatieve aspecten.

Deze problemen kunnen leiden tot onvolledige IT-investeringsaanvragen. Onvolledig in de betekenis van het ontbreken van bepaalde kosten- en/of batencomponenten. Voor het management is het veelal moeilijk hier doorheen te prikken, zeker als de aanvraag 'op gekleurde wijze' wordt ingediend door een direct belanghebbende zoals de eigen automatiseringsafdeling of als de verantwoordelijke zich sterk heeft laten leiden door een hardware- of software-leverancier. De investeringsaanvragen ogen veelal professioneel, waardoor de juistheid en/of volledigheid hiervan niet snel ter discussie wordt gesteld. Wellicht is in het land der blinden éénoog nog te veel koning. Voorbeelden van onaangename verrassingen die hieruit kunnen resulteren, blijken uit de praktijk.

CASUSSEN

Uit de EDP-audit-praktijk kunnen diverse voorbeelden worden opgesomd die genoemde problemen op het gebied van het bepalen en beheersen van de IT-kosten en -baten onderschrijven. Via een tweetal gestileerde voorbeelden zal het dilemma van het management bij het beoordelen van IT-investeringen worden belicht.

Casus 1. Voorstel voor vervanging hardware- en software-omgeving

Een bedrijf in de midden- en kleinbedrijfsector heeft al sinds een aantal jaren problemen met de huidige geautomatiseerde informatievoorziening. De support van de leverancier wordt als volstrekt onvoldoende ervaren en men heeft zich her en der georiënteerd op mogelijke andere oplossingen. Eén potentiële leverancier heeft zeer actief op deze problemen ingespeeld en de organisatie als het ware aan de hand genomen. Via een aantal sessies bij het bedrijf heeft de potentiële leverancier de toekomstige informatievoorziening voor het bedrijf vastgelegd. Daarop gebaseerd is door de leverancier een offerte voor de vervanging van de hardware en software opgesteld.

Het management is gezien de ervaringen van de afgelopen jaren argwanend geworden ten aanzien van de automatiseringsbranche. Al snel verdenkt men de leverancier van een te rooskleurige voorstelling van zaken, waardoor gedurende een aantal jaren over diverse details wordt onderhandeld. In dit proces stelt de leverancier zijn specificaties steeds bij, waardoor nieuwe offertes voorzien van andere prijsstellingen weer moeilijk vergelijkbaar zijn met de voorgaande offertes. Het management denkt alleen nog in termen van eventueel te verkrijgen kortingen op de totaalprijs.

Op een bepaald moment wordt een EDP-auditor ingeschakeld om duidelijkheid te creëren in de situatie. De volgende problemen worden onder andere onderkend:

- De eisen en wensen ten aanzien van de informatievoorziening van de organisatie zijn niet gestructureerd bepaald.

- Slechts de aanschaf- en onderhoudskosten voor de hardware en software zijn gespecificeerd. De kosten voor de implementatie en eventueel benodigde organisatorische veranderingen blijken vaag te zijn.

- De baten zijn niet onderkend.

- Vergelijkingscijfers over de kosten ten aanzien van automatisering in de branche ontbreken. Het management weet niet welke kosten acceptabel zijn voor zijn bedrijf.

Casus 2. Investeringsaanvraag 'maatwerk'-software

Bij een industriële onderneming met een aantal buitenlandse verkoopmaatschappijen wordt door het management besloten dat het gehele concern van hardware-omgeving moet veranderen. Met deze verandering van hardware-lijn is een investering gemoeid van ongeveer 2,5 miljoen gulden. De investeringsaanvraag wordt door de automatiseringsmanager gelegitimeerd met als argument dat de oude hardware-lijn dringend aan vervanging toe is. Het concern heeft namelijk te kampen met performance-problemen, te beperkte geheugencapaciteit en stijgende onderhoudskosten. Bovendien wordt door omschakeling naar een andere omgeving een jaarlijkse besparing van vijftien procent verwacht op produktie-/onderhoudskosten ten opzichte van de oude hardware-lijn.

Initiële kosten		**Aantal mensmaanden**	**Kosten**
Automatiseringspersoneel		12 (à 10)	120
Externe ondersteuning		12 (à 20)	240
Gebruikersorganisatie		20 (à 7,5)	150
Bijzondere kosten			50
Totaal initiële kosten A:			560
Operationele kosten	**Beslag op capaciteit door A**	**Totale operationele kosten**	**Kosten**
Automatiseringskosten	37,5 %	200	75
Onderhoudskosten	10 %	1.000	100
Bijzondere kosten			-
Totaal operationele kosten A:			175
Besparingen		**Aantal**	**Besparingen**
Personeel		10 (à 90)	900
Totaal besparingen A:			900
ROI A ([besparingen - operationele kosten]/initiële kosten) x 100 %			**129,46 %**

Figuur 1. 'ROI'-berekening deelproject A.

Figuur 2. ROI-overzicht project 'maatwerk'-software.

Deel project	Initiële kosten	Operationele kosten	Besparingen	%-ROI
A	560	175	900	129,46
B	...			
C				
...				
Totaal	2.000	1.200	4.000	140

De software is eveneens verouderd. In eerste instantie wordt de bestaande software geconverteerd naar de nieuwe hardware-omgeving, waarna aan de automatiseringsmanager wordt gevraagd een onderzoek in te stellen naar een geschikt softwarepakket voor het gehele concern. Na een uitgebreid onderzoek komt de automatiseringsmanager tot de conclusie dat er momenteel geen standaardsoftware-pakket op de markt aanwezig is dat volledig voldoet aan de eisen van de organisatie. Bovendien heeft de automatiseringsmanager het vermoeden dat 'maatwerk'-software ongeveer even duur zal uitvallen als het meest geschikte standaardpakket. Er wordt besloten een softwarebureau in te schakelen. Aan het software-bureau wordt gevraagd een offerte uit te brengen voor het ontwikkelen van specifiek maatwerk voor de organisatie.

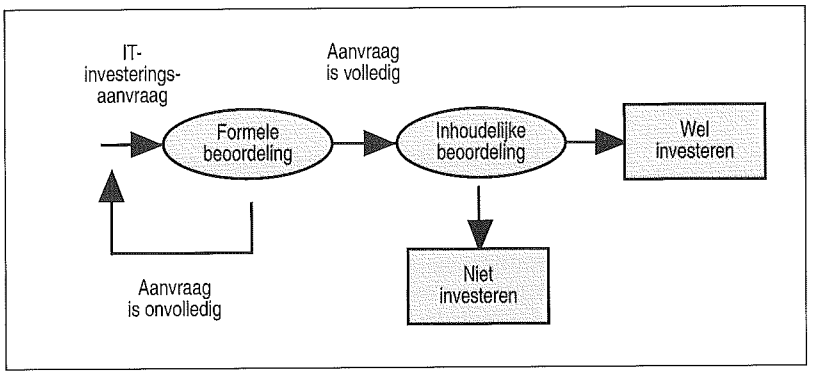
Na een uitgebreide voorstudie door het softwarebureau wordt het plan van aanpak voor de 'maatwerk'-software opgeleverd dat bestaat uit:

- De splitsing van de 'maatwerk'-software in een zestal deelprojecten:
  1. inkoop/produktie/opslag/uitlevering;
  2. bestandsopbouw;
  3. planning;
  4. marktbewerkingssysteem;
  5. ontwikkeling;
  6. financiën.
- Een 'Return On Investment' (ROI)-berekening per deelproject. De 'ROI'-berekening van deelproject A is in figuur 1 uitgewerkt.
- Een ROI-overzicht van het gehele project, zoals in figuur 2 is te zien.
- Een cash-flow-overzicht van het gehele project. Een overzicht waarin per jaar, per project de initiële kosten, operationele kosten en besparingen worden afgezet.
- Tevens maakt een compleet tijdsplan deel uit van het plan van aanpak.

Tijdens een management-vergadering wordt het plan van aanpak op een heldere en overtuigende wijze uiteengezet door het software-bureau. Met name de hoge ROI-percentages op de verschillende deelprojecten en de al reeds in het vijfde jaar verkregen positief gecumuleerde cash-flow maakt indruk op het management. Het management heeft wel een onbehaaglijk gevoel bij de opgestelde kosten/baten-berekening maar kan dit verder niet 'hard' maken.
De automatiseringsmanager is van mening dat het project een goede kans van slagen heeft. Bovendien zijn weliswaar de kosten van het project tien procent hoger dan de standaardoplossing, maar daar heeft men dan wel op maat gemaakte software voor. Het management besluit het project op te starten.

STRUCTUUR VAN DE IT-INVESTERINGSAUDIT

In de voorgaande twee casusposities is een aantal problemen beschreven die organisaties ondervinden bij investeringen in informatietechnologie. Om dergelijke problemen te voorkomen dient het management zich een oordeel te vormen over de inhoud van de investeringsaanvraag. De IT-investeringsaudit is een methode om een IT-investeringsaanvraag te beoordelen en kan het management dan ook ondersteunen bij zijn besluitvorming omtrent de investeringen in informatietechnologie.



Figuur 3. Fasen van een IT-investeringsaudit.

Doelstelling

Het uitgangspunt van de methode is een structuur aan te reiken waarlangs een IT-investeringsaanvraag gestructureerd kan worden geanalyseerd en beoordeeld.
De IT-investeringsaudit richt zich daarbij onder meer op:
- de volledigheid van de IT-investeringsaanvraag;
- de kosten en baten die in de investeringsaanvraag zijn onderkend;
- de maatregelen die zijn genomen om de risico's (bijvoorbeeld budget- of tijdsoverschrijding) te verkleinen.

De methode bevat dus geen volledige verzameling van kwantitatieve en kwalitatieve normen waaraan een IT-investeringsaanvraag kan worden getoetst. Dergelijke normen zijn op dit moment nog niet voorhanden.

Tweedeling van de audit

IT-investeringsaanvragen blijken regelmatig onvolledig te zijn. De aanvragen zijn bijvoorbeeld vanuit een te technische invalshoek opgesteld, waarbij bedrijfseconomische aandachtspunten onderbelicht zijn of investeringsaanvragen voldoen niet aan bepaalde richtlijnen die zijn opgesteld door het management of een moedermaatschappij. Heeft een organisatie bijvoorbeeld standaarden en richtlijnen op het gebied van informatietechnologie 'preferred suppliers', data- of berichtstandaarden, hardware-architectuur, enz.), dan moet in de investeringsaanvraag worden aangegeven of de IT-investering voldoet aan deze richtlijnen.
Als dergelijke aspecten in een investeringsaanvraag ontbreken is een verantwoorde beoordeling van de investeringsaanvraag niet mogelijk. Om te voorkomen dat onvolledige investeringsaanvragen toch inhoudelijk diepgaand worden beoordeeld, is de audit van IT-investeringsaanvragen gesplitst in twee delen (zie figuur 3).

Formele beoordeling

Het eerste deel van de audit bestaat uit een formele beoordeling van de investeringsaanvraag. Daarin wordt enerzijds beoordeeld of de investeringsaanvraag formeel voldoet aan de eisen zoals die gesteld zijn door bijvoorbeeld de moedermaatschappij of het management. Anderzijds wordt beoordeeld of de investeringsaanvraag dusdanig volledig is opgesteld dat de inhoudelijke beoordeling kan plaatsvinden zonder dat steeds een terugkoppeling noodzakelijk is naar de indieners van de aanvraag. Zo moeten het aantal jaren zijn aangegeven waarin de investering wordt afgeschreven, een inschatting van de niet-kwantificeerbare baten, enz.
Het hulpmiddel bij de formele beoordeling is een checklist bestaande uit diverse vragen zodat snel de volledigheid van de investeringsaanvraag kan worden geïnventariseerd (zie figuur 4). Als bij een vraag op de checklist 'Nee' wordt ingevuld, is de investeringsaanvraag onvolledig. In de checklist mag de optie 'N.v.t.' bij bepaalde vragen slechts worden aangekruist als aan voorwaarden is voldaan. Deze voorwaarden staan vermeld bij het nummer dat in de desbetreffende 'N.v.t.'-cel staat. Bij de vraag 'Wordt de IT-investering geplaatst binnen het IT-beleid?' wordt verwezen naar punt 4 waar de voorwaarde is opgenomen dat afhankelijk van de grootte van de organisatie deze vraag niet

Figuur 4. Gedeelte van de checklist voor de formele beoordeling.

	Ja	Nee	N.v.t.
Wordt de IT-investering geplaatst binnen het IT-beleid?			4
Is de gewenste situatie met betrekking tot de automatisering vastgelegd?			
Zijn de eisen van de gebruikers met betrekking tot de gewenste situatie vastgelegd?			
Heeft een inventarisatie van de huidige knelpunten plaatsgevonden? *(met name van belang bij herauotomatisering?)*			

van toepassing hoeft te zijn. Bij kleinere organisaties ontbreekt het veelal aan een formeel informatiebeleid waardoor deze vraag niet van toepassing is.

Tijdens de formele beoordeling wordt ook een inventarisatie van de kosten van de investering gemaakt. In investeringsaanvragen worden soms alleen de kosten van de investering meegenomen (initiële kosten van hardware en software). Dit leidt tot een onvolledige weergave van de kosten die met de investering zijn gemoeid. Behalve de initiële kosten brengt een investering in informatietechnologie ook kosten met zich mee in de gebruikersorganisatie (daarbij kan gedacht worden aan opleidingen, tijd (geld) die nodig is om met het systeem te leren werken). Deze categorie van kosten wordt vaak 'vergeten' in het kostenplaatje van de investering. Daarnaast worden de operationele en onderhoudskosten gedurende de levensduur van de IT-investering niet altijd meegenomen. Doordat deze kosten vaak een veelvoud van de initiële kosten van de investering bedragen hebben zij grote invloed op de totale kosten van de investering. Deze invloed wordt nog versterkt doordat de laatste jaren de initiële kosten van de investeringen (met name van hardware) alleen maar zijn gedaald en de operationele en onderhoudskosten een stijgende tendens laten zien.

Figuur 5. Typologie van IT-toepassingen.

Classificaties			Voorbeelden
IT die niet direct een bedrijfsproces in de organisatie ondersteunt	IT die noodzakelijk is voor het functioneren van andere IT-toepassingen		- Computers - Netwerken - Operating systemen - Datacommunicatie-software
	IT die een toegevoegde waarde geeft aan het functioneren van andere IT-toepassingen		- Toegangsbeveiligingssystemen - Doorbelastingssystemen - DBMS
IT die een bedrijfsproces in de organisatie ondersteunt	IT die een administratief proces ondersteunt	IT die processen op operationeel niveau ondersteunt	- Salarisverwerkingssystemen - Financiële systemen - Offertesystemen - Tekstverwerkingssystemen
		IT die processen op tactisch en strategisch niveau ondersteunt	- MIS - EIS - DSS
	IT die een produktieproces ondersteunt of vervangt	IT die een produktieproces ondersteunt	- Produktiebesturingssystemen - CIM - CAD/CAM - Chips in machines
		IT die een produktieproces vervangt	- Robots
	IT die het aanbieden van diensten ondersteunt		- Elektronisch bankieren - Databanken met commerciële informatie

Als nu blijkt dat bepaalde onderdelen in de aanvraag onvoldoende zijn toegelicht of wellicht geheel ontbreken, dan dienen de indieners van de aanvraag (de gebruikers- en/of automatiseringsorganisatie) de investeringsaanvraag eerst aan te vullen, zodat alsnog een inhoudelijke beoordeling van de investeringsaanvraag kan plaatsvinden.
De formele beoordeling kan leiden tot een tweetal conclusies:
- de investeringsaanvraag is onvolledig en dient nader te worden aangevuld voordat een inhoudelijke beoordeling kan plaatsvinden;
- de investeringsaanvraag verschaft voldoende gegevens om te kunnen komen tot een inhoudelijke beoordeling.

Inhoudelijke beoordeling

Tijdens de inhoudelijke beoordeling wordt de investeringsaanvraag geanalyseerd en beoordeeld. Daartoe wordt een onderscheid gemaakt in een drietal deelgebieden - kosten, baten en risico's - die afzonderlijk worden beoordeeld. Overigens hebben de deelgebieden wel invloed op elkaar. Met name de risico's van de investering hebben invloed op de kosten en de baten van de investeringsaanvraag. Zijn aan een investering in informatietechnologie grote risico's verbonden, dan kan dit zowel invloed hebben op de kosten (bijvoorbeeld budgetoverschrijding) als op de baten (bijvoorbeeld het niet optreden van 'verwachte' baten).
De traditionele bedrijfseconomische methoden voor investeringsselectie (Netto Contante Waarde en ROI) nemen van de drie deelgebieden de kosten en de baten mee in de berekening. De risico's daarentegen worden in de berekening niet expliciet meegenomen.
Een voordeel van de bedrijfseconomische methoden is echter dat de uitkomsten aan bedrijfsdoelstellingen of -normen kunnen worden getoetst. Zo kan ongeacht de soort of omvang van de investering als norm worden gesteld dat de ROI minimaal tien procent moet zijn. De methoden zijn echter sterk afhankelijk van de mogelijkheid de baten te kwantificeren. Aangezien bij veel investeringen in informatietechnologie de gekwantificeerde baten moeilijk zijn te bepalen kunnen methoden als NCW en ROI slechts in beperkte mate bij het beoordelen van IT-investeringsaanvragen worden toegepast.
Voor de beoordeling van IT-investeringsaanvragen waarvan het niet mogelijk is de ROI te berekenen moeten ook additionele normen worden bepaald waaraan de investeringsaanvraag moet voldoen. Daarbij dient onderscheid te worden gemaakt naar de soort investering. Investeringen in hardware of netwerken brengen andere kosten met zich mee dan investeringen in een standaard-software-pak-

ket voor de financiële administratie. Voor de baten van de investering geldt hetzelfde. De baten van een investering in een netwerk liggen op een geheel ander gebied dan de baten van een investering in een CAD/CAM-systeem.
Om structuur aan te brengen in het aantal verschillende soorten toepassingen van informatietechnologie is in figuur 5 een typologie van IT-toepassingen beschreven. Op basis van deze typologie kunnen voor zowel de kosten als de baten specifieke normen per soort IT-toepassing worden ontwikkeld. Tijdens de inhoudelijke beoordeling van de investeringsaanvraag worden de kosten en de baten van de investeringsaanvraag getoetst aan de normen die specifiek gelden voor de soort investering in informatietechnologie (op basis van de typologie). Overigens zijn op dit moment de normen nog niet volledig voorhanden; zij moeten in de praktijk nog nader worden geconcretiseerd.
Bij de onderdelen kosten en baten van deze subparagraaf wordt nader ingegaan op het gebruik van de typologie tijdens de inhoudelijke beoordeling.

Kosten
De weergegeven kosten in de investeringsaanvraag zijn niet altijd een realistische weergave van de werkelijke investeringskosten.
Enerzijds kunnen de kosten in de investeringsaanvraag bewust laag worden gehouden om zodoende de kunstmatig een hoog rendement van de investering te creëren. Een gevolg hiervan is dat tijdens de ontwikkeling en het gebruik van de informatietechnologie het budget wordt overschreden doordat de kosten vele malen hoger uitvallen dan oorspronkelijk gepland. Anderzijds kunnen de kosten juist ruim zijn ingeschat om te voorkomen dat later het budget wordt overschreden. Dit is mogelijk als het rendement van de investering niet wordt berekend waardoor een (te) ruime inschatting van de kosten geen gevolg heeft voor de berekening van de ROI.
Bij de inhoudelijke beoordeling van de investeringskosten is het met name de vraag of de kosten van de voorgestelde oplossing (IT-investering) realistisch zijn.
De IT-investeringsaanvraag wordt daartoe ingedeeld in de typologie van IT-toepassingen. Op basis van gegevens over de investering (investeringsbedrag, aantal gebruikers, enz.) kan een vergelijking worden gemaakt van de kosten van de investering met de normkosten (benchmarks) zoals die zijn opgesteld voor dergelijke investeringen. De ontwikkeling van de benchmarks waaraan de kosten van de investeringsaanvraag kunnen worden getoetst, zal echter nog een nadere invulling moeten krijgen.
Daarnaast kunnen de kosten van de investering (met name de initiële kosten van de investering) worden vergeleken met een aantal alternatieven. Het is bijvoorbeeld mogelijk dat een andere oplossing (andere hardware, andere infrastructuur of andere software) minder geld kost. Daarbij dient deze oplossing vanzelfsprekend minimaal dezelfde functionaliteiten af te dekken. De kosten van een investering in een bepaalde hardware-omgeving (bijvoorbeeld een mini) kunnen bijvoorbeeld worden vergeleken met de kosten van een soortgelijk investeringsalternatief (bijvoorbeeld client/server-concept, een andere mini of wellicht uitbesteding).

Risico's
Aan investeringen in informatietechnologie zijn risico's verbonden. Zo worden in de praktijk regelmatig projecten te laat opgeleverd of voldoet het systeem niet aan de verwachtingen van de gebruikers. Tijdens het beoordelen van de investeringsaanvraag moeten de risico's van de investering dan ook worden geïnventariseerd.
Allereerst worden de risico's ten aanzien van de investering geïnventariseerd. Vervolgens wordt de kans ingeschat dat het risico ook daadwerkelijk optreedt. Omdat een gedetailleerde kwantificering vaak moeilijk is, vindt een meer kwantitatieve beoordeling plaats (kansinschatting van laag tot en met zeer hoog). Een investeringsaanvraag in informatietechnologie leidt bijvoorbeeld vaak tot de definiëring van een project. Een risico bij het definiëren van een project is budgetoverschrijding. Afhankelijk van de soort investering is de kans op budgetoverschrijding laag (bij een standaardapplicatie in een stabiele omgeving) tot zeer hoog (maatwerk in een onzekere, snel veranderende omgeving). Soortgelijk aan dit voorbeeld worden de overige risico's ingeschat.
Ten slotte worden per onderkend risico de maatregelen vastgesteld die zijn getroffen om deze risico's te verkleinen. Om de diverse risico's van een IT-investering overzichtelijk te inventariseren zijn deze onderverdeeld in de categorieën organisatorisch risico, projectrisico en technisch risico.

1. Organisatorisch risico
Het organisatorisch risico richt zich voornamelijk op het risico dat de ontwikkeling en implementatie van de informatietechnologie in de organisatie problemen oplevert. Als de toekomstige gebruikers van de informatietechnologie niet gemotiveerd zijn ermee te werken, ontstaat een risico dat de investering niet de resultaten (verwachte baten) oplevert die ervan worden verwacht. Andere risicofactoren zijn bijvoorbeeld de stabiliteit van de omgeving en de omvang van de investering. De stabiliteit is in te schatten door het inventariseren van het aantal concurrenten in de markt of door het bepalen van de mate waarin produktspecificaties aan verandering onderhevig zijn. De omvang van het investeringsbedrag kan worden afgezet tegen financiële kenmerken van de organisatie, zoals de omzet, winst, IT-budget en liquiditeitspositie.

Na het inventariseren van de organisatorische risico's worden de maatregelen beoordeeld die zijn genomen om de risico's te verkleinen. Bij het eerder genoemde risico van niet-gemotiveerde gebruikers kan een maatregel zijn de gebruikers bij het gehele project (al tijdens het opstellen van de investeringsaanvraag) actief te betrekken om een goede motivatie te waarborgen.

2. Projectrisico
Het projectrisico geeft het risico weer dat de ontwikkeling en de implementatie van het project problemen opleveren. Daarbij zijn risico's te onderkennen als:
- budgetoverschrijding;

- tijdsoverschrijding;
- de kwaliteit van de opgeleverde informatietechnologie is onvoldoende.

Deze risico's kunnen worden verkleind door bijvoorbeeld in de investeringsaanvraag een stappenplan op te nemen waarin is beschreven wat wanneer moet worden opgeleverd en waarin afspraken over het budget zijn gemaakt.

3. Technisch risico
Bij het technisch risico wordt geanalyseerd of de gekozen oplossing technisch haalbaar is. Enerzijds wordt beoordeeld of de techniek/oplossing al 'volwassen' is. Daarbij kan onder meer worden gekeken naar het aantal implementaties van een systeem. Blijkt het systeem pas een aantal malen te zijn geïnstalleerd, dan zal implementatie een risico met zich meebrengen. Anderzijds moet worden beoordeeld of de organisatie 'gereed' is voor de investering en of voldoende kennis in de organisatie aanwezig is. Van een organisatie die bijvoorbeeld alleen de administratie heeft geautomatiseerd, kan niet worden verwacht dat daar direct een geheel geïntegreerd produktiesysteem kan worden geïmplementeerd.
Het resultaat van het inventariseren en beoordelen van de risico's is een overzicht van risico's die de organisatie loopt als wordt geïnvesteerd in de IT-toepassing. Deze onderkende risico's moeten worden meegenomen in de uiteindelijke afweging of wordt geïnvesteerd in de IT-toepassing.

Baten
Nadat het inhoudelijk beoordelen van de kosten en de risico's verbonden aan de investering is voltooid, wordt een analyse verricht naar de verwachte baten van de investering. De baten zijn daarbij te definiëren als voordelen/middelen ontvangen door de organisatie die voortvloeien uit het gebruik van informatietechnologie.
In dit onderdeel van de audit worden de verwachte baten van de investeringsaanvraag in de informatietechnologie geanalyseerd en beoordeeld.
In de praktijk blijkt dat het duidelijk identificeren van de baten van informatietechnologie op problemen stuit waardoor in veel IT-investeringsaanvragen de baten slechts summier of in het geheel niet zijn beschreven.
Op basis van de gegevens in de investeringsaanvraag (onder meer de eisen/wensen van de gebruikers, huidige knelpunten, indicatie van de verwachte baten) kan de toegevoegde waarde van de investering voor de organisatie worden ingeschat. Daarbij dienen zowel de kwantificeerbare als niet-kwantificeerbare baten te worden meegenomen.
Om de inventarisatie en beoordeling van de baten overzichtelijk uit te voeren zijn de baten onderverdeeld in een viertal categorieën, namelijk functionaliteiten, strategische betekenis, efficiëntie en noodzaak.

1. Functionaliteiten
Bepaalde investeringen in informatietechnologie creëren de mogelijkheid nieuwe activiteiten uit te voeren of bestaande activiteiten op een hoger kwaliteitsniveau te brengen. Op basis van de eisen/wensen van de gebruikers en de beschreven huidige situatie met knelpunten kan worden beoordeeld of met de investering nieuwe functionaliteiten mogelijk zijn.
Daarbij dient in acht te worden genomen dat de extra geboden functionaliteiten wel gebaseerd moeten zijn op de eisen/wensen van de gebruikers. Er moet met andere woorden wel behoefte zijn aan de geboden functionaliteiten, anders investeert een organisatie in informatietechnologie met diverse mogelijkheden waar verder geen gebruik van wordt gemaakt.

2. Strategische betekenis
Een investering in informatietechnologie is soms van belang voor het voortbestaan van de organisatie. Om de strategische betekenis van de informatietechnologie te bepalen kan de investeringsaanvraag worden getoetst aan de strategie, bedrijfsdoelstellingen en informatiebehoeften. Daarnaast wordt het belang van het bedrijfsproces voor de organisatie onderkend (proces waarin de informatietechnologie wordt ingezet) en vervolgens het belang van informatietechnologie om dat proces goed te kunnen ondersteunen. Ten slotte wordt gekeken naar de gevolgen voor het voortbestaan van de organisatie op korte en lange termijn als niet in informatietechnologie wordt geïnvesteerd (bijvoorbeeld een achterstand ten opzichte van de concurrentie).

3. Efficiëntie
Deze soort baten wordt vaak als enige beschreven in investeringsaanvragen, en wel omdat de verbetering in efficiëntie is uit te drukken in besparing van tijd en mankracht en dus uiteindelijk in geld. Doordat de baten kwantificeerbaar zijn in geld kan de ROI worden berekend. Het voordeel hiervan is dat het management zich een beter oordeel kan vormen over de investeringsaanvraag omdat ook overige investeringen in bedrijfsmiddelen met behulp van ROI worden geëvalueerd.

4. Noodzaak
Sommige investeringen in informatietechnologie moeten als noodzakelijk worden gezien, wil een organisatie kunnen functioneren. Deze noodzaak kan enerzijds het gevolg zijn van bepaalde wetgeving, maar kan ook voortvloeien uit het feit dat het functioneren in een bepaalde industrietak bepaalde minimale investeringen in informatietechnologie tot gevolg heeft (bijvoorbeeld CAD/CAM-systemen om vliegtuigen te ontwerpen).

Op basis van de indeling van de investeringsaanvraag in de typologie worden de verwachte baten van de investering in informatietechnologie getoetst aan de normen die bij de typologie van IT-toepassingen zijn opgenomen. Deze normen dienen daarbij te zijn afgeleid van bovenstaande indeling van de baten. Ook hier geldt dat momenteel nog geen eenduidige set van normen voorhanden is waaraan de verwachte baten van de investeringsaanvraag kunnen worden getoetst.
Voor een aantal soorten IT-toepassingen kunnen al wel richtinggevende normen worden onderkend. Een voorbeeld is PTT Post, die onlangs heeft besloten de sortering van de post grotendeels te automatiseren. Hierdoor gaat een aantal arbeidsplaatsen verloren. Deze investering is in te delen bij de

classificatie 'IT die een produktieproces vervangt'. Doordat bij dit soort investeringen de baten vaak te kwantificeren zijn, kan als norm gelden dat de ROI van de investering moet zijn berekend en minimaal moet voldoen aan de ROI-norm zoals die door PTT Post is opgesteld.
Voor vervangingsinvesteringen (vooral bij administratieve systemen op operationeel niveau) kan een norm zijn dat de onderhoudskosten van het nieuwe systeem (beduidend) lager moeten zijn dan de onderhoudskosten van het oude systeem. Daarnaast kan als norm gelden dat het nieuwe systeem betere functionaliteiten moet afdekken dan het vorige systeem; dit is met name van belang als het oude systeem onvoldoende functioneerde en de gebruikers diverse eisen en wensen hebben ten aanzien van het nieuwe systeem.
Een investering in een netwerk (classificatie 'IT die noodzakelijk is voor het functioneren van andere IT-toepassingen') genereert echter geen direct (kwantificeerbare) baten. Het berekenen van bijvoorbeeld een ROI als norm is hier dan ook niet realistisch. Wel kan worden geïnventariseerd hoeveel andere IT-toepassingen die wel directe baten genereren, door deze investering mogelijk worden (bijvoorbeeld de extra functionaliteiten van een mail-toepassing of de besparing op de licentiekosten doordat software-pakketten nog maar eenmalig worden aangeschaft).
In de volgende paragraaf wordt, gerelateerd aan de beschreven casusposities, ingegaan op de praktische uitvoering van zowel de formele als de inhoudelijke beoordeling.

UITWERKING CASUSPOSITIES MET DE IT-INVESTERINGSAUDIT

In casus 1 betrof het de herautomatisering van een aantal processen in een bedrijf, waarbij het management problemen had met de voorgestelde oplossing van een leverancier. In casus 2 werd een investeringsaanvraag beschreven inzake 'maatwerk'-software waaraan het management zijn goedkeuring had verleend.
In deze paragraaf wordt de toegevoegde waarde van de IT-investeringsaudit beschreven voor beide casusposities; daarbij wordt aangegeven op welke wijze de onderkende problemen met behulp van de IT-investeringsaudit hadden kunnen worden gesignaleerd.

Casus 1

Toepassing van de IT-investeringsaudit op de eerste casuspositie, waarbij door onvolledigheid van de investeringsaanvraag slechts een formele beoordeling wordt uitgevoerd.

Formele beoordeling
Bij de formele beoordeling van de investeringsaanvraag blijkt tijdens de inventarisatie van de kosten dat deze onvolledig zijn beschreven in de investeringsaanvraag. Zo zijn onder meer de kosten van de implementatie alsmede de kosten die gebruikers maken om met het systeem te kunnen werken niet of onvoldoende duidelijk meegenomen. Het gevolg is een onvolledige weergave van de verwachte kosten van de investering.
Tijdens het invullen van de checklist wordt geconstateerd dat een inventarisatie van de eisen/wensen van de gebruikers en een overzicht van de knelpunten ontbreken. Hierdoor is het onmogelijk te bepalen of de voorgestelde oplossing van de leverancier overeenstemt met de behoeften van de gebruikers. Doordat het een investeringsaanvraag betreft over de herautomatisering van een aantal administratieve processen is het bovendien belangrijk inzicht te hebben in de huidige status van de automatisering aangevuld met de knelpunten. Met behulp van de knelpunten kunnen immers de belangrijkste verbeteringen ten opzichte van de huidige situatie worden beschreven.
Daarnaast ontbreekt een beschrijving van de verwachte baten van de investering (dit is onder meer het gevolg van het ontbreken van de eisen/wensen van de gebruikers en het ontbreken van een beschrijving van de huidige knelpunten).

De conclusie na de formele beoordeling is dan ook dat de investeringsaanvraag op een aantal onderdelen onvolledig is. Alvorens een beslissing te nemen om te investeren (inhoudelijke beoordeling) moeten de ontbrekende delen in de investeringsaanvraag nader worden ingevuld. Pas dan kan een inhoudelijke beoordeling plaatsvinden.

Uitgangspunt van de investeringsaanvraag moeten de eisen en wensen van de gebruikers zijn. Daarbij moet een gradatie worden aangebracht in de mate van belang van de diverse eisen en wensen.

Uitgangspunt van de investeringsaanvraag moeten de eisen en wensen van de gebruikers zijn. Daarbij moet een gradatie worden aangebracht in de mate van belang van de eisen/wensen. Zo zijn er bijvoorbeeld eisen waaraan de oplossing minimaal moet voldoen (knock out-criteria) en wensen die van belang zijn maar niet essentieel. Met deze gradatie wordt voorkomen dat een oplossing wordt gekozen die onbetaalbaar is doordat naast alle eisen ook alle wensen van de gebruikers moeten worden verwezenlijkt.
Daarnaast moeten in de investeringsaanvraag de kosten verbonden aan de investering nader worden aangevuld/gespecificeerd, met name ten aanzien van de implementatiekosten en de kosten die de gebruikers maken (bijvoorbeeld opleidingen van de gebruikers).

Door deze aanvullingen op de investeringsaanvraag ontstaat:
- een beter inzicht in de huidige problemen van de geautomatiseerde systemen;
- een volledig en duidelijk beeld van de kosten van de investering;
- een indicatie van de baten van de investering.

Op basis van de aangevulde investeringsaanvraag kan een inhoudelijke beoordeling plaatsvinden van de door de leverancier gedefinieerde oplossing.

Casus 2

De formele beoordeling van de investeringsaanvraag uit de tweede casuspositie leidt tot de conclusie dat de aanvraag eveneens niet geheel compleet is: een beschrijving van de niet-kwantificeerbare baten ontbreekt en een onderbouwing van de verwachte gekwantificeerde baten is niet opgenomen.
Gerelateerd aan de structuur van de IT-investeringsaudit had de investeringsaanvraag eerst moeten worden gecompleteerd alvorens verder te gaan met de inhoudelijke beoordeling. Als toelichting op de wijze van uitvoering van de IT-investeringsaudit worden vervolgens enkele aspecten behandeld die tijdens de inhoudelijke beoordeling van casus 2 aan bod zouden zijn gekomen.

Inhoudelijke beoordeling

- Kosten

In de formele beoordeling is geconstateerd dat de kosten van de investering afdoende volledig zijn beschreven. Tevens is tijdens deze beoordeling vastgesteld dat niet alleen de onderhoudskosten zijn begroot, maar dat ook de kosten die optreden in de gebruikersorganisatie als gevolg van de implementatie van informatietechnologie zijn meegenomen.
Bij de inhoudelijke beoordeling wordt de investeringsaanvraag betreffende de herautomatisering van een aantal administratieve processen ingedeeld bij de 'IT die een administratief proces ondersteunt' in de typologie van de IT-toepassingen. Gerelateerd aan de opgebouwde benchmarks van deze typologie vindt de beoordeling plaats van de verwachte kosten uit de investeringsaanvraag. Bij de inhoudelijke beoordeling wordt tevens het onderzoek naar het software-pakket, zoals dat door de automatiseringsafdeling is uitgevoerd, betrokken. Eveneens wordt nagegaan wat de kosten zijn van alternatieve oplossingen voor de 'maatwerk'-software.

- Risico's

De organisatie heeft gekozen voor maatwerk in plaats van standaard-software. Hierdoor ontstaat een vrij uitgebreide projectontwikkelingsfase met risico's dat het budget wordt overschreden of dat het systeem te laat wordt opgeleverd. Het projectrisico is dus groter dan in vergelijking met de keuze voor standaard-software.
Daarnaast is het technisch risico ook groter in vergelijking met standaard-software omdat aan het begin van de investering onzeker is wat wordt opgeleverd (bijvoorbeeld aan programmatuur, documentatie, enz., terwijl dit bij de keuze voor standaardprogrammatuur wel bekend is). Bovendien wordt gekozen voor een andere hardware-omgeving waarmee de organisatie niet bekend is, waardoor het technisch risico ook wordt vergroot. Voor het gestructureerd in kaart brengen van de onderkende risico's, ingeschatte kansen en getroffen maatregelen bij de IT-investeringsaudit wordt gebruik gemaakt van een risicomatrix. Gerelateerd aan de casuspositie is deze op de volgende wijze ingevuld:

Risico's	Kans	Getroffen maatregelen
Project - Budgetoverschrijding - Tijdsoverschrijding - Kwaliteit maatwerk	ZH	Geen maatregelen getroffen
Technisch - Nieuwe hardware - Maatwerk	H	Geen maatregelen getroffen
Kans: ZH = Zeer hoog	H = Hoog	

Figuur 6. Risicomatrix casuspositie.

Het blijkt dat de organisatie geen maatregelen heeft getroffen het onderkende risico te verkleinen. Bijvoorbeeld door in het contract met de leverancier de volgende afspraken op te nemen:
- mijlpalen waarbij is aangegeven wat moet worden opgeleverd op welk tijdstip en de kosten die daaraan zijn verbonden;
- boeteclausules in geval de mijlpalen niet op tijd of binnen de gebudgetteerde kosten worden opgeleverd;
- de op te leveren programmatuur, documentatie, opleidingen, enz.

- Baten

Gerelateerd aan de indeling van de baten beschreven bij de structuur van de IT-investeringsaudit zijn in de investeringsaanvraag alleen de baten op het gebied van de efficiëntie meegenomen, namelijk een besparing van tien medewerkers als gevolg van de investering. Daarbij is aangegeven dat de baten optreden, direct na de implementatie van de informatietechnologie. Deze onderkende baten zijn vervolgens gebruikt om de ROI te berekenen. Bij de inhoudelijke beoordeling wordt de onderbouwing (indien deze aanwezig zou zijn) van de 'efficiëntie'-baten geverifieerd (zijn de uitgangspunten redelijk, randvoorwaarden reëel, etc.). Dit is zeer wezenlijk aangezien het management (ook in dit geval) vaak zijn beslissingen baseert op de ROI. Doordat het regelmatig voorkomt dat dergelijke baten wel worden ingeschat bij een investeringsaanvraag maar niet worden geverifieerd, ontstaat het gevaar dat de indiener van de investeringsaanvraag de kwantificeerbare baten zodanig inschat dat er altijd een goede ROI uitkomt. Daarnaast ontbreken meetpunten waarmee de verwachte baten in de toekomst kunnen worden geëvalueerd.

Gerelateerd aan de indeling van de investeringsaanvraag binnen de IT-typologie worden de onderkende baten bij de inhoudelijke beoordeling getoetst aan de normen die daarbij zijn opgenomen. Zo wordt voor de casuspositie gesteld dat er zeker baten te verwachten zijn op het gebied van nieuwe of betere functionaliteiten ten opzichte van de huidige situatie aangezien het immers herautomatisering van een aantal administratieve processen betreft.

Resultaat
Na de formele en inhoudelijke beoordeling van de investeringsaanvraag in casuspositie 2 is een aantal conclusies te trekken:

- De niet-kwantificeerbare baten zijn niet beschreven, waardoor het niet mogelijk is de toegevoegde waarde van de investering te bepalen op het gebied van functionaliteiten en/of de noodzaak van de investering.

- Doordat in het contract met de leverancier onvoldoende maatregelen/waarborgen zijn opgenomen ten aanzien van de beheersing van het gehele project, loopt de organisatie risico's dat het project niet op tijd wordt opgeleverd, het budget wordt overschreden of dat de kwaliteit van de software onvoldoende is.

- In de investeringsaanvraag zijn de gekwantificeerde baten summier beschreven. Een verificatie van de onderbouwing kan hierdoor niet plaatsvinden en daardoor is het onduidelijk of de berekende ROI (die grotendeels afhankelijk is van de verwachte gekwantificeerde baten) ook daadwerkelijk kan worden gerealiseerd.

De IT-investeringsaudit kan, zoals blijkt uit bovenstaande casusposities, een toegevoegde waarde hebben voor de organisatie. Zo zullen onvolledige investeringsaanvragen inhoudelijk niet worden beoordeeld alvorens ze gecompleteerd zijn en wordt bij de inhoudelijke beoordeling meer zekerheid verkregen over de redelijkheid van het kosten/baten-niveau en de onderkende risico's.

TOT BESLUIT

Doordat veel organisaties in de praktijk problemen ondervinden met het beoordelen van IT-investeringsaanvragen wordt de beoordeling vaak slechts summier uitgevoerd of compleet achterwege gelaten. In dit artikel is een praktische methode beschreven waarin de aspecten worden behandeld die tijdens een gestructureerde beoordeling van een IT-investeringsaanvraag aan bod dienen te komen. Door toepassing van de IT-investeringsaudit wordt voorkomen dat onvolledige investeringsaanvragen inhoudelijk worden beoordeeld. Bovendien wordt door de inhoudelijke beoordeling meer zekerheid verkregen over de aanvaardbaarheid van de geschatte kosten, baten en risico's van de investeringsaanvraag. Op dit moment echter ontbreken vooralsnog de normen om een IT-investeringsaanvraag volledig inhoudelijk te beoordelen. Deze methode kan een aanzet zijn concrete normen te ontwikkelen waaraan de IT-investeringsaanvragen kunnen worden getoetst. Een gestructureerde beoordeling door middel van de IT-investeringsaudit (ook al is deze nog niet geheel compleet) verdient zeker, gezien het vaak op het spel staande belang, de voorkeur boven een ad hoc-benadering.

LITERATUUR

[Bigg92] S.R.M. van den Biggelaar; *Kosten-/Batenbeheersing van IT*, afstudeerscriptie, augustus 1992.

[Farb92] F. Farbey, F. Land en D. Targett, *Evaluating investments in IT*, Journal investments in IT, 1992.

[Fole89] C.K. Foley en J.C. Henderson, *Evaluating Investments in Information Technology*, January 31, 1989.

[Lege91] A. Legerman, *Besluitvorming over investeringen in informatica;* Informatie, 1991 nr. 4.

[Nowa91] P. Nowak, chapter 7, *Cost-benefit analysis for MIS expenditures,* The Economics of Information System and Software, Butter Worthe Heinemann, 1991.

[Powe92] P. Powell, *Information Technology Evaluation: Is it Different?*, Journal of the Operational Research Society, 1992, p.p. 29-40.

[Swin92] G.J.P. Swinkels en H.G.P. van Irsel, *Investeren in informatietechnologie: take IT or leave IT*, Compact, 1992/2.

[Will92] L. Willcocks, *Evaluating Information Technology investments: research findings and reappraisal,* Journal of Management of Information Systems, 1992.

Drs.ing. S.R.M. van den Biggelaar
Is sinds 1992 werkzaam bij KPMG Klynveld EDP Auditors. Hij heeft zijn studie Bestuurlijke Informatiekunde aan de Katholieke Universiteit Brabant in 1992 afgerond en is momenteel bezig met de post-doctorale opleiding EDP Audit. Hij houdt zich met name bezig met opdrachten op het gebied van effectiviteit en efficiëntie van de geautomatiseerde gegevensverwerking.

Drs. P.P.M.G.G. Brouwers
Is sinds 1989 werkzaam bij KPMG Klynveld EDP Auditors. Heeft als opleiding de studie Bestuurlijke Informatiekunde aan de Katholieke Universiteit Brabant (KUB) voltooid en is nu bezig met de post-doctorale opleiding Accountancy aan de KUB. Hij heeft audits uitgevoerd op verschillende EDP-audit-gebieden naar met name de kwaliteitsaspecten betrouwbaarheid, effectiviteit en efficiëntie. Hij is lid van de Werkgroep Information Economics van EKSBIT (Vereniging van afgestudeerde Bestuurlijke Informatiekundigen uit Tilburg).

Verzekerbaarheid van automatiseringsrisico's

Mw. mr.drs. A.W. Duthler

Automatisering levert lang niet altijd de gewenste resultaten op. Software-bedrijven kunnen hiervoor aansprakelijk worden gesteld. Dit risico zouden zij kunnen afwentelen door het afsluiten van een beroepsaansprakelijkheidsverzekering. De beroepsaansprakelijkheidsverzekering voor software-bedrijven staat echter nog in de kinderschoenen.

INLEIDING

De aansprakelijkheid van software-bedrijven voor geleverde produkten en diensten krijgt de laatste jaren steeds meer aandacht. Aansprakelijkheid voor overschrijding van kosten en opleveringstermijnen en teleurgestelde verwachtingen over het uiteindelijke resultaat van de automatisering doen zich met de regelmaat van de klok voor [Fran92].

Onder software-bedrijven worden in dit artikel verstaan zowel software-leveranciers als automatiseringsadviseurs. Bovenstaande voorbeelden hebben betrekking op beroepsaansprakelijkheid.
Met beroepsaansprakelijkheid wordt bedoeld de aansprakelijkheid voor fouten die in zuivere vermogensschade resulteren.
Onder zuivere vermogensschade wordt in verzekeringskringen verstaan financiële schade zonder dat er sprake is van een inleidende materiële beschadiging [Wans87]. Of anders gezegd, schade die niet een gevolg is van dood, lichamelijk letsel, verlies of beschadiging van goederen.
Verzekeringen tegen beroepsaansprakelijkheid (BAV's) voor de automatiseringsbranche zijn betrekkelijk nieuw.[1] Voor software-bedrijven zijn deze verzekeringen het meest interessant omdat de schade als gevolg van bijvoorbeeld een foutief ontwikkeld software-programma of verkeerd gegeven advies vooral op het gebied van de zuivere vermogensschade zal liggen. De vermogensschade kan bijvoorbeeld ontstaan doordat de gebruiker de software niet kan gebruiken voor de doelen waarvoor deze is gemaakt of doordat de software aanleiding geeft tot foutieve beslissingen.
Dat software-bedrijven in de praktijk ook behoefte hebben aan een BAV blijkt uit een studie van Degens en Bakker [DeBa90]. In dit artikel wordt nagegaan in hoeverre in Nederland beroepsaansprakelijkheidsrisico's verzekerbaar zijn. Eerst wordt beschreven op grond van welke criteria uit de wet, literatuur en jurisprudentie software-bedrijven aansprakelijk kunnen worden gesteld. Daarna wordt een overzicht gegeven van de voorwaarden waaronder beroepsaansprakelijkheidsverzekeringen in Nederland worden aangeboden. Vervolgens wordt aan de hand van een onderzoek nagegaan onder welke voorwaarden BAV's zouden kunnen worden aangeboden, maar nog niet als zodanig op de markt zijn verschenen [Duth92].

De verzekeringsmaatschappijen zijn nog zeer terughoudend in het aanbieden van een BAV. De reden daarvoor is dat ze geen goed inzicht hebben in de risicofactoren. Door het inventariseren van deze risicofactoren wordt inzicht verkregen in de mogelijkheden om beroepsaansprakelijkheid van software-bedrijven te verzekeren.
Door middel van het treffen van voldoende preventieve maatregelen kunnen de risico's worden verkleind dat software-bedrijven aansprakelijk worden gesteld. De EDP-auditor zou hierbij zowel een beoordelende als een adviserende rol kunnen spelen, met name indien hij gespecialiseerd is in software-ontwikkelingsprocessen. Verderop in dit artikel wordt hierop nader ingegaan.

GRONDEN VAN AANSPRAKELIJKHEID (WANPRESTATIE OF ONRECHTMATIGE DAAD)

Software-bedrijven kunnen aansprakelijk worden gesteld op grond van wanprestatie (art. 6:74 BW) of op grond van onrechtmatige daad (art. 6:162 BW).[2] Wanprestatie wordt in de wet omschreven als een toerekenbare tekortkoming in de nakoming van een verbintenis. Daarvan is sprake indien de leverancier niet, niet tijdig of niet behoorlijk heeft gepresteerd. Het kan bijvoorbeeld gaan om het uit de hand lopen van de kosten van een project als gevolg van een fout van de adviseur bij het opstellen van een tijdschema en/of begroting.
Van een onrechtmatige daad is sprake indien wordt gehandeld in strijd met de maatschappelijke zorgvuldigheid. Gedacht kan worden aan een onzorgvuldige of onwettige verkrijging, verwerking of verstrekking van gegevens en informatie, of aan het in het verkeer brengen van ondeugdelijke produkten.

Voor de aansprakelijkheid op grond van wanprestatie is het onderscheid tussen inspannings- en resultaatsverbintenis van belang. In geval van een inspanningsverbintenis verplicht de schuldenaar zich tot het betrachten van een zekere inspanning tot het bereiken van een zeker resultaat. De schuldenaar is aansprakelijk als hij onvoldoende inspanning heeft verricht. In geval van een resultaatsverbintenis verplicht de schuldenaar zich tot het tot stand brengen van het resultaat zelf. De schuldenaar is aansprakelijk als het resultaat zelf is uitgebleven.
Het verschil tussen inspannings- en resultaatsverbintenis is vooral van betekenis voor de verdeling van de bewijslast. Bij een inspanningsverbintenis moet de cliënt bewijzen dat het software-bedrijf een fout heeft gemaakt, die een goede beroepsbeoefenaar in de gegeven omstandigheden niet zou hebben gemaakt. Bij een resultaatsverbintenis leidt het uitblijven van de beoogde resultaten in beginsel tot een vermoeden van aansprakelijkheid van het software-bedrijf, en moet het software-bedrijf overmacht bewijzen (bewijzen dat de tekortkoming niet toerekenbaar is) [Stuu86-1].

Resultaats- of inspanningsverbintenis?

In de literatuur zijn de meningen verdeeld over de vraag of een overeenkomst tussen een software-bedrijf en een cliënt moet worden gekwalificeerd als een resultaats- of als een inspanningsverbintenis. Vandenberghe bijvoorbeeld was van mening dat software-contracten tot de categorie resultaatsverbintenissen moeten worden gerekend [Vand84]. Het belangrijkste argument dat hij daarvoor aanvoerde is dat anders de opdrachtgever de zwaarste lasten zou moeten dragen hoewel hij als ondeskundige de zwakste partij is. Hij is de zwakste partij zowel met betrekking tot het beoordelen van de risico's, als met betrekking tot het leveren van het bewijs van een fout van de adviseur. Automatiseringsprojecten behoren immers niet tot de alledaagse praktijk van de opdrachtgever. Stuurman is echter een andere mening toegedaan. Hij typeert het contract tussen een software-adviseur en de cliënt als een inspanningsverbintenis. Zijn belangrijkste motivatie hiervoor is dat het de opdrachtgever is die uiteindelijk beslist, zij het op basis van de opties aangedragen door de adviseur [Stuu86-1].
Insinger en Pot-Merlin stellen dat de verplichting van de leverancier een quasi-resultaatsverbintenis is wanneer hij standaardwerk levert. Wanneer hij maatwerk levert heeft hij een inspanningsverbintenis. Voor de adviseur geldt volgens hen dat hij of zij een inspanningsverplichting heeft [InPo87].
Beredeneerd kan worden dat de kwalificatie van inspannings- dan wel resultaatsverbintenis afhangt van de soort prestatie die is overeengekomen en de mate waarin het te bereiken resultaat of te geven advies is gespecificeerd. Is bijvoorbeeld levering van een standaard-software-pakket voorwerp van de overeenkomst, dan zal eerder sprake zijn van een resultaatsverbintenis, dan wanneer het om een adviesovereenkomst gaat. Echter, de opdracht tot levering van een maatwerk-softwarepakket of de opdracht tot het uitbrengen van een advies kan dermate gespecificeerd zijn dat ook deze als een resultaatsverbintenis zijn te kwalificeren. Overigens vloeien uit een overeenkomst niet louter resultaats- of inspanningsverbintenissen voort; het betreft steeds een bundel verbintenissen, waarvan sommige een resultaats- en andere een inspanningskarakter dragen.

CRITERIA VOOR AANSPRAKELIJKSTELLING

In de jurisprudentie en literatuur zijn criteria ontwikkeld op grond waarvan software-bedrijven aansprakelijk kunnen worden gesteld.
Eén van de belangrijkste uitspraken die de laatste jaren is gedaan, is het arrest Brinkers/RBC [Comp84].
In deze procedure werd een automatiseringsadviseur aansprakelijk geacht voor een onjuist advies. RBC had aan Brinkers advies uitgebracht over automatisering van de bedrijfsvoering, die vooral handelsactiviteiten betrof. Het had Brinkers geadviseerd tot aanschaf van een minicomputer met directe overschakeling van de bestaande gegevensverwerking in de oude computer op de nieuwe computer. Het nieuwe computersysteem functioneerde zeer gebrekkig. Er ontstond grote achterstand in de administratie bij Brinkers en er werd een aanzienlijke schade geleden. Brinkers stelde een vordering tot schadevergoeding in van bijna 2 miljoen gulden. Het Hof stelde dat *'het voor de beoordeling van de vraag of door RBC wanprestatie is gepleegd beslissend is of het advies - mede gelet op de gegevens omtrent de gang van zaken in het bedrijf van Brinkers die RBC ten tijde van het geven van het advies ter beschikking stonden - al of niet voldeed aan de mate van zorgvuldigheid en deskundigheid die van een redelijk handelend en bekwaam automatiseringsdeskundige geëist mag worden'.*

Gezien de grote belangen die op het spel stonden, mocht van een zorgvuldig handelend adviseur

1 *Verzekeringen tegen materiële schade aan eigen computerapparatuur en computerfraudeverzekeringen zijn al vrij lang op de markt aanwezig.*

2 *Ook andere aansprakelijkheidsgronden zijn denkbaar, zoals zaakwaarneming. Zaakwaarneming is het zich willens en wetens en op redelijke grond inlaten met de behartiging van eens anders belang, zonder de bevoegdheid daartoe aan een rechtshandeling of een elders in de wet geregelde rechtsverhouding te ontlenen (art. 6:198 BW). Aansprakelijkstelling op basis van deze grond zal zich niet vaak voordoen.*

worden verwacht dat hij, alvorens zijn advies uit te brengen, een deugdelijk onderzoek instelde naar de structuur van het bedrijf. Dit ondanks het feit dat Brinkers op grote spoed aandrong.
De schending van de onderzoeksplicht en waarschuwingsplicht vormen de belangrijkste gronden voor de conclusie van het Hof dat RBC heeft gehandeld in strijd met de zorgvuldigheid die van een deskundig adviseur mag worden geëist. In casu had de adviseur een diepgaand onderzoek naar de bedrijfsstructuur van Brinkers moeten instellen en Brinkers expliciet duidelijk moeten waarschuwen voor dreigende risico's, zelfs ondanks het feit dat de opdrachtgever uitdrukkelijk haastwerk eiste. Op de adviseur rust ten aanzien van de onderzoeks- en waarschuwingsplicht een zware verantwoordelijkheid.
Een ander arrest dat betrekking heeft op mislukte automatisering, is het arrest Blommestein/ICL [Comp86]. De overeenkomsten tussen Blommestein en ICL strekten mede ertoe dat een standaardprogramma voor de groothandel werd aangepast aan de administratieve wensen van Blommesteins bedrijf. Een dergelijke aanpassing vereist veel inzet aan de zijde van het bedrijf waarvan de automatisering wordt gewenst. Blommestein heeft echter in dit opzicht minimale medewerking verleend, zo oordeelde de rechtbank, en onvoldoende gezorgd voor de aanwezigheid van geschoold personeel.

Uit het centrale criterium voor de aansprakelijkstelling van software-bedrijven, namelijk de zorgvuldigheid en deskundigheid die van een redelijk handelend en bekwaam automatiseringsdeskundige mag worden geëist, worden in de literatuur een aantal concrete verplichtingen afgeleid [Stuu86-2].

Voor software-bedrijven is een BAV het meest geschikt omdat de aansprakelijkheidsrisico's zich vooral uiten in financiële risico's, in het bijzonder vermogensschade.

De deskundige dient vakbekwaam te zijn, te onderkennen dat hij een eigen verantwoordelijkheid heeft tegenover zijn cliënt, hij moet zorgvuldig eigenbelang en het belang van de cliënt scheiden en tijdig naar andere specialisten verwijzen als zijn kennis tekort schiet. Ten slotte heeft hij een informatieplicht: de deskundige dient zijn cliënt zo volledig mogelijk te informeren over eventuele risico's en over alle aspecten met betrekking tot de opdracht. Tevens zal hij zelf zich maximaal moeten inspannen om alle relevante informatie bijeen te garen.

Het centrale criterium voor het aansprakelijk stellen van software-bedrijven uit de jurisprudentie is dus 'de zorgvuldigheid en deskundigheid die van een redelijk handelend en bekwaam automatiseringsdeskundige geëist mag worden'. De belangrijkste verplichtingen die hieruit kunnen worden afgeleid, zijn voor een automatiseringsdeskundige de onderzoeksplicht en waarschuwingsplicht, en voor de gebruiker de medewerkingsplicht. Ook voor EDP-auditors kan het van belang zijn dat ze zich bewust zijn van deze verplichtingen en daar in de dagelijkse praktijk rekening mee houden.

VERZEKERING VAN AANSPRAKELIJKHEID

In de vorige paragraaf zijn de gronden van en de criteria voor aansprakelijkstelling behandeld. In deze paragraaf komt de verzekering van het risico van aansprakelijkstelling aan de orde. Bedrijven dienen de nodige voorzorgsmaatregelen te treffen om het vermogen van de ondernemingen te beschermen voor het geval ze aansprakelijk worden gesteld. Die voorzorgsmaatregelen kunnen, naast maatregelen van technische, organisatorische en juridische aard, bestaan uit het afsluiten van verzekeringen.
In de Inleiding is gesteld dat voor software-bedrijven een beroepsaansprakelijkheidsverzekering het meest geschikt is, omdat de aansprakelijkheidsrisico's zich vooral uiten in financiële risico's, in het bijzonder vermogensschade. Een BAV dekt de aansprakelijkheid voor zuivere vermogensschade veroorzaakt door beroepsfouten. Persoonsschade of schade aan goederen wordt door een BAV niet gedekt.
Er zijn slechts enkele verzekeringsmaatschappijen in Nederland die een BAV aan software-bedrijven aanbieden (Bloemers, Haagman, Nationale Nederlanden, Kröller & Co, Hudig-Langeveldt en Chubb). De meeste verzekeraars bieden (nog) geen BAV aan, omdat ze niet voldoende inzicht hebben in de risicofactoren en omdat de financiële schade enorm hoog kan oplopen. Naar mijn mening kunnen de risico's worden beperkt door het treffen van preventieve maatregelen. Door na te gaan wat de oorzaak is van de fouten die tot beroepsaansprakelijkheid leiden, kunnen deze preventieve maatregelen daarop worden afgestemd en eventueel in de verzekeringsvoorwaarden worden opgenomen. Zo kunnen de risico's enigszins in de hand worden gehouden.
Navolgend wordt eerst nagegaan onder welke voorwaarden BAV's op de Nederlandse markt worden aangeboden. Daarna wordt, aan de hand van een inventarisatie van de risicofactoren, nagegaan welke verzekeringsmogelijkheden er nog open liggen. Met andere woorden, onder welke voorwaarden BAV's zouden kunnen worden aangeboden die beter tegemoet komen aan de verzekeringsbehoeften. Het blijkt bijvoorbeeld dat overschrijding van levertijden een belangrijke aansprakelijkheidsgrond is. Door veel verzekeringen wordt deze aansprakelijkheidsgrond juist van dekking uitgesloten. Als verzekeringsvoorwaarde zou dan gesteld kunnen worden dat bijvoorbeeld voorafgaand een projectdiagnose wordt gesteld of een vorm van risico-management wordt toegepast. Op deze laatste twee termen wordt nog teruggekomen.

Aangeboden beroepsaansprakelijkheidsverzekeringen

Zoals gezegd zijn er slechts enkele Nederlandse verzekeraars die een BAV aan software-bedrijven aanbieden. Hun polissen verzekeren 'de aansprakelijkheid van de verzekerde voor door derden geleden schade veroorzaakt door een fout van de verzekerde'. Onder beroepsfout wordt meestal verstaan: 'vergissingen, onachtzaamheden, nalatigheden, verzuimen, onjuiste adviezen of dergelijke fouten begaan bij werkzaamheden die de verzekerde ten dienste van derden heeft verricht'.

De meeste verzekeringen bieden geen dekking voor de aansprakelijkheid voor schade die betrekking heeft op hardware, tenzij de aansprakelijkheid direct voortvloeit uit de door verzekerde ontwikkelde en/of geadviseerde software. Geen enkele verzekering dekt schade ten gevolge van inbreuk op intellectuele eigendomsrechten, waaronder schending van auteursrechten, licenties en het wederrechtelijk kopiëren van programma's.
Met uitzondering van één polis wordt ook niet gedekt de aansprakelijkheid ten gevolge van het niet of niet tijdig nakomen van verplichtingen uit een overeenkomst. Dit is opmerkelijk, nu de overschrijding van levertijden een belangrijke aansprakelijkheidsgrond blijkt te zijn.
Vier van de vijf polissen dekken niet de aansprakelijkheid voortvloeiende uit een boete-, schadevergoedings-, garantie-, vrijwarings- of soortgelijk beding, behalve indien en voor zover de aansprakelijkheid ook zou hebben bestaan zonder deze uitsluitingen.
Een laatste uitsluiting betreft nog de aanspraak op het honorarium, salaris, verschotten en onkosten van de verzekerde zelf, indien hij deze ten gevolge van een door hem gemaakte fout niet aan zijn cliënt in rekening kan brengen, of deze cliënt het recht heeft deze van hem terug te vorderen.
Overigens is dit niet een volledige opsomming van gehanteerde uitsluitingen. Alleen de meest gebruikelijke, en voor een BAV de meest typerende, uitsluitingen zijn hier genoemd.

De meeste polissen worden in beginsel gesloten op claims-made basis, eventueel gecombineerd met het act-committed systeem. Claims-made basis wil zeggen dat dekking wordt geboden wanneer de aanspraak binnen de looptijd van de verzekering is gemeld, ongeacht wanneer de fout is gemaakt. In het act-committed systeem moet niet alleen de claim zijn ingesteld binnen de looptijd van de verzekering, maar ook de fout die tot de claim aanleiding heeft gegeven, moet in die periode zijn gemaakt. Eén polis dekt alleen de schade die ontstaat na zes maanden na de levering van niet-standaardpakketten, wat enigszins bevreemding wekt omdat de meeste schade ontstaat in de eerste maanden direct na de levering. Het zogenaamde narisico wordt door drie polissen gedekt. Narisico heeft betrekking op aanspraken voortvloeiend uit omstandigheden die tijdens de contractduur van de verzekering schriftelijk ter kennis van de verzekeraar zijn gebracht, maar die pas na beëindiging van de verzekeringsovereenkomst tot een daadwerkelijke claim leiden.

De verzekeringen bieden alleen dekking voor fouten binnen Nederland begaan of gemaakt bij de uitvoering van opdrachten voor binnen Europa gevestigde opdrachtgevers. Wordt de aanspraak ingesteld in de Verenigde Staten of Canada, dan wel is deze onderworpen aan het recht van de Verenigde Staten of Canada, dan geeft de verzekering geen dekking. De reden hiervoor is dat in de Verenigde Staten en Canada men sneller geneigd is claims in te stellen en dat de claims veel hoger zijn dan in Nederland en de rest van Europa.

Een vergelijking met de verzekeringen voor advocaten, artsen en notarissen leert dat de verzekeringsvoorwaarden in sterke mate overeenkomen [Duth92]. Dit is opmerkelijk, aangezien de risico's van advocaten, artsen en notarissen enerzijds en automatiseerders anderzijds, verschillend zijn.
Kunnen advocaten, artsen en notarissen zelf de risico's in zeker opzicht in de hand houden, software-bedrijven hebben die mogelijkheid in veel beperktere mate. De eerste beroepsbeoefenaars kunnen meestal zelf de risico's inschatten en deze meedelen aan de cliënt/patiënt, waarna de cliënt/patiënt zelf kan beslissen of bijvoorbeeld wel of niet tot handelen moet worden overgegaan. Ze kunnen alle voors en tegens op een rijtje zetten en de kans op een geslaagd resultaat redelijk inschatten. Advocaten en notarissen kunnen, door onder andere het volgen van de wettelijke kaders, zelf meer invloed uitoefenen op het risico.
De kans dat software-bedrijven fouten maken is veel groter. Er zit praktisch altijd wel een zogenaamde 'bug' in het programma; het blijkt moeilijk te zijn automatiseringsprojecten te budgetteren en het blijkt dat het slagen van automatiseringsprojecten vaak afhangt van menselijke factoren, waarop de software-bedrijven veel moeilijker invloed kunnen uitoefenen. Dat toch min of meer dezelfde verzekeringsvoorwaarden worden gehanteerd, wekt - in het licht van het bovenstaande - verwondering.
Kennelijk hebben verzekeraars de polissen voor advocaten, artsen en notarissen min of meer gekopieerd voor software-bedrijven, met hier en daar wat aanpassingen. Daarbij kan een rol hebben gespeeld dat advocaten, artsen en notarissen enerzijds en software-bedrijven anderzijds op grond van dezelfde criteria aansprakelijk kunnen worden gesteld. Dit is ook met zoveel woorden in het eerder genoemde arrest Brinkers/RBC door de Hoge Raad bepaald.
Dit is een aanwijzing dat de verzekeringsmogelijkheden voor software-bedrijven nog niet zijn uitgekristalliseerd en meer toegesneden zouden kunnen worden op software-bedrijven.

Mogelijke beroepsaansprakelijkheidsverzekeringen

Voordat op de mogelijke beroepsaansprakelijkheidsverzekeringen wordt ingegaan, wordt eerst nagegaan welke factoren van invloed zijn op de risico's van automatiseerders.

Deze factoren zijn onder te verdelen in drie groepen, namelijk factoren die betrekking hebben op menselijke, organisatorische achtergronden, factoren die te maken hebben met kostenbeheersing en

budgettering, en factoren die voortvloeien uit onvoldoende projectdiagnose of risico-management.

Risicofactoren
De eerste groep van factoren speelt vooral een rol in de sociaal-organisatorische context van de gebruikersorganisatie. Uit onderzoek van onder anderen De Brabander en Thiers is gebleken dat de cruciale factor in het tot stand komen van succesvolle informatiesystemen was gelegen in het feit of de managers op effectieve wijze konden worden betrokken bij de ontwikkeling van systemen [BrTh85]. Metze noemt als belangrijkste redenen voor de problemen rond automatisering dat men in de ontwerpfase niet goed specificeert wat het systeem moet doen, dat de gebruiker onvoldoende wordt betrokken bij de keuze van de configuratie en de opbouw van de programmatuur en dat te vaak deelsystemen worden ontwikkeld zonder voldoende samenhang [Metz90]. Hij stelt dat automatisering te lang in handen van deskundigen is geweest en dat het tijd is meer en beter rekening te houden met de wensen, mogelijkheden, kennis en behoeften van de gebruiker. De verzekeraar zou kunnen vragen op welke wijze de gebruiker wordt betrokken bij het tot stand komen van informatiesystemen en zou hier een verzekeringsvoorwaarde aan kunnen verbinden, bijvoorbeeld dat het software-bedrijf erop toeziet dat gebruikers in voldoende mate worden betrokken bij de ontwikkeling van systemen. De EDP-auditor zou het software-bedrijf hierin kunnen adviseren en eventueel aan de verzekeraar een verklaring kunnen afgeven zowel met betrekking tot het stelsel van te treffen maatregelen voor een effectieve communicatie (vooraf) als met betrekking tot het naleven van de getroffen maatregelen (achteraf).

Verzekeraars zouden door het opnemen in de verzekeringsvoorwaarden van de verplichting tot het treffen van voorzorgsmaatregelen, de dekking van de bestaande BAV's kunnen uitbreiden.

De tweede groep factoren, kostenbeheersing en budgettering, heeft te maken met het feit dat forse overschrijdingen van budgetten bij het ontwikkelen van geautomatiseerde informatiesystemen eerder regel dan uitzondering zijn. Siskens, Heemstra en Van der Stelt hebben onderzoek gedaan naar de stand van zaken bij het beheersen c.q. begroten van automatiseringsprojecten in Nederland [Sisk91]. De belangrijkste conclusies uit dit onderzoek zijn dat 35 procent van de responderende organisaties geen begrotingen opstelt voor automatiseringsprojecten. 65 procent zegt wel te begroten, maar 62 procent baseert de begroting mede op intuïtie en ervaring. 50 procent van de organisaties die gereageerd hebben, registreert niets van een automatiseringsproject in uitvoering en 57 procent van de responderende organisaties geeft te kennen niet na te calculeren. Dit betekent dat meer dan de helft van de organisaties geen idee heeft van de bestede middelen. Slechts 16 procent van degenen die begroten, maakt hierbij gebruik van een begrotingsmodel. Van de 51 modelgebruikers zijn er 18 die niet nacalculeren. Het gebruik maken van begrotingsmodellen, het überhaupt begroten van automatiseringsprojecten en het nacalculeren kunnen belangrijke instrumenten zijn om de kostenoverschrijdingen in de hand te houden. Dit is een belangrijke vingerwijzing voor verzekeraars. Zij kunnen in hun verzekeringsvoorwaarden de verplichting van begroten en narekenen opnemen. Bij nietnakoming van deze verplichting zouden ze als sanctie kunnen stellen dat in geval van schade niet behoeft te worden uitgekeerd. Tevens zou door de EDP-auditor (jaarlijks) een verklaring kunnen worden afgegeven dat deze verplichtingen in voldoende mate zijn nagekomen. Twee momenten zijn daarbij te onderscheiden: het afgeven van een verklaring door de EDP-auditor dat maatregelen zijn getroffen voor het opstellen van een begroting en narekening, en het afgeven van een verklaring door de EDP-auditor dat deze maatregelen ook daadwerkelijk zijn nageleefd.

De derde groep van factoren, projectdiagnose en risico-management, heeft te maken met het feit dat veel mislukkingen bij automatiseringsprojecten zijn terug te voeren op onvoldoende analyse van de risico's of onvoldoende openheid van opdrachtgever en projectleider over deze risico's.
Met projectdiagnose wordt bedoeld het onderzoek naar de omstandigheden waaronder een automatiseringsproject wordt gestart. Een projectdiagnose kan snel inzicht geven in de risico's die het verloop van het project nadelig kunnen beïnvloeden. Onder risico-management is te verstaan het bewust nemen van een permanent en evenwichtig pakket van maatregelen die risico's tot een minimum beperken, het blijven toetsen van de genomen maatregelen aan de opgetreden risico's en het voortdurend bijstellen van het pakket van maatregelen zodat het optreden van risico's tot een minimum beperkt blijft.
Een noodzakelijke aanvulling op een goede begroting en rekening bestaat dan ook uit het bewaken van de voortgang, het onderkennen van de risico's en het beheersen van de risico's.
Verzekeraars zouden als voorwaarde kunnen stellen dat een projectdiagnose en methoden van risico-management worden toegepast. Blijkt in geval van schade dat aan deze voorwaarde niet is voldaan, dan zouden ze als sanctie kunnen stellen dat niet hoeft te worden uitgekeerd. Ook hier zou de EDP-auditor kunnen worden ingeschakeld, door hem (jaarlijks) een verklaring te laten afgeven dat aan deze voorwaarde is voldaan, zowel vooraf dat maatregelen zijn getroffen voor het opstellen van een projectdiagnose en het toepassen van risicomanagement als achteraf dat deze maatregelen daadwerkelijk en in voldoende mate zijn nageleefd.

Naast de drie genoemde groepen zijn er nog factoren die niet zozeer als oorzaak zijn aan te wijzen

van het slagen of falen van automatiseringsprojecten, maar die er wel verband mee houden. Daarbij kan worden gedacht aan de omvang van het project, de grootte van de gebruikersorganisatie, de aard van de bedrijfstak, het soort toepassingsgebied, de omvang van het software-bedrijf, het type automatiseringsvoorzieningen, etc.

Gemiste kansen
Hiervoor is duidelijk gemaakt wat de risicofactoren zijn voor software-bedrijven. Nu meer inzicht in deze factoren is verkregen, kunnen voorzorgsmaatregelen daarop worden afgestemd. Verzekeraars zouden door het in de verzekeringsvoorwaarden opnemen van de verplichting tot het treffen van voorzorgsmaatregelen, zoals het toepassen van een projectdiagnose en risico-management, het opstellen van een begroting en de toepassing van nacalculatie, de dekking van de bestaande beroepsaansprakelijkheidsverzekeringen kunnen uitbreiden. Indien deze verplichting niet wordt nagekomen, kan als sanctie worden gesteld dat in geval van schade niet wordt uitgekeerd. Wordt nu nog vaak de overschrijding van leveringstermijnen van de verzekering uitgesloten, op deze manier zou dat onder de dekking kunnen worden opgenomen. Zo kan beter tegemoet worden gekomen aan de verzekeringsbehoeften van software-bedrijven.

SAMENVATTING EN CONCLUSIE

De beroepsaansprakelijkheidsverzekering voor software-bedrijven staat nog in de kinderschoenen. De drempel voor verzekeraars om een dergelijke verzekering aan software-bedrijven aan te bieden is zeer hoog omdat ze geen of weinig inzicht hebben in de risicofactoren en in de hoogte en frequentie van de schadeclaims die uit beroepsfouten kunnen voortvloeien. Software-bedrijven kunnen voor beroepsfouten aansprakelijk worden gesteld.
Een manier om het risico aansprakelijk gesteld te worden af te wentelen, is het afsluiten van een BAV. Een BAV beschermt het vermogen van de verzekerde tegen eventuele schadeclaims. Zij vergoedt alleen vermogensschade, dat wil zeggen financiële schade zonder dat er sprake is van een inleidende materiële beschadiging.
In dit artikel is nagegaan in hoeverre in Nederland beroepsaansprakelijkheidsrisico's van software-bedrijven verzekerbaar zijn.

Vooraf is beschreven op grond van welke criteria uit de wet, literatuur en jurisprudentie, software-bedrijven aansprakelijk kunnen worden gesteld. Het centrale criterium voor de aansprakelijkstelling van software-bedrijven was: de zorgvuldigheid en deskundigheid die van een redelijk handelend en bekwaam automatiseringsdeskundige mag worden geëist. Hieruit is een aantal concrete verplichtingen afgeleid, waaronder een onderzoeks- en waarschuwingsplicht van de automatiseringsdeskundige en een medewerkingsplicht van de gebruiker.

Vervolgens is nagegaan onder welke voorwaarden BAV's reeds worden aangeboden. De polissen van de BAV's die in Nederland worden aangeboden, dekken alle 'de aansprakelijkheid van de verzekerde voor door derden geleden schade veroorzaakt door een fout van de verzekerde'. Onder fout wordt meestal verstaan: 'vergissingen, onachtzaamheden, nalatigheden, verzuimen, onjuiste adviezen of dergelijke fouten begaan bij werkzaamheden die de verzekerde ten dienste van derden heeft verricht'.
Geen enkele verzekering dekt schade als gevolg van inbreuk op intellectuele eigendomsrechten en de meeste verzekeringen dekken ook niet aansprakelijkheid ten gevolge van het niet of niet tijdig nakomen van verplichtingen uit een overeenkomst.

Daarna is aan de hand van een inventarisatie van mogelijke risicofactoren nagegaan welke mogelijkheden tot het verzekeren van beroepsaansprakelijkheidsrisico's er nog zijn die nog niet worden benut: de zogenaamde gemiste kansen.
De belangrijkste factoren die van invloed zijn op de risico's, hebben betrekking op een al dan niet effectieve communicatie tussen de informaticadeskundigen en de eindgebruiker, het al dan niet opstellen van een begroting of nacalculeren, en het al of niet toepassen van een projectdiagnose en risicomanagement. Verzekeraars zouden bepaalde eisen in hun verzekeringsvoorwaarden kunnen opnemen, zoals het toepassen van een projectdiagnose en het gebruik maken van begrotingsmodellen. Hieraan gekoppeld kan de bepaling worden opgenomen dat als blijkt dat in geval van schade niet aan deze eisen is voldaan, de verzekeraar niet verplicht is uit te keren. Op deze manier kunnen de bestaande verzekeringsmogelijkheden voor software-bedrijven worden uitgebreid. In de voorwaarden moet dan wel duidelijk worden omschreven wat wordt verstaan onder 'bepaalde voorwaarden' en wanneer er sprake is van 'voldoende'. De EDP-auditor zou hierin zowel een adviserende als een beoordelende rol kunnen spelen. De auditor zou kunnen aangeven wanneer er sprake is van 'voldoende' maatregelen en zou 'goedkeurende verklaringen' kunnen afgeven over het stelsel van te treffen maatregelen (vooraf) en over de daadwerkelijke naleving van deze maatregelen (achteraf).

Het doel van dit artikel was na te gaan of en in hoeverre beroepsaansprakelijkheidsrisico's van software-bedrijven in Nederland verzekerbaar zijn. Geconstateerd is dat er inderdaad BAV's in Nederland aan software-bedrijven worden aangeboden, maar dat ze meer toegesneden kunnen worden op de speciale beroepsgroep van software-bedrijven. De mogelijkheden daartoe zijn in dit artikel aan de orde gesteld.

Mw. mr.drs. A.W. Duthler · Is sinds februari 1993 werkzaam bij KPMG Klynveld EDP Auditors als adviseur informaticarecht. In deze functie houdt zij zich bezig met de juridische aspecten van automatisering en de connecties daarvan met EDP-auditing. Tot haar werkzaamheden behoren onder andere het beoordelen van automatiseringscontracten, het adviseren inzake privacy-wetgeving, de Wet cmputercriminaliteit en EDI. Zij studeerde Bestuurskunde aan de Technische Universiteit Twente en Rechten aan de Rijksuniversiteit Leiden.

LITERATUUR

[BrTh85] B. de Brabander en G. Thiers, *Een onderzoek naar de factoren die het succes van automatiseringsprojecten beïnvloeden*, Informatie jaargang 25, nr. 12, p. 13-21, 1985.

[Comp84] Hof 's-Gravenhage, 8 maart 1984, Computerrecht 1984/2.

[Comp86] Rb 's-Gravenhage, 26 maart 1986, Computerrecht 1986/3.

[DeBa90] B.W. Degens en C.M.B.J. Bakker, *De zin van de polis, een onderzoek naar de mogelijkheden van en de behoefte aan beroepsaansprakelijkheidsverzekeringen voor softwarebureaus*, oktober 1990, interne publikatie Universiteit Twente.

[Duth92] A.W. Duthler, *De verzekerbaarheid van automatiseringsrisico's, Een onderzoek naar de verzekerbaarheid van beroepsaansprakelijkheidsrisico's van software-bedrijven in Nederland*, afstudeerrapport voor de faculteit der Rechtsgeleerdheid aan de Rijksuniversiteit Leiden, november 1992.

[Fran92] H. Franken, *Recht en computer*, Kluwer Deventer, 2e druk, p. 80.

[InPo87] R.C. Insinger en P. Pot-Merlin, *De verzekerbaarheid van computerrisico's*, Computerrecht 1987/4.

[Metz90] M. Metze, *Hoe nu verder met de automatisering?*, Intermagazine januari/februari 1990, nr. 1/2.

[Sisk91] W.J.A. Siskens, F.J. Heemstra en H. van der Stelt, *Kostenbeheersing bij automatiseringsprojecten: een empirisch onderzoek*, Informatie jaargang 31, nr. 1, p. 34-43.

[Stuu86-1] C. Stuurman, *De aansprakelijkheid van de automatiseringsadviseur*, Computerrecht 1986/3.

[Stuu86-2] C. Stuurman, *Aansprakelijkheid en automatisering, de positie van de adviseur*, Vermande, 1986.

[Vand84] G.P.V. Vandenberghe, *Partijenaansprakelijkheid bij softwarecontracten*, Kluwer, Deventer 1984.

[Wans87] J.H. Wansink, *De algemene aansprakelijkheidsverzekering*, dissertatie Rotterdam, 1987, p. 39.

Beveiligingsstandaard voor informatiesystemen

Prof.dr.ir. R. Paans RE

Het belang van een beveiligingsstandaard voor informatiesystemen wordt allerwege onderkend. Paans geeft aan op welke wijze bij IBM deze problematiek is aangepakt en heeft bijgedragen aan een verhoging van het beveiligingsniveau.

INLEIDING

De bestaande internationale standaarden voor computerbeveiliging, zoals het *Orange Book* van het Amerikaanse ministerie van Defensie [DoD83] en *Information Technology Security* van de Europese Gemeenschap [ITSE91, ITSE92], hebben een zeer beperkt geldigheidsgebied. Zo richten de DoD-criteria zich op de *Trusted Computing Base*, die de centrale apparatuur, het besturingssysteem en de logische toegangsbeveiliging omvat. Een classificatie zoals C2 *(discretionary access control)* en B1 *(mandatory access control)* heeft alleen betrekking op de kern van een informatiesysteem, namelijk de machines in de computerzaal en een deel van de programmatuur die op magneetband van de leverancier wordt ontvangen. Vele andere componenten die van vitaal belang zijn voor de uiteindelijke bescherming van informatiesystemen en gegevens, worden buiten beschouwing gelaten: dit zijn bijvoorbeeld de lokale modificaties van het besturingssysteem, programmapakketten, toepassingsprogrammatuur, netwerken, technische infrastructuur, organisatie, procedures en fysieke bescherming. Hierdoor leveren deze internationale standaarden slechts een geringe toegevoegde waarde voor het management van de automatisering, de beveiligingsmedewerkers en de EDP-auditors.

Aangezien men zowel voor de beveiliging van rekencentra als voor de controle op de compleetheid en doelmatigheid van de beveiligingsmaatregelen eenduidige normen nodig heeft, is door IBM een internationale werkgroep ingesteld. Hierin participeerden beveiligingsdeskundigen van alle Operating Units, onder anderen de schrijver van dit artikel namens IBM Europe Information Systems. De groep had als opdracht het inventariseren van de bestaande normen, het onderkennen van maatregelen die als bureaucratisch werden ervaren door de gebruikers, en het opstellen van normen die passen binnen de huidige organisatie en aansluiten bij de huidige stand der techniek. Dit overleg heeft geresulteerd in het document *'Information Security Standards for Providers of Information Systems Ser-vices'* [IBM92], dat nu als Information and Telecommunication Systems-standaard I&TCS 200 is geaccepteerd door alle IBM-organisaties wereldwijd. Deze standaard heeft geleid tot het ontwikkelen van interne beveiligingsprodukten, die te zamen met nieuwe procedures worden geïmplementeerd in alle interne rekencentra. Daarnaast dient I&TCS 200 als toetsingsnorm voor de interne EDP-audits. Op deze wijze vormt het een richtlijn voor managers en medewerkers binnen de automatisering, en een basis voor de interne audit-programma's.

De standaard omvat de fysieke en logische toegangsbeveiliging voor mainframes, middelgrote systemen en netwerken, inclusief de verantwoordelijkheden van gebruikers en beheerders, en regels voor de externe netwerkverbindingen, printers en niet-reguliere medewerkers. Deze regels worden in de volgende paragrafen besproken. Een nieuwe werkgroep ontwikkelt momenteel de standaard I&TCS 201 voor de *Local Area Network* (LAN)-omgeving.

FYSIEKE TOEGANGSBEVEILIGING

In het verleden werden de grotere computers geplaatst in zalen met een afdoende fysieke toegangsbeveiliging, de *restricted areas*, die bijna werden beschermd als goudkluizen. Nu steeds meer grote en middelgrote systemen decentraal worden opgesteld, ontstaat de noodzaak tot meer differentiatie bij het treffen van kostbare beveiligingsmaatregelen. Deze maatregelen moeten in balans zijn met de waarde van de te beschermen systemen en gegevens. Hiervoor is via I&TCS 200 een classificatie van de systemen ingevoerd, gebaseerd op:

- De hoogste gegevensclassificatie die wordt toegestaan binnen het systeem. Dit is ter beoordeling van de systeembeheerder; deze beheerder dient passende preventieve maatregelen te treffen, zoals het installeren van encryptiefaciliteiten voor het opslaan van gegevens met een hogere classificatie dan Confidential. Bovendien moet de beheerder de gebruikers inlichten, bijvoorbeeld door op het logon-scherm te vermelden: 'op dit systeem mogen geen gegevens met een hogere classificatie dan Confidential worden verwerkt of opgeslagen' of 'geheime gegevens mogen worden verwerkt, maar dienen versleuteld te worden opgeslagen'.

Nu steeds meer grote en middelgrote systemen decentraal worden opgesteld, ontstaat de noodzaak tot meer differentiatie bij het treffen van kostbare beveiligingsmaatregelen.

- De waarde van het informatiesysteem voor de zakelijke processen. Zo bevat een computer die het internationale netwerk bestuurt slechts laag-geclassificeerde informatie, maar is van vitaal belang voor de gehele internationale informatie-uitwisseling.

- De waarde van de apparatuur. Dit betreft met name de kosten en gevolgen voor het bedrijf bij verlies of beschadiging. Zo zal men een mainframe met randapparatuur ter waarde van 50 miljoen gulden, zelfs als daarop alleen ongeclassificeerde gegevens worden verwerkt, op dezelfde wijze beschermen als een systeem waarop geheime gegevens worden verwerkt.

Voor het tweede en derde punt is de besluitvorming afhankelijk van de lokale situatie binnen een bedrijfsonderdeel. Vandaar dat deskundigen een advies opstellen, waarna de Directeur Automatisering de classificatie van een systeem of van een groep systemen binnen een rekencentrum vaststelt. Afhankelijk van deze beslissing kunnen de systemen geplaatst worden in:
- ruimten toegankelijk voor publiek (alleen voor Unclassified-gegevens);
- interne ruimten die alleen toegankelijk zijn voor medewerkers (voor Internal Use-gegevens);
- afgesloten ruimten waarbij een beheerder expliciet medewerkers moet autoriseren voor toegang (voor Confidential-gegevens);
- afgesloten ruimten met elektronische toegangscontrole, beveiligde nooduitgangen, wanden die van betonnen vloer tot betonnen plafond lopen, geen buitenramen op de begane grond, begeleiding en registratie van extern onderhoudspersoneel, enz. (voor hoger geclassificeerde gegevens).

Een ander aandachtspunt is de procedure voor opslagmedia, onder andere gericht op de draagbare media (magneetbanden, floppy disks, enz.). Zo worden richtlijnen verstrekt voor classificatie van de draagbare media, vermelding van de classificatie op stickers, opslag binnen het rekencentrum, opslag op een *backup*-locatie, inventarisatie, transport en vernietiging van restantgegevens. Bij deze procedures is het invoeren van een voldoende mate van functiescheiding van belang ter voorkoming van diefstal, abusievelijke verspreiding van gevoelige informatie of zoekraken door slordigheid.

LOGISCHE TOEGANGSBEVEILIGING

Voor het beheer van de logische toegangsbeveiliging zijn administratieve functies gedefinieerd, die permanent ter beschikking staan aan de beheerders en tijdelijk aan systeemprogrammeurs. Ondanks dat het tijdelijk gebruik van dergelijke functies een zekere mate van oncontroleerbaarheid introduceert, valt hieraan niet te ontkomen aangezien systeemprogrammeurs door de huidige architectuur van de besturingssystemen deze functies nodig hebben voor het installeren van nieuwe produkten en het onderhouden van bestaande programmatuur. In het verleden heeft deze architectuur vele beveiligingsfunctionarissen en EDP-auditors doen verzuchten dat de systemen onbeveiligbaar zijn tegen systeemprogrammeurs. Door het invoeren van een effectief proces voor *change* en *problem management*, aangevuld door de onderstaande maatregelen van I&TCS 200, kan men de risico's van incorrecte handelingen door systeemprogrammeurs minimaliseren doordat de systeembeheerders een beter inzicht verkrijgen in de activiteiten van deze specialisten en betrokken worden bij de besluitvorming over nieuwe programmatuur en onderhoud.

Bij een systeem met *Resource Access Control Facility* (RACF) omvatten deze administratieve functies onder andere de SPECIAL-bevoegdheid, waarmee user-ids en beveiligingsprofielen kunnen worden gedefinieerd en gemodificeerd. Voor toekenning van deze functies is schriftelijke toestemming en periodieke herbevestiging noodzakelijk, zodat duidelijk wordt wie waarom over welke bevoegdheden beschikt. Bij iedere toekenning dient ook een vervaldatum te worden vastgesteld, waarop de be-

voegdheid automatisch op alle desbetreffende systemen wordt verwijderd. Voor beheerders is dat bijvoorbeeld twaalf maanden, waarbij de herbevestiging vóór de vervaldatum dient plaats te vinden, terwijl systeemprogrammeurs slechts gedurende enkele dagen over de SPECIAL-bevoegdheid mogen beschikken voor het realiseren van door de systeembeheerder goedgekeurde wijzigingen van de besturingsprogrammatuur. Deze I&TCS 200-maatregelen vereisen een nieuwe database voor het opslaan van de bevoegdheden, de motivatie van iedere toekenning en de vervaldata, en programmatuur voor het tijdig verwijderen van de vervallen bevoegdheden en het verifiëren dat niemand op een incorrecte wijze een dergelijke bevoegdheid heeft bemachtigd.

Daarnaast dient te worden gecontroleerd of de beheerders en systeemprogrammeurs hun werkzaamheden uitvoeren conform hun functiebeschrijving, door op onregelmatige tijdstippen een audit uit te voeren op basis van de vastleggingen van het systeem. De definitie van deze 'onaangekondigde 24 uur/maand audit' bleek in Europa zeer moeilijk te zijn, onder andere doordat in Italië het volgen van de activiteiten van personen via de computer juridisch discutabel is en in Duitsland per locatie onderhevig is aan afspraken met de ondernemingsraad. Niettemin is het onaangekondigd analyseren van alle activiteiten van de betrokkenen gedurende 24 uur per maand een vitaal onderdeel van het proces, aangezien dit het volgen van de regels door voorheen 'ongrijpbare' medewerkers aanmoedigt. Dit is vergelijkbaar met het plaatsen van een camerakast bij een verkeerslicht, waarin men gedurende één dag per maand een camera plaatst: doordat de verkeersdeelnemers nimmer weten op welke dag de kast echt in gebruik is zullen zij minder snel geneigd zijn door het rode licht te rijden.

Een ander belangrijk onderwerp zijn de *user-ids*, die uniek en herleidbaar moeten zijn naar personen en verantwoordelijke managers, en de wachtwoorden. Om de risico's van hackers te minimaliseren is in I&TCS 200 gekozen voor een zeer robuuste syntax voor de wachtwoorden, die taal- en toetsenbord-onafhankelijk is. Dit laatste was een belangrijk punt voor Europa: in het verleden waren veel syntaxregels gebaseerd op het uitsluiten van deelteksten zoals JAN voor *January* en MAR voor *March* om te voorkomen dat gebruikers voorspelbare wachtwoorden zouden gebruiken zoals JAN1992 en 1992MAR. Deze regels bleken in Europa nutteloos door het grote aantal talen en het internationaal gebruik van de systemen: zo heeft het uitsluiten van JAN en MAR geen zin voor een Hongaarse eindgebruiker, terwijl het uitsluiten van alle namen van maanden in ruim vijftig talen het invoeren van een correct wachtwoord schier onmogelijk maakt.
Ook het uitsluiten van naast elkaar liggende toetsen op een QWERTY-toetsenbord bleek nutteloos, aangezien men bijvoorbeeld in Frankrijk het AZERTY-toetsenbord gebruikt met een totaal andere indeling. Binnen Europa zijn meer dan twintig verschillende toetsenborden in gebruik (zoals het Nederlandse, Belgische, Duits-Oostenrijkse, Finse, enz.).

I&TCS 200 specificeert voor een wachtwoord nu de volgende regels:
- een lengte van ten minste zes posities;
- ten minste één alfabetische en één numerieke positie (om triviale namen zoals MERCEDES of cijferreeksen zoals 123456 te voorkomen);
- geen cijfer in de eerste of laatste positie (om JUNI1992 en 1992JUNI te voorkomen);
- niet meer dan drie overeenkomstige tekens ten opzichte van het vorige wachtwoord (om de reeks R2PAANS, R3PAANS en R4PAANS of andere triviale en voorspelbare vuistregels te voorkomen);
- niet meer dan twee aaneengesloten herhalende tekens (dus geen A1AAAA);
- ongelijk aan het user-id;
- ongelijk aan de 24 voorgaande wachtwoorden.

Een gewone gebruiker dient het wachtwoord ten minste iedere 186 dagen te wijzigen, terwijl een gebruiker met administratieve bevoegdheden dit ten minste iedere 31 dagen moet doen.

Door het invoeren van een effectief proces voor change en problem management kan men de risico's van incorrecte handelingen door systeemprogrammeurs minimaliseren.

In aanvulling op deze robuuste syntax is gekozen voor maatregelen zoals het bevriezen van user-ids na vijf mislukte pogingen om een wachtwoord te raden, en een mechaniek om systematische aanvallen door hackers snel onder de aandacht van de systeembeheerders te brengen. Op deze wijze zal een poging van een hacker om door het systematisch aanbieden van foutieve wachtwoorden de toegang tot een systeem of netwerk voor de rechtmatige gebruikers te blokkeren in een vroeg stadium worden gesignaleerd, waarna direct maatregelen kunnen worden getroffen.

Voor gebruikersgegevens bevat I&TCS 200 de volgende basisregel: 'niemand kan andermans gegevens benaderen tenzij expliciet geautoriseerd'. In het verleden werd het rekencentrum door veel EDP-auditors verantwoordelijk gesteld voor de inhoud van gebruikersbestanden en moest er regelmatig worden gespeurd naar geclassificeerde informatie die algemeen toegankelijk was. Dit was een gevolg van de nimmer beantwoorde vraag of het rekencentrum alleen de faciliteiten levert aan de eindgebruiker of ook de gebruikers dient te begeleiden bij het correct gebruik van deze faciliteiten. In I&TCS 200 wordt voor het eerste antwoord gekozen en verplaatst men de verantwoordelijkheid voor het gebruik van de faciliteiten, zoals schijfruimte, volledig naar de eigenaar van de gegevens. Hier staat tegenover dat een eigenaar een bestand nu niet meer publiekelijk toegankelijk mag maken, tenzij dit bestand als zodanig is geregi-

streerd binnen het rekencentrum en de eigenaar expliciet verklaart dat er nimmer geclassificeerde gegevens in zullen worden opgenomen. Het rekencentrum controleert ten minste maandelijks of bestanden publiekelijk zijn opengesteld door de eigenaren en blokkeert de algemene toegang tot het bestand indien dit niet als zodanig is geregistreerd. Deze procedure vereist het invoeren van nieuwe programmatuur om de eigenaren te beperken in hun mogelijkheden tot het ongecontroleerd openstellen van bestanden voor alle gebruikers en het invoeren van controleprogrammatuur voor de rekencentra om automatisch overtredingen op te sporen en te corrigeren. Op deze wijze wordt de juiste verantwoordelijkheid aan de juiste instantie toegekend.

Alle bestanden en bibliotheken die geen gebruikersgegevens bevatten, worden beschouwd als componenten van het besturingssysteem (*operating system resources*), waarvoor de volgende regels zijn gedefinieerd:

- Een component mag worden gelezen of verwerkt door de gewone gebruikers, tenzij dit de veiligheid van het systeem kan bedreigen: in zo een geval moet de toegang tot dit bestand of programma worden geblokkeerd om een inbreuk op de beveiliging te voorkomen.

- Geen enkele gewone gebruiker mag een component kunnen veranderen (alleen beheerders en systeemprogrammeurs mogen over deze bevoegdheid beschikken).

- Alle wijzigingen van de algemeen leesbare componenten en alle lees-activiteiten op de afgeschermde componenten moeten door het systeem worden vastgelegd.

- Een 'onaangekondigde 24 uur/maand audit' wordt uitgevoerd op basis van deze vastlegging ter controle van de correcte beveiliging en van de activiteiten van systeemprogrammeurs (ook deze audit heeft een preventieve functie zoals de camerakast bij een verkeerslicht).

Lokale modificaties mogen alleen worden geïnstalleerd na een certificatie-review, waarbij is vastgesteld dat zij geen risico's voor de beveiliging en integriteit van het systeem opleveren.

Wijzigingen van deze componenten zijn in vrijwel alle rekencentra onderhevig aan de procedures voor *change management*, waarbij via de periodieke audit wordt geverifieerd of alle wijzigingen vooraf zijn aangemeld en goedgekeurd. Deze maatregel forceert het volgen van de geldende procedures.

De onderhoudswerkzaamheden op systeemcomponenten omvatten onder andere het aanbrengen van *Program Temporary Fixes* (PTF's) ter correctie van fouten in de programmatuur. Sommige van deze PTF's, namelijk de *Integrity PTF's*, hebben betrekking op het sluiten van beveiligingslekken. Eén van de nieuwe I&TCS 200-maatregelen is het centraal evalueren van alle ontwikkelde Integrity PTF's, en deze classificeren als:

- *ernstig*. Als er sprake is van een lek dat door kwaadwillende gebruikers zeer eenvoudig kan worden uitgebuit, licht de Vice-President Automatisering alle rekencentra in dat deze PTF's binnen een nader te bepalen aantal dagen moeten worden aangebracht.

- *noodzakelijk*. Als het lek kan worden benut door gebruikers met speciale bevoegdheden of een meer dan gebruikelijke kennis, dienen de PTF's binnen 90 dagen te worden aangebracht.

- *gewenst*. Als het lek niet via de voor de gewone gebruiker gangbare commando's kan worden uitgebuit, dienen de PTF's binnen 18 maanden bij de eerstvolgende vervanging van het systeemplatform te worden aangebracht.

Het centraliseren van deze beoordelings- en waarschuwingsfunctie voorkomt dat ieder rekencentrum zelf de maandelijkse stroom van honderden PTF's moet evalueren om prioriteiten voor het onderhoud vast te stellen.

Lokale modificaties mogen alleen worden geïnstalleerd na een certificatie-review, waarbij is vastgesteld dat zij geen risico's voor de beveiliging en integriteit van het systeem opleveren. Het invoeren van deze certificaties is een preventieve maatregel, waarmee de in het verleden geconstateerde beveiligingslekken ten gevolge van onzorgvuldige lokale modificaties worden uitgebannen.

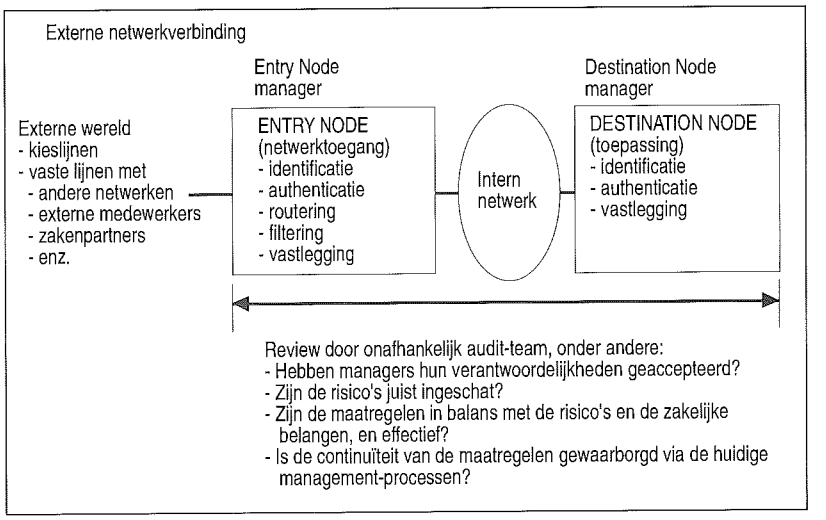
Om te verifiëren of alle systemen daadwerkelijk bestand zijn tegen hackers en interne aanvallen, is per Operating Unit een penetratiegroep opgericht. In Europa omvat deze groep negen ervaren systeemprogrammeurs, die via het netwerk de vele honderden systemen testen en bij elke penetratie of geconstateerde zwakheid het lokale management adviseren over het verbeteren van de beveiliging. Dankzij de centralisatie van de penetratie-testfunctie kan men de meest getalenteerde medewerkers benutten en zo een redelijke mate van zekerheid creëren dat de systemen op verantwoorde wijze zijn beschermd. De effectiviteit van dit proces wordt gemeten door het aantal systemen dat bij de eerste test faalde te vergelijken met de resultaten bij volgende tests: de waargenomen afname met een factor twee of meer geeft aan dat het lokale management de testresultaten actief gebruikt om het penetratierisico te verminderen.

Als laatste onderwerp van de logische toegangsbeveiliging worden in I&TCS 200 de maatregelen tegen schadelijke programmatuur (virussen, Trojaanse paarden en wormen) behandeld, met name het filteren van het berichtenverkeer op executeerbare code en het scannen van systemen. Deze

maatregelen zijn voornamelijk gericht op de gewone gebruiker, die beschermd dient te worden tegen het onbewust ontvangen en activeren van schadelijke programma's.

EXTERNE NETWERKVERBINDINGEN

Indien de interne systemen openstaan voor externe medewerkers die via kiesverbindingen of externe netwerken toegang kunnen verkrijgen, of voor klanten en zakenpartners, zijn aanvullende maatregelen nodig om misbruik of onbevoegd gebruik te voorkomen. Hiervoor is de standaard *Inter Enterprise Systems Connection* (IESC) ingevoerd als onderdeel van I&TCS 200, waarbij verantwoordelijkheden worden omschreven voor systeembeheerders, inclusief registratie van alle externe verbindingen en reviews door onafhankelijke auditteams vóór ingebruikname.



Figuur 1. Een schematische weergave van een Inter Enterprise Systems Connection (IESC).

In figuur 1 is een dergelijke externe verbinding schematisch weergegeven. Het systeem dat de voordeur van het interne netwerk vormt, wordt de *Entry Node* genoemd. Hierin wordt de identificatie van iedere externe gebruiker gecontroleerd (bijvoorbeeld via user-id en wachtwoord) en de bevoegdheid om gebruik te maken van interne systemen. Als de gebruiker bevoegd is tot een toepassing wordt een gecontroleerde verbinding opgebouwd door het interne netwerk, waar de gebruiker nimmer van kan afwijken, en krijgt deze toegang tot de *Destination Node*. Dit is het eindpunt voor de sessie van de gebruiker en mag geen mogelijkheden bevatten voor verdere routering (zoals DIAL of PASSTHRU op VM-systemen). Voor vitale toepassingen wordt veelal geëist dat de wachtwoorden op de Entry en Destination Node verschillend zijn, om zo een extra barrière op te werpen voor hackers en fraudeurs.
Deze standaard bevat ook een classificatieschema voor de risico's die de externe verbinding oplevert voor de interne systemen en gegevens, namelijk:

– *hoog risico.* Indien gegevens geclassificeerd als Confidential of hoger via kieslijnen kunnen worden benaderd via een enkel wachtwoord, of als belangrijke zakelijke transacties zonder tussenkomst van interne medewerkers kunnen worden ingevoerd, vereist ingebruikname van de verbinding de expliciete goedkeuring van de Directeur Automatisering.

– *gevoelig.* Alle verbindingen met interne systemen en netwerken dienen te worden beoordeeld door het audit-team op de juiste implementatie van user-id/wachtwoordmechanieken en het op gecontroleerde wijze toegang verlenen tot geautoriseerde systemen.

– *gedelegeerd.* Indien de verbinding alleen een persoonlijk systeem zonder geclassificeerde informatie betreft, zoals een PS/2 met een modem voor het benaderen van gegevensbestanden van een externe informatieleverancier, is geen onafhankelijke audit noodzakelijk.
De IESC-standaard omvat ook een audit-programma met een specificatie van de aandachtspunten tijdens de audit en de normen waaraan de beveiliging van de externe verbinding moet voldoen. Tijdens dit onderzoek wordt eveneens het proces gecontroleerd dat voor de continuïteit van de beveiliging ná certificatie moet zorg dragen.

Voor iedere IESC moeten de verantwoordelijke managers van de Entry Node en de Destination Node schriftelijk verklaren hun verantwoordelijkheden voor het installeren en onderhouden van de vereiste maatregelen te accepteren. Het audit-team controleert deze schriftelijke acceptatie, en deze documentatie wordt te zamen met het audit-rapport opgenomen in het IESC-register. Hiermee verkrijgt men een uitputtend overzicht van alle externe verbindingen en de conclusies van de auditteams over de getroffen maatregelen ter minimalisatie van de externe risico's.

De ervaringen hebben geleerd dat het IESC-programma de beheersbaarheid en controleerbaarheid van externe netwerkverbindingen in aanzienlijke mate verbetert, en dat vele inbreuken in computernetwerken van vele organisaties hadden kunnen worden voorkomen als men gelijkwaardige maatregelen had getroffen.

PRINTERS

In het verleden waren de print-faciliteiten onder het directe beheer van het rekencentrum, waardoor de distributie en het op verantwoorde wijze omgaan met geclassificeerde informatie een centrale verantwoordelijkheid was. Door het aansluiten van grote aantallen *remote printers*, eventueel via LAN's, binnen afdelingen en op andere locaties, vervalt dit centrale toezicht. Het rekencentrum heeft geen technische mogelijkheden de classificatie van print-gegevens vast te stellen, aangezien alleen de eindgebruiker weet wat de waarde van de inhoud van een *print-file* is. Door slordigheid en vergeetachtigheid resulteert dit vaak in geclassifi-

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 is hij werkzaam bij IBM, momenteel als Manager Corporate Programs voor het Europese hoofdkantoor, betrokken bij de wereldwijde standaardisatie van beveiligingsprocessen binnen IBM, bij de ontwikkeling van de daarvoor benodigde programmatuur en procedures, en bij de Europese implementatie van deze standaarden. Daarnaast is hij hoogleraar bij de post-doctorale opleiding EDP-Auditing van de Vrije Universiteit te Amsterdam en Europees redacteur van het tijdschrift Computers & Security.

ceerde documenten die blijven liggen bij de printers en door iedere voorbijganger kunnen worden gelezen of meegenomen. Vandaar dat de volgende regels zijn ingevoerd via I&TCS 200:

- Het beheer van geclassificeerde informatie geprint via een niet binnen het rekencentrum geplaatste printer is de verantwoordelijkheid van de eindgebruiker.

- De omgeving van de printer is de verantwoordelijkheid van een printer-eigenaar, benoemd door de manager van de desbetreffende locatie; deze printer-eigenaar stelt regels op voor het gebruik van de printer door eindgebruikers en houdt toezicht op naleving van deze regels.

- Het rekencentrum dient vast te stellen dat er een printer-eigenaar is benoemd voordat een printer wordt gekoppeld aan het netwerk, en dient jaarlijks te controleren of deze eigenaar nog bestaat.

De lokale regels dienen in overeenstemming te zijn met een aantal algemene voorschriften, zoals het gebruik van een *capture-release*-faciliteit voor geclassificeerde documenten. Hierbij plaatst de eindgebruiker een print-opdracht vanaf zijn of haar terminal in een wachtrij, loopt naar de printer, en geeft deze print-opdracht dan vrij voor het werkelijke printen onder persoonlijk toezicht. Bij afwezigheid van deze faciliteit is ook tijdig afhalen van Confidential-documenten mogelijk, bijvoorbeeld binnen een half uur, waarbij de tijdigheid regelmatig door de printer-eigenaar dient te worden gecontroleerd. Documenten die hoger geclassificeerd zijn dan Confidential dienen altijd onder persoonlijk toezicht te worden geprint.

NIET-REGULIERE MEDEWERKERS

Uit bedrijfseconomische overwegingen worden voor steeds meer functies binnen de automatisering niet-reguliere medewerkers ingezet, zoals uitzendkrachten. Soms krijgen deze zelfs tijdelijk vertrouwelijke functies, die in het verleden alleen door eigen medewerkers mochten worden vervuld. In principe gelden voor deze personen dezelfde beveiligingsregels als voor de eigen medewerkers, behalve voor:

- ondersteunende functies waarbij zij inzage kunnen krijgen in informatie met een hogere classificatie dan Confidential;

- functies waarbij de beveiliging op niet-detecteerbare wijze kan worden gefrustreerd (zoals beheerders van de logische toegangsbeveiliging en systeemprogrammeurs).

Voor deze twee groepen is een expliciete goedkeuring van een directielid noodzakelijk, die de risico's afweegt tegen de zakelijke belangen van het laten vervullen van de desbetreffende functie door een niet-reguliere medewerker. Bij voorkeur dient dit directielid de eigenaar van de gegevens te zijn.

IMPLEMENTATIE

In de appendices bij de standaard wordt aangegeven hoe deze systeem-onafhankelijke richtlijnen dienen te worden geïmplementeerd in systemen met het MVS-, VM- en OS/400-besturingssysteem, en in omgevingen met relationele databases.

SAMENVATTING

De standaard I&TCS 200 is een aanvulling op de bestaande internationale standaarden zoals het DoD Orange Book en ITSEC/ITSEM, en richt zich op complete informatie- en communicatiesystemen, inclusief de organisatie en de managementprocessen. Een dergelijke standaard is van essentieel belang voor iedere grote organisatie om het management en de medewerkers in te lichten over hoe moet worden beveiligd, en om over eenduidige audit-normen te beschikken. Het blijkt dat het ontwikkelen en invoeren van deze standaard bijdraagt zowel aan een verhoging van het beveiligingsniveau als aan een besparing op beveiligingskosten, aangezien men nu door centrale ontwikkeling van de vereiste programmatuur en procedures voorkomt dat ieder rekencentrum zelf het wiel moet uitvinden. Dit voorkomt een grote diversiteit aan lokaal ontwikkelde maatregelen, die kostbaar waren in implementatie en onderhoud, en die soms onvoldoende bescherming boden tegen doortastende 'inbrekers'.

LITERATUUR

[DoD83] US Department of Defense, *Trusted computer system evaluation criteria*, CSC-STD-001-83, 1983.

[IBM92] IBM, *Information security standards for providers of information systems services*, standaard I&TCS 200, 1992 (version 1.0) - verkrijgbaar via de auteur van dit artikel.

[ITSE91] *Information Technology Security Evaluation Criteria (ITSEC)*, Europese Gemeenschap, 1991 (draft version 1.2).

[ITSE92] *Information Technology Security Evaluation Manual (ITSEM)*, Europese Gemeenschap, uitg. ECSC-EEC-EAEC, Brussel, 1992 (draft version 0.2).

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

Ir. A. van Kooij

X.400 als toverformule om zeer uiteenlopende electronic mail-systemen over de hele wereld met elkaar te koppelen. Van Kooij geeft, puttend uit ervaringen in een project met dat doel, uitleg over de mogelijkheden en onmogelijkheden van de huidige X.400-produkten en belicht de belangrijkste aandachtspunten bij een dergelijke integratie. Wereldwijde invoering van elektronische post blijkt geen sinecure!

INLEIDING

Van het tijdschrift Compact heeft u zojuist de wikkel gehaald. Het adres op de wikkel zorgt ervoor dat dit tijdschrift op de juiste bestemming wordt afgeleverd. Is uw adres onbekend, dan had PTT Post dit tijdschrift niet bij u bezorgd. Een eenduidige adressering is een belangrijke voorwaarde waaraan moet worden voldaan om tot een wereldwijde postverzending te komen. Elektronische post verschilt in essentie niet van de papieren post, en kent soortgelijke problemen.

Een andere voorwaarde bij de uitwisseling van informatie is de leesbaarheid van de inhoud van de boodschap. Wanneer dit artikel in een vreemde taal was geschreven die u niet beheerst, dan had u dit artikel zonder meer overgeslagen. Dit geldt evenzo voor de opmaak van het artikel. Beide elementen hebben invloed op de leesbaarheid van dit artikel. Bij de distributie van elektronische documenten via elektronische post zijn deze elementen eveneens bepalend voor de mate van leesbaarheid. Alleen hebben ondernemingen in het kader van elektronische post ook nog te maken met de verscheidenheid aan informatiesystemen en programmatuur die elektronische documenten moeten kunnen verwerken. Standaardisatie en koppelbaarheid zijn twee sleutelwoorden bij de realisatie van global electronic mail.

INTRODUCTIE VAN BEGRIPPEN EN RAAMWERK

Alvorens het raamwerk te schetsen waarbinnen de kernvraag van dit artikel aan de orde komt, worden eerst enkele begrippen toegelicht.

Elektronische post: business-communicatie

Elektronische post heeft zich in de afgelopen jaren ontwikkeld tot gemeengoed voor de communicatie tussen mensen binnen kantoren. Daarnaast biedt elektronische post mogelijkheden om te worden toegepast voor interpersoonlijke communicatie tussen geografisch verspreide vestigingen en zelfs verschillende ondernemingen. Daarmee neemt zij een belangrijk deel van de huidige traditionele communicatiemiddelen over, te weten: telex, telefoon, facsimile en zelfs postale en koeriersdiensten.

Elektronische post is een toepassing binnen de informatisering die een aanmerkelijke bijdrage kan leveren tot verbetering van de (business-)communicatie.

Elektronische post is een toepassing binnen de informatisering die een aanmerkelijke bijdrage kan leveren tot verbetering van de (business-)communicatie. Ervaring leert dat het optimaal gebruiken van elektronische-postfaciliteiten leidt tot hogere effectiviteit van de interpersoonlijke communicatie binnen organisaties en tot reductie van de kosten verbonden aan het distribueren van poststukken, en daarmee uiteindelijk tot een verhoging van de produktiviteit.

X.400: intermediair voor elektronische-postsystemen

Met name in grote ondernemingen komen in de praktijk veelal verscheidene elektronische-postsystemen voor, die onderling verschillen. Het betreft hier veelal een diversiteit aan elektronische-postomgevingen gebaseerd op mainframe- en minicomputersystemen, en lokale PC-netwerken. Deze elektronische-postsystemen hebben een 'gesloten' karakter. Gebruikers van elektronische post kunnen in principe alleen berichten uitwisselen met diegenen die gebruiker zijn van hetzelfde postsysteem. Bij communicatie met derden is er vrijwel altijd sprake van verschillende elektronische-postsystemen.
Om organisatorische en technische redenen is het overgaan tot het gebruik van één elektronische-postsysteem vaak niet mogelijk. Teneinde de uitwisseling van elektronische post op een meer gestandaardiseerde wijze mogelijk te maken, overwegen organisaties steeds vaker gebruik te maken van X.400 als intermediair tussen de desbetreffende postsystemen. X.400, de standaard voor het elektronisch uitwisselen van berichten, is alom erkend. Hoewel X.400 zelf ook een standaard voor een elektronische-postsysteem is, en binnen organisaties ook zelfstandig kan worden toegepast, leent deze standaard zich bij uitstek voor de koppeling van verschillende lokale elektronische-postsystemen. Er zijn inmiddels X.400-produkten beschikbaar die de noodzakelijke koppeling met deze 'gesloten' elektronische-postsystemen kunnen verzorgen. Daarnaast zijn er aanbieders in de markt van openbare X.400-netwerkdiensten.

De kernvraag die in dit artikel aan de orde komt is hoe organisaties binnen de verscheidenheid aan bestaande elektronische-postsystemen de mogelijkheden van integratie van elektronische post met behulp van X.400 maximaal kunnen benutten. Invalshoek is het elektronische berichtenverkeer tussen vestigingen die geografisch verspreid zijn: global electronic mail.

Het antwoord op deze kernvraag ligt besloten in een gedegen aanpak voor de invoering van de integratie van elektronische post via X.400. In de praktijk blijkt dat organisaties zich onvoldoende bewust zijn van met name de organisatorische consequenties van het gebruik van X.400 bij de integratie van elektronische post. Er wordt een raamwerk aangereikt, waarin aandacht wordt besteed aan de verschillende aspecten rondom de complexe invoering van de integratie van elektronische post via X.400.

Vijf aandachtsgebieden ter voorbereiding

Het raamwerk is opgebouwd uit vijf aandachtsgebieden, te weten:
1. architectuur: inrichting van het X.400-netwerk;
2. adressering: informatie op de envelop van elektronische post;
3. interoperabiliteit: uitwisseling van elektronische berichten;
4. adresinformatie: toegankelijkheid van adresbestanden;
5. beheer en administratie: actualiseren van adresbestanden.

Dit artikel gaat op deze aandachtsgebieden in. Successievelijk worden de vijf aandachtsgebieden in de navolgende paragrafen afzonderlijk belicht, telkens met de technische en organisatorische consequenties.

De eerste voorwaarde tot integratie is het creëren van een basisinfrastructuur voor uitwisseling van elektronische post. Op grond van een inventarisatie van de bestaande elektronische-postomgevingen en van de eisen van de gebruikersorganisatie(s) kan de inrichting van het X.400-netwerk worden bepaald. Aan de orde komen de gateways voor de koppeling van de elektronische-postsystemen met X.400 en de mogelijke invulling van dit netwerk.

Vervolgens wordt ingegaan op de problematiek

rondom de adressering bij de integratie van elektronische post, de interoperabiliteit van de elektronische-postsystemen en de beschikbaarheid van adresinformatie voor de gebruikers van elektronische post. Deze drie aspecten vormen te zamen de kritische succesfactoren voor het welslagen van de integratie.

Ten slotte worden het beheer en de administratie van de totaal geïntegreerde elektronische-postomgeving belicht. Aan de orde komen beheerinstrumentarium, beveiliging en de noodzakelijke administratieve handelingen voor het beheer van betrokken elektronische-postsystemen.

De uitspraken en voorbeelden in dit artikel zijn gebaseerd op ervaringen die de auteur van dit artikel heeft opgedaan bij het ontwerpen, selecteren en realiseren van een wereldwijd X.400-netwerk voor elektronische post.

ARCHITECTUUR

De gebruikers van de te integreren elektronische-postsystemen bepalen uiteindelijk door de mate van acceptatie het succes van de integratie van elektronische post. Behalve de gebruikersinterface en de structuur van de bestaande elektronische-postsystemen zijn de aanwezige datacommunicatievoorzieningen, de geografische spreiding van vestigingen en de eisen die de onderneming aan de integratie van elektronische post stelt mede voorwaarden voor het gebruik van X.400. Uiteraard dient daarnaast de inrichting van de totale elektronische-postomgeving alsmede de inrichting van de architectuur aan te sluiten bij de IT-strategie van de onderneming.
De architectuur voor de integratie van elektronische-postsystemen bestaat uit:
- een gemeenschappelijke netwerkinfrastructuur, ook wel aangeduid als de backbone, waarop alle bestaande elektronische-postsystemen zijn aangesloten;
- gateways voor de koppeling van de elektronische-postsystemen met de backbone.

In deze paragraaf wordt ingegaan op de inrichting van de backbone en de functie van de elektronische-post-gateway. Hoewel de inrichting van de backbone betrekking heeft op de keuze van de toe te passen technologie, liggen organisatorische redenen ten grondslag aan de definitieve keuze. Voor deze organisatorische motieven wordt verwezen naar [Evel93].

Backbone-netwerk

Het X.400-backbone-netwerk ontsluit de autonome ('gesloten') elektronische-posteilanden en verzorgt het onderlinge elektronische berichtenverkeer. Voor de realisatie van het X.400-backbone-netwerk zijn er twee mogelijke opties, die successievelijk worden besproken:
- een privé X.400-netwerk door gebruik te maken van een privé X.25-netwerk;
- een openbare X.400-netwerkdienst.

In termen van X.400 (zie ook het aparte kader over dit onderwerp verderop in dit artikel) wordt een particulier elektronische-postsysteem beschouwd als een Private Management Domain (PRMD). Een openbare X.400-netwerkdienst is een Administration Management Domain (ADMD). Wanneer de backbone een privé X.400-netwerk is, is de totaal geïntegreerde elektronische-postomgeving inclusief alle afzonderlijke elektronische-postsystemen binnen de onderneming te beschouwen als één PRMD (figuur 1). Bij het gebruik van een openbare X.400-netwerkdienst voor de backbone heeft daarentegen elk elektronische-postsysteem afzonderlijk de status van een PRMD (figuur 2).

De realisatie van een dergelijk backbone-netwerk vergt voor internationale ondernemingen meer inspanning en afstemming dan voor een nationaal georiënteerd netwerk. In de landen waar de vestigingen zich bevinden, zal de koppeling met deze vestigingen veelal in overleg met de lokale PTT-organisaties tot stand moeten worden gebracht. Elk land heeft zijn 'eigen' regelgeving ten aanzien van het gebruik van de telecommunicatiefaciliteiten. Bovenal verschilt de kwaliteit van de datacommunicatieverbindingen alsmede de dienstverlening onderling nogal sterk. Daartegenover heeft een nationale onderneming slechts te maken met één partij: de nationale PTT-organisatie.

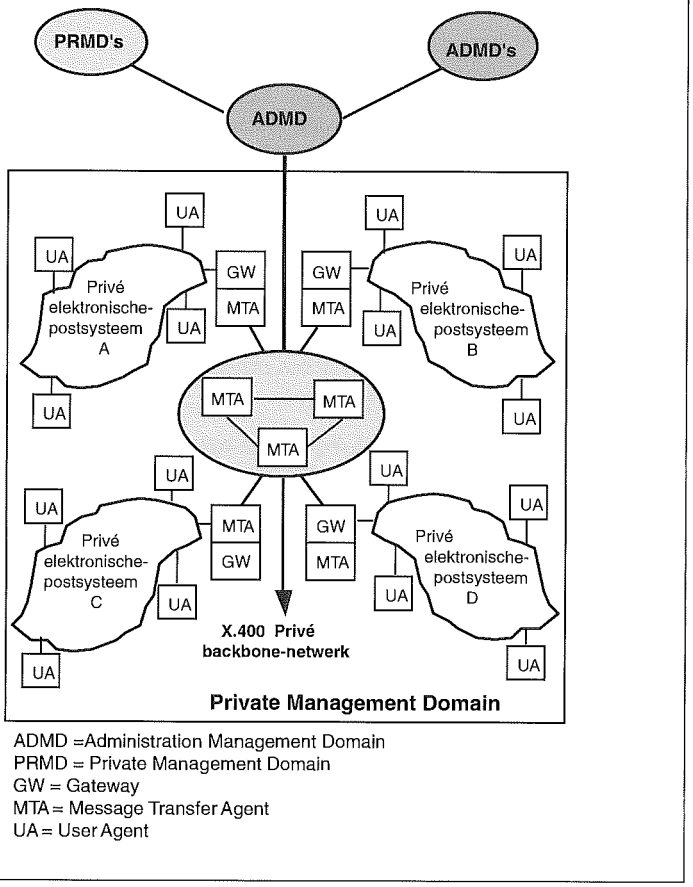
Privé X.400-netwerk

Het backbone-netwerk kan gebruik maken van een bestaand Wide Area Netwerk (WAN). Een WAN is een privé (inter)nationale datacommunicatie-infrastructuur die door de onderneming zelf wordt geëxploiteerd en beheerd. Zo'n netwerk bestaat uit vaste datacommunicatieverbindingen tussen de vestigingen of is opgebouwd rondom openbare X.25-netwerkdiensten.

Voorts moeten organisaties bij een privé X.400-netwerk wel rekening houden met eventuele additionele investeringen. Deze investeringen hebben niet alleen betrekking op de benodigde hardware en software, maar ook op het beheer van het privé X.400-netwerk: de beheerorganisatie inclusief instrumentarium en personeel. De investering voor de inrichting van het privé X.400-netwerk wordt met name bepaald door het aantal te koppelen elektronische-postsystemen en de eisen die aan het netwerk worden gesteld zoals beschikbaarheid en beveiliging.

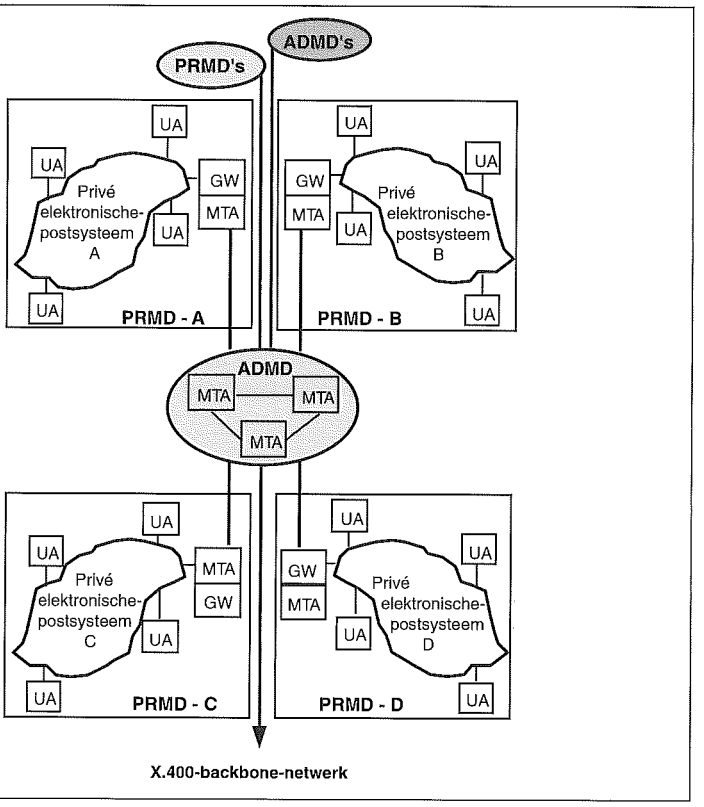
Openbare X.400-netwerkdiensten

Naast een privé-netwerk zijn openbare X.400-netwerkdiensten voorhanden die de rol van backbone goed kunnen vervullen. Het verdient hier de voorkeur dat de backbone wordt opgebouwd rondom één X.400-netwerkservice van één leverancier. Het gebruik van een zelfde ADMD als backbone voor de integratie van elektronische post levert de volgende additionele voordelen op:
- één identiteit van de onderneming zowel in-



Figuur 1. Privé X.400-backbone-netwerk.

Figuur 2. Publieke X.400-netwerkservice ADMD als backbone.



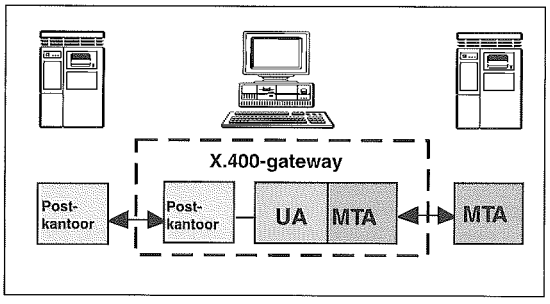
ternationaal als nationaal;
- één elektronische weg naar het particuliere elektronische-postsysteem;
- een eenduidige interorganisatorische communicatie met cliënten;
- het gebruik van telex en facsimile gateway-functionaliteit. Veelal beschikken publieke X.400-netwerkdiensten over een koppeling met zowel het publieke telexnetwerk als met publieke facsimilenetwerken;
- één partij, die tevens kennis heeft van de lokale problematiek in de verschillende vestigingslanden;
- een wereldwijd netwerk met lokale toegang;
- een wereldwijde support-organisatie met kantoren in de verschillende landen.

Behalve de nationale PTT-organisaties zijn er ook internationale aanbieders in de markt voor netwerkdiensten. Deze organisaties opereren internationaal en beschikken over een wereldwijde dienstverlening met lokale support-organisaties in een groot aantal landen en toegang tot een wereldwijde netwerkinfrastructuur. Deze zogenaamde Value Added Network (VAN)-leveranciers richten zich primair op de toegevoegde waarde van het gebruik van telecommunicatie en netwerkdiensten. Daartoe onderhouden zij nauwe relaties met nationale PTT-organisaties.

X.400-produkten - gateways

Elk elektronische-postsysteem beschikt over één gateway voor de uitwisseling van elektronische post met het X.400-backbone-netwerk. Deze gateway vertaalt de inkomende X.400-berichten in het formaat dat door het desbetreffende elektronische-postsysteem kan worden verwerkt, en omgekeerd voor uitgaande elektronische post. Feitelijk bestaat de gateway (zie figuur 3) uit een tweetal postkantoren:
- een X.400-postkantoor: Message Transfer Agent (MTA) die de communicatie met de backbone verzorgt;
- een postkantoor overeenkomstig het lokale elektronische-postsysteem voor de uitwisseling van berichten met deze postomgeving. Dit postkantoor zorgt tevens voor de vertaling van elektronische post in X.400 en terug. Voor de X.400-communicatie maakt dit postkantoor gebruik van een X.400 User Agent (UA).

Figuur 3. Opbouw X.400-gateway.



Dergelijke gateways maken soms deel uit van het produktassortiment van leveranciers van de desbetreffende elektronische-postsystemen. Daarnaast leveren ook gespecialiseerde producenten van X.400-produkten de vereiste gateways.

Aan de selectie van de gateways liggen veelal twee belangrijke uitgangspunten voor de integratie van elektronische post ten grondslag:

- *Transparantie voor de gebruiker van elektronische post.*
Gebruikersinterface, prestatieniveau, betrouwbaarheid en ondersteuning zijn zoals de gebruikers dat gewend zijn. De gebruikers van elektronische post mogen geen verschil ervaren in het verzenden ongeacht of de geadresseerden postbussen hebben op hetzelfde postsysteem als de zender, dan wel op andere postsystemen.

- *Minimaal verlies aan functionaliteit.*
De toe te passen gateway zal niet alleen de vertaling en de heradressering tussen de verschillende formaten op een correcte wijze moeten verzorgen, maar ook een goede afbeelding van verzendgegevens die een zender aan het bericht meegeeft. Bijvoorbeeld, een urgent bericht geïnitieerd in het ene postsysteem dient door het andere systeem als urgent te worden herkend en evenzo behandeld. Hetzelfde geldt voor het meezenden van documenten en andere functies die tot de basisfunctionaliteit van de lokale systemen behoren.

Om een verantwoorde keuze van de gewenste gateways te kunnen maken dienen de volgende aspecten aan de orde te komen:

- *Adresvertaling*
Zijn de adresconversies geheel transparant voor de gebruikers?

- *Management*
Welke administratieve en beheerfuncties worden geboden?

- *Interoperabiliteit*
Worden alle benodigde functies van zowel X.400 als het desbetreffende elektronische-postsysteem ondersteund?
Wat is het resultaat wanneer een zekere functionaliteit niet door één der beide postomgevingen wordt ondersteund?
In hoeverre kunnen binaire bestanden met elektronische post worden meegezonden?
Welke X.400-profiles worden ondersteund?

- *Specificaties*
Wat zijn de beperkingen van de gateways in termen van de te ondersteunen datacommunicatieprotocollen, aantal gebruikers en adresvertaling?

- *Adresuitwisseling*
In hoeverre wordt X.500 dan wel een directory-synchronisatiemechanisme ondersteund?
Wat is de produktstrategie van de producent daarin?

- *X.400-functionaliteit*
Is er volledige ondersteuning van Message Transfer Agent-functionaliteit of is er slechts sprake van een subset?
Is de implementatie gebaseerd op 1984- of 1988-X.400-specificaties?

- *Integratie*
In hoeverre is de gateway geïntegreerd met het desbetreffende elektronische-postsysteem in relatie tot adressering, het meezenden van elektronische documenten, gebruikersinterface en administratieve functies?

- *Afleveringnotificatie*
Wordt er bij het al dan niet kunnen afleveren van een boodschap een melding gegeven?
Bevestiging van ontvangst bij aflevering en indicatie met reden bij het niet kunnen afleveren. Redenen daartoe zijn bijvoorbeeld:
  - een onbekend of verkeerd adres van de postbus van de geadresseerde;
  - het onbereikbaar zijn van het postsysteem waartoe de geadresseerde behoort.

- *Routering*
Worden alternatieve routes ondersteund?

- *Beveiliging*
Welke beveiligingsfuncties worden ondersteund?
In welke mate sluiten de functies aan op het beveiligingsbeleid?

- *Certificaat*
Zijn er tests uitgevoerd met de X.400-MTA van de gateway door de producent en de verschillende VAN-leveranciers?
Is dit produkt gecertificeerd?

ADRESSERING

Met het X.400-backbone-netwerk is de basisinfrastructuur voor de uitwisseling van elektronische post gelegd. Zoals aangegeven in de inleiding moet de envelop bij elektronische post in analogie met het postale verkeer een adres bevatten op grond waarvan het bericht kan worden gesorteerd, doorgestuurd en afgeleverd bij de geadresseerde. De adressering binnen het backbone-netwerk moet dus eenduidig en consistent zijn. Onduidelijkheden mogen niet voorkomen en afwijkingen moeten zoveel mogelijk worden vermeden.

De backbone hanteert de in X.400 gedefinieerde adressering, terwijl elk op de backbone aangesloten elektronische-postsysteem een 'eigen' adresstructuur heeft om berichten naar een bestemmingspostkantoor te routeren en vervolgens in de postbus van de geadresseerde te deponeren. Daarin schuilt dan ook meestal het venijn van de adressering en vereiste vertaling. Het gevolg is vaak onjuiste conversie door onduidelijke afspraken over de invulling van het X.400-adres en vertaaltabellen met verkeerde adresinformatie. Bovendien kunnen de beperkte vertaalmogelijkheden van de gateways hierbij parten spelen.

Ter verduidelijking van deze problematiek worden

achtereenvolgens het X.400-adresformaat en het elektronische-postadres toegelicht en wordt de afbeelding van het X.400-adres op de adresstructuur van de 'gesloten' (= proprietary) elektronische-postsystemen behandeld.

Uniek postbusadres

Ofschoon de postbushouders binnen hun elektronische-postsysteem een uniek postbusadres hebben, moeten zij evenzo vanuit de (veel grotere) X.400-wereld eenduidig zijn te adresseren. Dit betekent dat de structuur van de X.400-adressering voor alle aangesloten elektronische-postsystemen gelijk moet zijn.

Voor de uitwisseling van elektronische post tussen de aangesloten elektronische-postomgevingen moeten de adressen van zowel de zender als de ontvanger successievelijk worden vertaald van het zendende postsysteem in X.400 en van X.400 in het postsysteem van bestemming. De gateways van de desbetreffende elektronische-postsystemen dragen elk zorg voor de correcte vertaling van het 'eigen' postadres in een X.400-equivalent en omgekeerd.

X.400-adresformaat

Het X.400-adresformaat heeft qua opbouw een hiërarchische structuur en bestaat uit de elementen zoals weergegeven in tabel 1.

C	= Landcode	Netwerk
ADMD	= ADMD-naam	
PRMD	= PRMD-naam	
Org	= Organisatienaam	Organisatie
OU1	= Organisatie-eenheid 1	
OU2	= Organisatie-eenheid 2	
OU3	= Organisatie-eenheid 3	
OU4	= Organisatie-eenheid 4	
Sn	= Familienaam	Persoon
Gn	= Voornaam	
I	= Initialen	

Tabel 1. Hiërarchische structuur.

Deze adresstructuur omvat informatie over het netwerk van het particuliere elektronische-postsysteem van de desbetreffende organisatie, over de organisatie zelf (de structuur van de organisatie) en over haar werknemers. De eerste drie elementen zijn bepalend voor de bereikbaarheid van het particuliere elektronische-postsysteem:

- hoe wordt het elektronische-postsysteem van de organisatie aangeduid: PRMD-naam;
- via welke openbare elektronische weg is het bereikbaar: ADMD-naam;
- in welk land bevindt zich de ADMD: de landcode.

(Zie voor de verklaring van PRMD en ADMD het tweede kader, verderop in dit artikel.)

De overige informatie is louter voor interne routering naar het bestemmingsadres.

Opmerking: X.400 kent meerdere varianten van adressering.

'Gesloten' elektronische-postadres

Een 'gesloten' elektronische-postsysteem daarentegen kent een eenvoudiger adressering. Een postbus wordt meestal bepaald door een combinatie van drie elementen: postnetwerk, naam/postkantoor en naam/postbusadres.

De adresstructuur is zeer plat. Veelal moet de benaming van een postbusadres niet alleen uniek zijn binnen het postkantoor en -netwerk, maar ook voor de totale 'eigen' elektronische-postomgeving.

Afbeelding X.400-adres - elektronische-postadres

Het X.400-adres nodigt uit om de medewerkers conform hun organisatorische positie/plaats door middel van bedrijfsonderdelen binnen de onderneming te beschrijven. In de praktijk hebben de benamingen van postkantoren en -netwerken van 'gesloten' elektronische-postsystemen veelal geen logisch verband met de bedrijfsonderdelen van de onderneming. Bovendien maken meerdere bedrijfsonderdelen doorgaans gebruik van postbussen op hetzelfde postkantoor. Dit bemoeilijkt de eenduidige vertaling naar een X.400-adres.

Wanneer ondernemingen op deze wijze hun organisatiestructuur in het X.400-adres benoemen, betekent dit dat ten behoeve van routering minimaal één gateway per bedrijfsonderdeel en/of afdeling nodig is. Immers, elk benoemd element binnen het X.400-adres vertegenwoordigt een knooppunt binnen de routering. Ter illustratie onderstaand voorbeeld.

Twee personen van het bedrijf ELPOST presenteren zichzelf met hun business-kaarten. De ene persoon is account manager bij de Sales-divisie

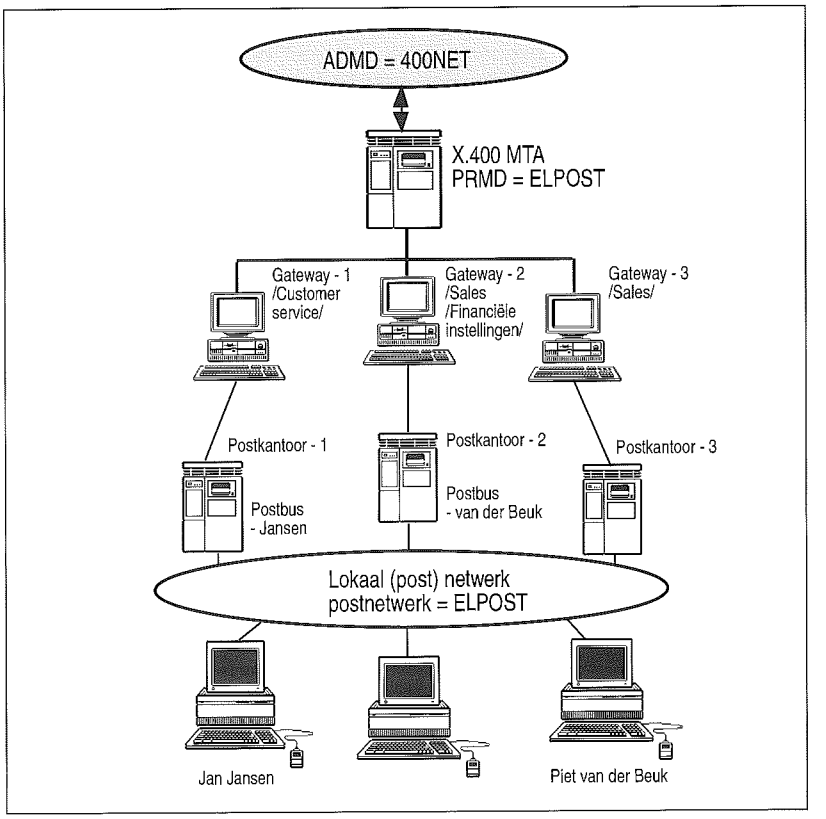
Tabel 2. Visitekaartje.

	Voor account manager Piet van der Beuk	Voor manager Customer service Jan Jansen
C	NL	NL
ADMD	400NET	400NET
PRMD	ELPOST	ELPOST
Org	Sales	Customer service
OU1	Financiële instellingen	
Sn	Van der Beuk	Jansen
Gn	Piet	Jan

Financiële instellingen, terwijl de ander manager van Customer service is. Beiden hebben een postbus binnen hetzelfde elektronische-postsysteem van dat bedrijf, maar op verschillende postkantoren. Op de visitekaartjes staat onder meer hun X.400-adres.
Figuur 4 illustreert dat er ten minste drie gateways nodig zijn. Eén gateway voor Sales en één voor Customer service, terwijl de derde minimaal nodig is om de andere personen (en afdelingen) in het bedrijf te adresseren.
Bij een vereenvoudiging van het X.400-adres zou er met slechts één gateway kunnen worden volstaan. Dit is weergegeven in tabel 3 en figuur 5.

	Voor account manager Piet van der Beuk	Voor manager Customer service Jan Jansen
C	NL	NL
ADMD	400NET	400NET
PRMD	ELPOST	ELPOST
Org	ELPOST	ELPOST
Sn	Van der Beuk	Jansen
Gn	Piet	Jan

Tabel 3. Vereenvoudiging van het X.400-adres.



Figuur 4. Elektronische-postsysteem van de firma ELPOST.

Feitelijk wordt gepoogd een hiërarchisch gestructureerde omgeving als X.400 af te beelden op een platte netwerkstructuur van de 'gesloten' elektronische-postsystemen. In de regel vertoont een dergelijk 'gesloten' elektronische-postnetwerk geen relatie met de organisatie zelf. Derhalve is het advies de X.400-naamgeving niet-hiërarchisch weer te geven.

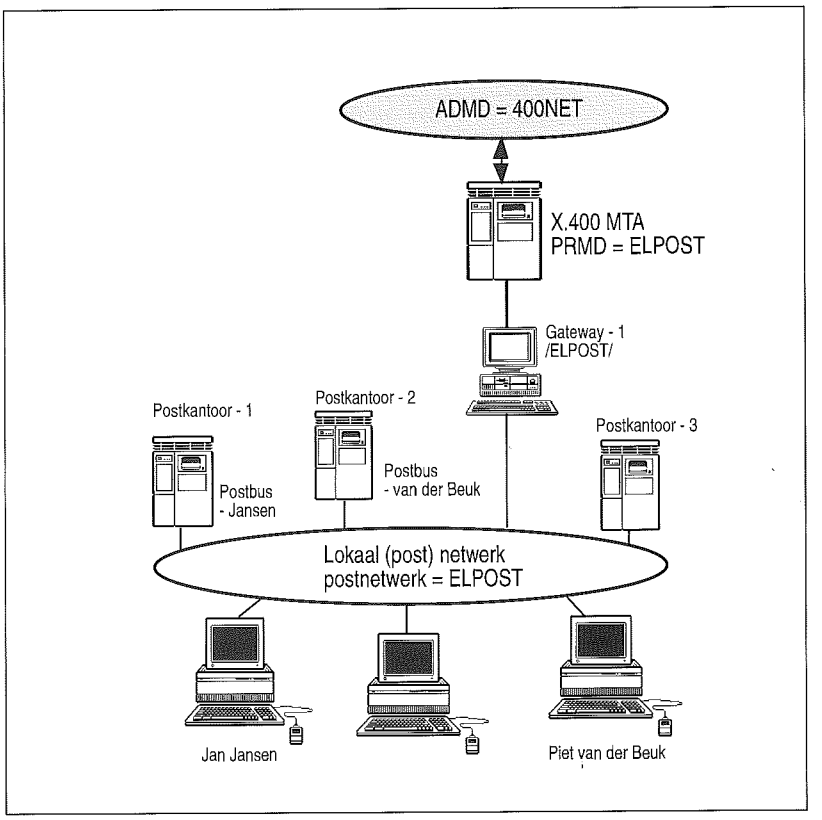
(Inter)nationale identiteit van ondernemingen

In tegenstelling tot de adressering van 'gesloten' elektronische-postsystemen presenteren ondernemingen zich met het X.400-adres aan derden. Veelal wordt de naam van de onderneming als PRMD-naam gebruikt. Voorts associëren en identificeren organisaties zich met de landcode (C) in het X.400-adres. De landcode geeft het land aan waar de ADMD is geregistreerd. Volgens de X.400-standaard kan een ADMD slechts in één land zijn geregistreerd. Dit kan in de praktijk een probleem zijn.

In het geval dat internationale organisaties overwegen voor de backbone van een zelfde X.400-netwerkdienst gebruik te maken, kunnen zij op grote interne tegenstand stuiten. Immers, één ADMD betekent één netwerkleverancier en dus één partij die voor de desbetreffende onderneming de backbone verzorgt en lokaal de X.400-connecties met de nationale vestigingen bewerkstelligt.

Ten gevolge van de verschillende nationale culturen binnen de onderneming hechten lokale vestigingen in de desbetreffende landen een groot belang aan de nationale herkenbaarheid. Zij willen zichzelf kunnen identificeren als een nationaal be-

Figuur 5. Elektronische-postsysteem van de firma ELPOST met één gateway.



drijf, ofschoon ze tot een internationale organisatie behoren. Zeker wanneer deze vestigingen met lokale relaties berichten via X.400 gaan uitwisselen. Een nationale identiteit met X.400 kan dus alleen worden verkregen wanneer een vestiging een koppeling met een lokaal openbaar X.400-netwerk realiseert. De optie om wereldwijd van een zelfde X.400-netwerkdienst als backbone gebruik te maken vervalt daarmee.

Vooralsnog bieden nationale X.400-koppelingen nog geen volledige garantie voor een wereldwijde uitwisseling van X.400-berichten tussen alle bestaande openbare X.400-netwerken onderling. Hoewel nationale PTT-organisaties en VAN's naar zoveel mogelijk koppelingen met andere netwerken streven, zitten zij nog in de beginfase van dit proces.

Voorbeeld: De firma ELPOST heeft meerdere vestigingen in het buitenland. Het hoofdkantoor bevindt zich in Nederland. Voor de integratie van elektronische post overweegt deze firma voor de invulling van de backbone gebruik te maken van de openbare X.400-netwerkdienst van PTT Telecom: 400NET. De Canadese vestiging heeft echter bezwaren tegen de landcode NL in het X.400-adres en besluit vanwege de nationale identiteit voor een koppeling met het openbare X.400-netwerk van de Canadese PTT: ENVOY.

De X.400-adressering zou er daardoor moeten uitzien als in tabel 4.

	Hoofdkantoor Nederland	Vestiging Engeland	Vestiging Canada
C	NL	NL	CA
ADMD	400NET	400NET	ENVOY
PRMD	ELPOSTNL	ELPOSTUK	ELPOSTCA
Org	ELPOST	ELPOST	ELPOST
Sn	Van der Beuk	Smith	Donaldson
Gn	Piet	Bob	Brian

Tabel 4. Adressering.

De VAN-leveranciers hebben dit probleem van nationale identificatie onderkend. Daarom zijn ze thans doende hun ADMD's, die nu veelal alleen in Amerika of Engeland zijn geregistreerd, ook in andere landen te registreren. Dit betekent echter niet dat de desbetreffende ADMD ook daadwerkelijk in dat land is gelokaliseerd. Multinationale registratie biedt internationale ondernemingen een wereldwijde presentatie met een nationale identiteit.

Als voorbeeld is de structuur van de elektronische-postomgeving van KPMG in tabel 5 weergegeven.

Tabel 5. Globale elektronische-postomgeving.

	Hoofdkantoor Nederland	Vestiging Engeland	Vestiging Canada	Vestiging USA	Vestiging Australië
C	NL	GB	CA	US	AU
ADMD	MARK400	MARK400	MARK400	MARK400	MARK400
PRMD	KPMG	KPMG	KPMG	KPMG	KPMG
Org	KPMG	KPMG	KPMG	KPMG	KPMG
Sn					
Gn					

INTEROPERABILITEIT

De inleiding gaf al aan dat er aan ten minste twee voorwaarden moet zijn voldaan om het gebruik van elektronische post te bevorderen. Naast adressering geldt de leesbaarheid van berichten en elektronische documenten. Het feit dat elektronische post via X.400-adressering kan worden uitgewisseld, is nog geen garantie dat de boodschap ook daadwerkelijk door de geadresseerde kan worden gelezen dan wel dat een correcte vertaling van de zendgegevens door de gateways heeft plaatsgevonden. Naast verschillende elektronische-postsystemen kunnen ook de informatiesystemen waartoe de zender en de ontvanger behoren, verschillend zijn.

Het door de ontvanger kunnen lezen en interpreteren van elektronische post alsmede de meegezonden documenten wordt bepaald door:
- de interoperabiliteit van elektronische-postsystemen;
- de compatibiliteit van de elektronische documenten.

X.400-interoperabiliteit

In de praktijk blijken er nauwelijks problemen te zijn met de transfer en uitwisseling van berichten via X.400. Belangrijkste reden hiervoor is dat producenten van X.400-produkten en netwerkleveranciers van openbare X.400-diensten groot belang hechten aan het met elkaar kunnen samenwerken van hun produkten en diensten. De VAN-leveranciers certificeren bijvoorbeeld X.400-produkten waarmee goede testresultaten zijn behaald. Daarnaast buigen normalisatie-instituten zich over deze interoperabiliteitsproblematiek en ook verzorgen zij testdocumentatie om het raamwerk van de X.400-interoperabiliteit te kunnen bepalen.

Benadrukt moet worden dat deze tests en de testdocumenten zich thans beperken tot X.400. Tests voor de bepaling van de interoperabiliteit van elektronische-postsystemen via X.400 ten aanzien van functionaliteit vinden niet plaats. Ook de normalisatie-instituten schenken geen aandacht aan deze problematiek.

Profiles

De interoperabiliteit van X.400-systemen is vervat in afspraken omtrent de te ondersteunen functio-

naliteit. Dit stelsel van afspraken is door internationale standaardisatie-organen beschreven in zogenaamde profiles. Er zijn twee typen profiles gedefinieerd: één voor de uitwisseling van X.400-berichten tussen een ADMD en een PRMD, en één voor het berichtenverkeer tussen PRMD's onderling.

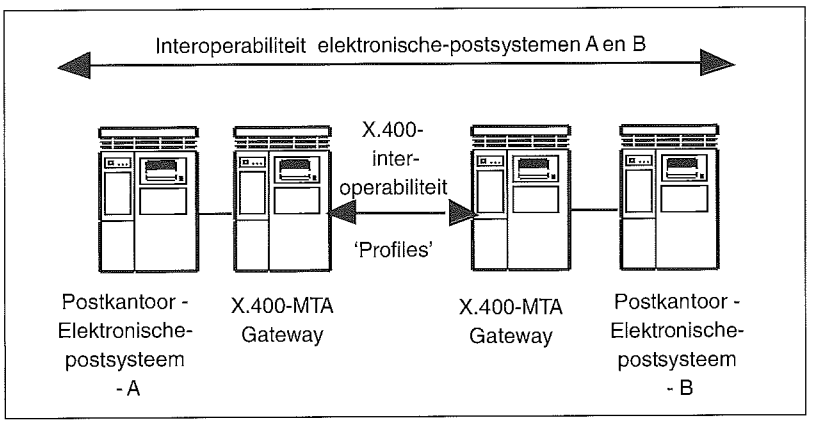
Interoperabiliteitstests van elektronische-postsystemen

De producenten van gateways trachten elk naar eigen vermogen de vertaling van X.400 naar een elektronische-postsysteem in te vullen. Dit geldt zowel voor de berichten (al dan niet inclusief de meegezonden documenten) als voor de te ondersteunen zendgegevens. Momenteel bestaan er geen formele afspraken op grond waarvan zij de interface tussen een elektronisch postsysteem en X.400 moeten verzorgen (zie figuur 6).
Vooralsnog moeten de ondernemingen zelf de noodzakelijke interoperabiliteitstests tussen de elektronische-postsystemen uitvoeren. Aan de hand van de testresultaten kunnen vervolgens de beperkingen van de functionaliteit van elektronische post alsmede de integratie via X.400 worden vastgesteld. Met behulp van deze informatie kunnen de help desk-medewerkers worden onderricht voor de vereiste ondersteuning aan de gebruikersorganisatie en kunnen de gebruikers van elektronische post worden geïnstrueerd.

Compatibiliteit van elektronische documenten

Afgezien van de verschillen in elektronische-postsystemen en gateways kunnen de zender en ontvanger(s) gebruik maken van totaal verschillende informatiesystemen. De gebruikers van elektronische post worden geconfronteerd met de incompatibiliteit van elektronische documenten. Feitelijk betreft het de traditionele problematiek rondom de uitwisseling en opmaak van elektronische documenten. Documenten die via elektronische post worden meegezonden en niet door de ontvangers kunnen worden gelezen doordat de zender en ontvanger(s) al dan niet gebruik maken van:
- verschillende tekstverwerkers: WordPerfect, MSWord, etc.;
- verschillende versies van een zelfde type tekstverwerker;
- verschillende computersystemen: Apple Macintosh, IBM compatibele personal computers, DEC, IBM, etc.

Bij elektronische post herleven deze problemen dus weer. De gebruikers moeten noodzakelijkerwijs worden geïnstrueerd hoe zij moeten handelen. Zolang het eenvoudig berichtenverkeer betreft, kan bijvoorbeeld worden afgesproken dat een elektronisch document in ASCII-tekstformaat (ook wel IA5-code) wordt verzonden: print- en leesbaar. Voor meegestuurde documenten die op de bestemming verder moeten worden verwerkt, vermeldt de afzender expliciet de gebruikte tekstverwerkerprogrammatuur inclusief de versie. In dat geval converteren de ontvangers zelf naar het juiste tekstformaat. Daartoe dienen zij te beschikken over de vereiste vertaal/conversiemiddelen.



Figuur 6. Interoperabiliteit tussen elektronische-postsystemen.

ADRESINFORMATIE

In de vorige drie paragrafen werden de basiselementen voor de integratie van elektronische post via X.400 beschouwd, te weten:
- de architectuur: het X.400-backbone-netwerk inclusief de vereiste gateways voor de elektronische-postsystemen;
- de adressering: het adres op de envelop van elektronische post;
- de interoperabiliteit: de uitwisseling van de inhoud van elektronische post.

Echter, de gebruikers van elektronische post bepalen het succes van de integratie van elektronische post door hun acceptatie. Deze acceptatie wordt in belangrijke mate bepaald door twee factoren:
- het feilloos transporteren van berichten en documenten tussen de verschillende elektronische-postomgevingen;
- het beschikken over adressen van postbushouders, ook wanneer zij niet tot hetzelfde elektronische-postsysteem behoren.

Het adresseren van elektronische berichten bestemd voor een postbus van een ander postsysteem moet even eenvoudig zijn als voor postbussen die tot hetzelfde postsysteem behoren. Dit betekent dat de gebruikers van elektronische post in principe lokaal toegang moeten hebben tot alle adressen van de geïntegreerde elektronische-postomgeving.

X.500-standaard

De standaard X.400 voorziet niet in de automatische uitwisseling van adressenbestanden van de postbussen tussen de verschillende elektronische-postsystemen. De standaard X.500 is hiertoe specifiek gedefinieerd. Momenteel zijn er echter nauwelijks X.500-produkten voorhanden. De verwachting is dat binnen drie jaar deze standaard in X.400-gateways is geïntegreerd.

De standaard X.500 beschrijft een zogenaamd Directory service-systeem, een gedistribueerd in-

formatiesysteem dat gebruikers in staat stelt op een gestandaardiseerde wijze informatie op te vragen over gebruikers, organisaties en applicatieprocessen. De gebruikers kunnen zowel personen als computersystemen zijn. De functie die een Directory service vervult, is te vergelijken met die van een elektronisch telefoonboek.

Synchronisatie van lokale adresbestanden

In de praktijk moeten thans nog alternatieve manieren worden gebruikt om de adresbestanden van de verschillende elektronische-postsystemen voor alle gebruikers van elektronische post lokaal toegankelijk te maken. Vooralsnog leidt synchronisatie van adresbestanden van de verschillende elektronische-postsystemen onderling tot de gewenste situatie. Hoewel sommige producenten van gateway-produkten een 'eigen' directory-synchronisatiemechanisme ondersteunen, blijven altijd elektronische-postsystemen over die niet worden ondersteund. Derhalve zal de synchronisatie dus vaak deels handmatig moeten plaatsvinden.

Uitgangspunt is dat alle lokale adresbestanden van de deelnemende postsystemen in principe de complete adresinformatie van dat elektronische-postnetwerk bevatten. De consequentie daarvan is wel dat in geval dat een onderneming 80.000 werknemers heeft, de gebruikers van elektronische post lokaal een adreslijst met 80.000 namen moeten doorzoeken op het gewenste adres van de ontvanger. Een alternatief is hier om een verkorte, lokale lijst aan te leggen met de adressen van diegenen die potentieel elektronische post via X.400 versturen en ontvangen.

De lokale bestanden worden gevoed vanuit een centrale adres-database, waarin alle actuele adressen zijn opgenomen. De beheerders van de elektronische-postsystemen zorgen ervoor dat periodiek alle mutaties centraal worden gemeld: het toevoegen, verwijderen en/of wijzigen van postbusadressen. Al deze mutaties worden handmatig in het centrale adresbestand verwerkt. Vervolgens wordt een kopie van dit bestand elektronisch naar de lokale beheerders gedistribueerd. Zij zijn weer verantwoordelijk voor de toevoeging van deze adresinformatie in de lokale adreslijsten.

Vertaal/conversie-adressen

In de paragraaf Adressering is reeds ingegaan op de problematiek rondom de vertaling van postbusadressen naar X.400. Ter ondersteuning maken sommige gateways gebruik van vertaaltabellen waarin postbusadressen met de corresponderende X.400-adressen zijn opgenomen, terwijl andere gateways het X.400-adres invullen aan de hand van de benaming van het postbusadres. Deze systemen bieden vaak niet de vrijheid en flexibiliteit om de X.400-adressen op de afgesproken wijze te gebruiken. Bij de selectie van de toe te passen gateways moet hiermee rekening worden gehouden (zie ook de checklist voor de keuze van de vereiste gateway(s) in de paragraaf Architectuur hiervoor).

BEHEER EN ADMINISTRATIE

Naast het ontwerpen en inrichten van de X.400-backbone-infrastructuur moet het beheer ervan worden geregeld alsmede de administratie voor het actualiseren van de adresinformatie en de benodigde vertaaltabellen. Afhankelijk van de wijze van exploitatie is het beheer van de backbone al dan niet uitbesteed. In beide gevallen is de onderneming zelf verantwoordelijk voor de administratie.

Adequaat beheer is een eerste voorwaarde voor de continuïteit van de netwerkstructuur ten behoeve van elektronische post. Met behulp van het noodzakelijke instrumentarium moet de elektronische-postomgeving worden bewaakt. Stagnatie van berichten, het niet kunnen ontvangen en/of afleveren van berichten en onjuiste adressering alsmede het verbreken van de noodzakelijke datacommunicatieverbindingen moeten worden gesignaleerd, geregistreerd, geanalyseerd en vervolgens opgelost. Administratie is hierbij een wezenlijk onderdeel van beheer.

Beheerinstrumentarium

In de afgelopen jaren zijn standaarden voor het beheer van met name OSI-communicatiecomponenten gedefinieerd en daarmee ook geldig voor X.400. Het betreft de OSI-systeem-managementstandaarden X.700 en X.800. Het netwerkmanagement van de huidige X.400-produkten is hierop nog niet gebaseerd. Vaak beschikken deze X.400-produkten over een geheel 'eigen' invulling van netwerkmanagement. De functionaliteit ervan varieert sterk per produkt.

Minimaal geboden netwerkmanagement-functies zijn:
- het configureren van de MTA (zie toelichting in het tweede kader verderop in dit artikel) en gateway(s);
- het al dan niet online monitoren van zend- en ontvangst-queues;
- het bijhouden van alle activiteiten van de MTA en gateways;
- het autoriseren van gebruikers van elektronische post om met X.400 te communiceren;
- het aanmaken en wijzigen van de noodzakelijke vertaaltabellen.

Beveiliging

De huidige X.400-produkten zijn gebaseerd op de 1984-versie van de X.400-standaard en bezitten nauwelijks beveiligingsfuncties. Dergelijke functionaliteit wordt pas vanaf de 1988-versie ondersteund. De benutting van deze beveiligingsfunctionaliteit vervalt indien X.400-produkten die op de 1988-aanbevelingen zijn gebaseerd, berichten uitwisselen met X.400-produkten die de 1984-standaard van X.400 ondersteunen. Daarom moet de beveiliging van informatie thans worden gezocht in het meesturen van een authenticiteitscode ter controle van de integriteit en in het versleutelen

van de meegezonden documenten ter waarborging van de vertrouwelijkheid. In geval van een privénetwerk kan ook worden volstaan met het versleutelen van de datacommunicatielijnen (line-encryptie) tussen de X.25-knooppunten.

Met de koppeling van het particuliere elektronische-postsysteem aan een openbaar X.400-netwerk wordt feitelijk de deur voor derden wijd opengezet. Zolang de adressering juist is worden inkomende berichten in principe toegelaten. Toegang aan onbekende derden, die door het versturen van zogenaamde elektronische-junkpost het postnetwerk stagneren, moet worden vermeden teneinde aanzienlijke schade te voorkomen. Denk in dit verband bijvoorbeeld aan de situatie waarin de argeloze gebruiker van elektronische post een bericht met een meegezonden besmet document van een onbekende ontvangt. Vervolgens leest hij uit nieuwsgierigheid dit document en infecteert hiermee zijn PC met een virus. Toegang tot het 'eigen' elektronische-postsysteem moet selectief worden geboden. Dit betekent dat alle elektronische post afkomstig van geautoriseerde personen zoals eigen personeel en bekend gemaakte relaties wordt doorgelaten en die van anderen niet.

Bij de semi-automatische synchronisatie van lokale adresbestanden dient expliciet aandacht te worden besteed aan de integriteitshandhaving bij de distributie van adresinformatie alsmede aan het vaststellen van de authenticiteit van de zender.

Administratie

De taken van de beheerders van elektronische-postsystemen worden uitgebreid met de administratie van de benodigde gateways voor de uitwisseling met X.400. De huidige gebruikers van het 'eigen' elektronische-postsysteem moeten een X.400-adres toegekend krijgen. Bij sommige gateways moeten ook de X.400-adressen van mogelijke zenders en/of geadresseerden van andere elektronische-postsystemen vooraf bekend zijn. Anders zijn deze gateways niet in staat de berichten te routeren.

Gebaseerd op het voorafgaande moeten vertaaltabellen en adresbestanden worden ingevoerd en onderhouden. Mutaties van lokale postbusadressen hebben al dan niet invloed op de inhoud van deze bestanden. Bij toevoeging moet de gebruiker van elektronische post de vereiste rechten toegekend krijgen om via X.400 berichten te kunnen versturen. In de regel kan elke postbushouder elektronische post via X.400 ontvangen mits zijn X.400-adres correct en bekend is.

CONCLUSIE

De integratie van elektronische post via X.400 heeft duidelijk consequenties voor de organisatie. Belangrijke aandachtspunten zijn:

- de wijze van X.400-naamgeving: bij voorkeur niet-hiërarchisch;
- de (inter)nationale identiteit van de onderneming: de verschillende nationale culturen;
- de compatibiliteit van elektronische documenten: het gebruik van dezelfde tekstverwerkers binnen de onderneming, een eenduidig software-platform;
- het beheer en de administratie: de toegankelijkheid van adresinformatie en actualiseren van de adresbestanden en de vertaaltabellen.

Voorts moeten organisaties zelf de tests uitvoeren voor de interoperabiliteit van de betrokken elektronische-postsystemen. Al met al vergt de realisatie van deze integratie met X.400 de onderneming veel inspanning en tijd.

De gehanteerde vijf aandachtsgebieden gelden in het algemeen voor de integratie van elektronische-postsystemen en hebben feitelijk niets te maken met X.400 in het bijzonder. Alleen door gebruik te maken van X.400 wordt de bijbehorende problematiek op een 'gestandaardiseerde'wijze opgelost.

Een jonge standaard als X.400 wekt de verwachting te groeien naar nieuwe mogelijkheden en toepassingen op het gebied van zowel intra- als interorganisatorische communicatie. Immers, X.400 is de schakel in de communicatie met derden. Bovendien biedt X.400 steeds meer nieuwe functionaliteit en adopteren producenten van elektronische-postsystemen X.400 als standaard binnen hun produkten. Daartegenover zien we grote verschillen in kwaliteit van met name de huidige in de markt te verkrijgen produkten voor de X.400-koppeling met de bestaande elektronische-postsystemen. Beheerders van elektronische-postsystemen worden hier met problemen geconfronteerd die gewoonlijk integraal in de bestaande elektronische-postsystemen zijn opgelost.

De X.400-standaard ontgroeit geleidelijk aan de kinderschoenen en begint volwassen te worden. Wat nog ontbreekt is de bereidheid van organisaties en ondernemingen om X.400 daadwerkelijk voor hun business-communicatie te gebruiken.

EERSTE KADER: ELEKTRONISCHE POST

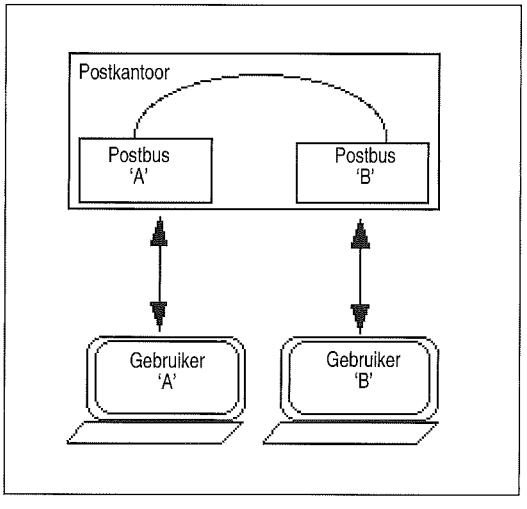
Wat is elektronische post

Elektronische post is een systeem voor transport van elektronische objecten (berichten, documenten, spraak en beelden) tussen personen, tussen applicaties, en tussen personen en applicaties. Dit transport vindt plaats over een diversiteit aan computersystemen en datacommunicatienetwerken.

Structuur elektronische-postsysteem

Een elektronische-postsysteem is te vergelijken met de postale afhandeling van brieven en documenten door PTT Post. Ook het postsysteem bestaat uit één of meer postkantoren. Deze postkantoren bezitten postbussen voor de gebruikers. In deze postbussen worden alle berichten die voor de postbushouder bestemd zijn, gedeponeerd. De postkantoren zijn met elkaar verbonden. De adresinformatie van de gebruikers van postbussen wordt onderling uitgewisseld. Op grond van de adresinformatie kunnen de postkantoren berichten van geadresseerden doorsturen naar het bestemmingspostkantoor.

Figuur 7. Structuur elektronische-postsysteem.



Voordelen van elektronische post

In iedere organisatie vindt veelvuldig communicatie tussen medewerkers plaats. Daartoe beschikken zij over een verscheidenheid aan communicatiemiddelen als telefoon, telex en telefax alsmede (intern) postaal en koerierverkeer. Telefoneren bijvoorbeeld is persoonlijk, het gaat eenvoudig en kan snel. Voor zover nog niet gebruik wordt gemaakt van een antwoordapparaat is een groot nadeel dat de gewenste persoon wel aanwezig moet zijn. Er is dus een zekere voorwaarde zowel in tijd als in plaats. Voor elektronische post gelden deze voorwaarden niet. Een boodschap kan worden achtergelaten zonder dat de geadresseerde aanwezig is op zijn of haar werkplek, zelfs zonder dat er sprake is van een vaste werkplek. Zodra er gebruik wordt gemaakt van het elektronische-postsysteem worden berichten 'afgeleverd' en kan de gewenste actie worden ondernomen.

Daarentegen vereist het gebruik van elektronische post een zekere mate van discipline. Een dringend verzoek via elektronische post heeft geen zin als de geadresseerde een aantal dagen zijn post niet leest.

De voordelen worden nog groter bij het uitwisselen van formele documenten. Verspreiding vindt sneller plaats. Bovendien kan de elektronische versie van documenten verder worden verwerkt. Elektronische post biedt derhalve een aantal voordelen die een belangrijke bijdrage kunnen leveren aan de verbetering van de effectiviteit van de interpersoonlijke communicatie en daarmede een verhoging van de produktiviteit.

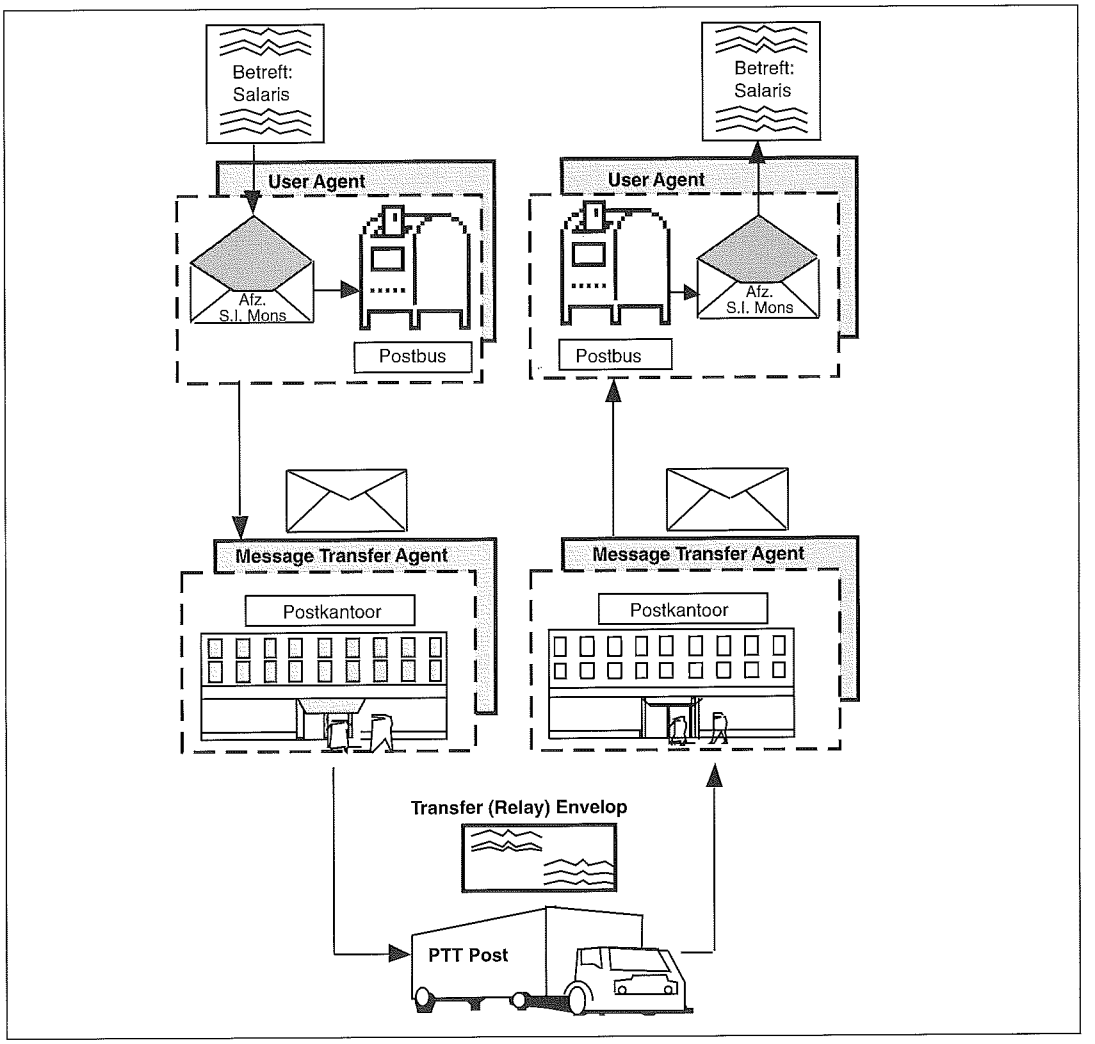
Voor grote organisaties met verscheidene vestigingen die geografisch (inter)nationaal verspreid zijn, wordt het uitwisselen van informatie eenvoudiger. Gebruikers van elektronische post hoeven niet meer na te denken over tijdverschillen en kantoortijden van vestigingen. Het bericht staat klaar als er aan de andere kant van de wereld gewerkt gaat worden.

TWEEDE KADER: X.400

Message Handling System

X.400 is een formele beschrijving van een structuur voor een elektronische-postsysteem om berichten binnen een datacommunicatienetwerk af te handelen. Zo'n elektronische-postsysteem wordt een *Message Handling System* (MHS) genoemd. Naast postkantoren en postbussen beschrijft X.400 ook de wijze van transfer van elektronische post: store and forward-principe (opslag en transport). Dat wil zeggen dat een bericht bij het passeren van een postkantoor tijdelijk wordt opgeslagen alvorens het wordt doorgestuurd naar een volgend postkantoor dan wel in de gewenste postbus van de geadresseerde wordt gedeponeerd.

Figuur 8. Traditionele postafhandeling.



Open standaard elektronische post

In 1984 heeft een internationale normalisatie-organisatie voor telecommunicatie, het Comité Consultatif International Télégraphique et Téléphonique (CCITT), de aanbevelingen van de X.400-standaard geïntroduceerd. CCITT kwam in 1988 met een nieuwe verzameling aanbevelingen. Deze versie kent vooral meer functionaliteit voor beveiliging (autorisatie, authenticiteit en integriteit). Bovendien volgt deze versie de open standaarden van ISO (International Standardization Organization). Eind 1992 werden reeds de 1992-X.400-aanbevelingen geratificeerd. Ze bevatten met name voor toepassing van Electronic Data Interchange (EDI) toegevoegde functionaliteit.

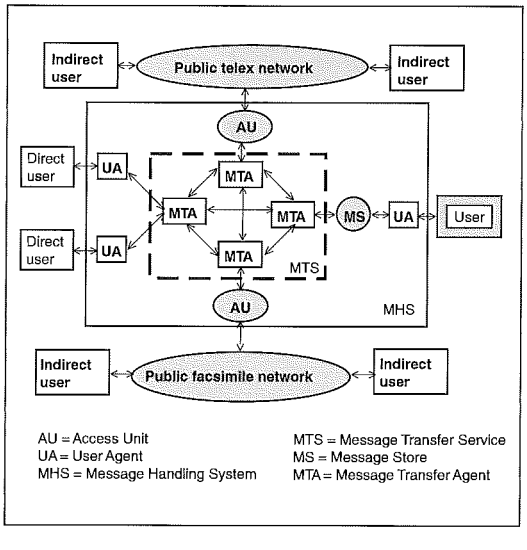
De X.400-standaard is onafhankelijk van de hardware-architectuur gedefinieerd en is daarmee een open systeem. Dit betekent dat systemen, hoewel ze op verschillende apparatuur geïmplementeerd kunnen zijn, toch onderling kunnen samenwerken.

Message Transfer Agent en User Agent

De kern van de X.400-MHS-omgeving is de *Message Transfer Service* (MTS), die zorgt voor de uitwisseling van informatie tussen de diverse op het netwerk opererende systemen. De MTS is opgebouwd uit één of meer postkantoren, de *Message Transfer Agents* (MTA's). De functie van een MTA bestaat uit het routeren en doorsturen van berichten naar een naastliggend MTA, en het afleveren van de informatie op de eindbestemming.

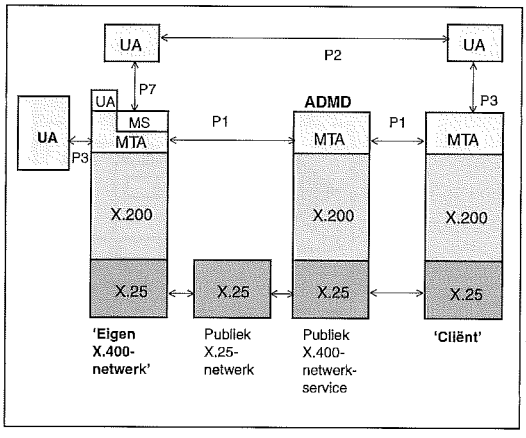
De MTA's vormen te zamen met de op de MTS aangesloten computers, de User Agents (UA's), de twee basiselementen van een X.400-MHS. De UA vertegenwoordigt hier de postbus van een geadresseerde. De UA kan ook worden aangeduid als Access Unit (AU) of soms als Message Store (MS), naargelang de functie die hij vervult. Het fundamentele verschil tussen UA en AU is dat een UA bestemd is voor interpersoonlijke communicatie, terwijl een AU de koppeling verzorgt met andere communicatiewerelden zoals telex, teletex, telefax of zelfs fysieke post. Daarentegen kan de MS beschouwd worden als het verlengstuk van een UA.
Iedere UA kan één dienst ondersteunen. Elektronische post en EDI kunnen niet via één UA worden verstuurd. Hiervoor dienen aparte UA's te worden ingericht.

Figuur 9. Message Handling Environment.



Protocollen

Tussen UA's zijn protocollen afgesproken: de *Inter Personal Message* (IPM) voor het uitwisselen van elektronische post en een EDI-protocol voor gestructureerde uitwisseling tussen applicaties. Evenzo kent X.400 standaardprotocollen voor de uitwisseling van berichten tussen MTA's onderling en tussen MTA en UA: respectievelijk P1- en P3-protocol. IPM wordt ook wel het P2-protocol genoemd. Het P7-protocol heeft betrekking op de communicatie tussen UA en MS.



Figuur 10. Protocollen.

X.400-envelop

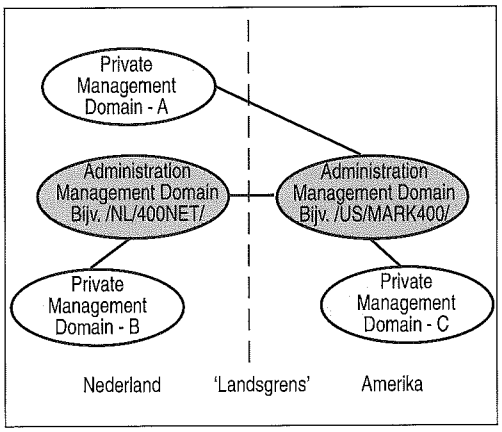
In analogie met de traditionele papieren post bestaan X.400-berichten uit een envelop en inhoud. De envelop bevat ten minste de adressen van een geadresseerde en een afzender. Deze gegevens zijn nodig om de sorteerders en bezorgers aan te sturen. Additioneel kan de envelop zendgegevens bevatten, zoals 'spoed' of 'aangetekend', en dienovereenkomstig als respectievelijk exprespost of aangetekende brief worden bezorgd. In het laatste geval zal aan de afzender ook een bevestiging van ontvangst worden gevraagd.

Management Domeinen

De X.400-omgeving onderscheidt een tweetal domeinen: een Administration Management Domain (ADMD) en een Private Management Domain (PRMD). Een ADMD heeft betrekking op openbare X.400-netwerk(diensten) beheerd door nationale PTT's en andere zogenaamde Value Added Network (VAN)-leveranciers. PRMD duidt het privé elektronische-postsysteem van een organisatie aan.

Momenteel beperken domeinen zich tot één land; landsgrenzen kunnen alleen door koppeling tussen ADMD's worden overschreden. Onder druk van verschillende grote internationale ondernemingen, die hun eigen domein niet tot één land beperken, lijkt het erop dat de X.400-aanbevelingen op dit punt moeten worden bijgesteld. In principe mogen alleen ADMD's onderling direct met elkaar gekoppeld zijn. Dit geldt niet voor PRMD's. Deze mogen uitsluitend met elkaar communiceren via ten minste één ADMD. In afwijking van de X.400-standaard worden PRMD's in de praktijk echter wel direct aangesloten op ADMD's die in een ander land zijn geregistreerd.
Thans is met X.400 een standaard ontstaan vanuit de belangen van de PTT's, maar deze zal door de toenemende marktvraag uitkristalliseren tot datgene wat uiteindelijk aansluit op de wensen van met name de grote ondernemingen.

Figuur 11. ADMD en PRMD.



LITERATUUR

[Evel93] E.J. Evelo, *Netwerkmanagement, de organisatorische opzet en financiële beheersing*, Compact 1993/1.

X.400: CCITT Blue book - Volume VIII - Fascile VIII.7, *Data Communications Network Message Handling Systems*, Recommendations X.400 - X.420, 1988.

X.500: CCITT Blue book - Volume VIII - Fascile VIII.8, *Data Communications Network Directory*, Recommendations X.500 - X.520, 1988.

X.700: Information processing systems - Open Systems Interconnection - Basic Reference model - Part 4: Management Framework (DIS 7498-4), 1988.

X.800: Information processing systems - Open Systems Interconnection - Basic Reference model - Part 2: Security Architecture (ISO 7498-2), 1988.

[Viss92] C.H. Visser, *Elektronische post*, Handboek Apple Macintosh aflevering 19, juni 1992.

Ir. A. van Kooij
Is sinds 1990 werkzaam als Telecommunications Consultant bij KPMG Klynveld Management Consultants. Zijn advies gebied betreft lokale en Wide Area-netwerken en de geboden netwerkfunctionaliteit zoals X.400 en X.500. In dat kader is hij betrokken bij ontwerp, selectie, realisatie en invoering van een wereldwijd X.400-netwerk voor de koppeling van bestaande elektronische-postsystemen.

EDP AUDITORIUM

BOEKBESPREKING

Informatie-economie; investeringsstrategie voor de informatievoorziening, R. van Oirsouw, J. Spaanderman en H. de Vries

Drs. E.W. Berghout

Inleiding

Het boek is geschreven om mensen te helpen die investeringsbeslissingen over informatiesystemen moeten nemen. De auteurs hebben zich daarbij geconcentreerd op, zoals zij zelf zeggen, 'het slaan van een brug tussen het 'informatisch' denken en het 'bedrijfseconomisch' denken'.

De auteurs definiëren informatie-economie als 'een management-benadering van de automatiseringsportefeuille'. Hierbij worden bedrijfseconomische technieken gecombineerd met technieken uit de informatieplanning, met als doel een scherp beeld te geven van:

a. de kosten en baten van automatiserings- en informatiseringsprojecten;
b. de bijdrage van ieder project aan het functioneren en de realisatie van de strategie van de onderneming;
c. de urgentie van de te onderscheiden projecten;
d. de risico's die de organisatie loopt met ieder project.

Het boek bevat daarvoor een verzameling praktische methoden en technieken. Deze zijn veelal gebaseerd op werk van andere auteurs (vooral het werk van M. Parker, R. Benson en H. Trainor wordt vaak aangehaald). De diverse bronnen zijn op een coherente manier samengebracht en soms aangepast aan de ideeën van de auteurs. De onderwerpen in het boek worden geïllustreerd met veel voorbeelden. Het boek is door de vele voorbeelden duidelijk ook bedoeld als studieboek voor het hoger onderwijs.

Onderwerpen

Het boek bestaat uit vier delen. Hieronder volgt een korte samenvatting.

In het eerste deel, getiteld *Concept*, worden de benodigde begrippen uitgelegd die in het boek zullen worden gehanteerd, zoals kosten, baten, waarde en risico's. Tevens wordt de kern van het boek geïntroduceerd: de scorecard-techniek. Hiermee zullen de diverse voorstellen voor informatiesystemen worden beoordeeld op:

a. De initiële investering, om een indruk te krijgen van de financiële omvang van een project.

b. Het 'return-on-investment', als maat voor de financiële aantrekkelijkheid van een voorstel.

c. De bijdrage, als maat voor de niet-financiële baten van een voorstel. De bijdrage wordt opgebouwd met behulp van de waardecategorieën 'strategic match', 'competitive advantage', 'management information' en 'competitive response'. Het relatieve belang van een waardecategorie ten opzichte van een andere waardecategorie wordt uitgedrukt door het toekennen van een weegfactor. De bijdrage van een voorstel wordt bepaald door de som van de scores per categorie nadat deze met de weegfactor is vermenigvuldigd.

d. Risico-index, de som van de verschillende risicocategorieën. Dit zijn 'strategic IS architecture', 'project/organizational risk', 'definitial uncertainty', 'technical uncertainty' en 'infrastructure risk'.

In het tweede deel van het boek, getiteld *Scorecards*, wordt de scorecard-techniek verder beschreven. Er wordt vooral ingegaan op hoe de techniek in de praktijk kan worden toegepast. Er wordt uitgelegd hoe:

- de 'verwachte contante return-on-investment' kan worden berekend;
- de diverse niet-financiële bijdragen kunnen worden geïdentificeerd;
- de risico's kunnen worden ingeschat.

Het derde deel van het boek, getiteld *Proces*, gaat specifiek in op het probleem van het bepalen van weegfactoren voor het afwegen van het relatieve belang van de niet-financiële baten.
Vijf strategieën worden behandeld:

1. Het weglaten van een weging.

2. Het bepalen van de weegfactoren met behulp van de kritieke succesfactoren van een organisatie.

3. Het bepalen van de weging met behulp van de contingentiefactoren van een organisatie (zeven factoren van Mintzberg worden aangehaald: leeftijd/omvang van de organisatie, regulering door het operationele proces, dynamiek van de omgeving, complexiteit van de omgeving, diversiteit van markten en vijandigheid van de omgeving).

4. Het bepalen van de weging op basis van de positie van de bedrijfsactiviteit waarop het informatiesysteem van toepassing is in de portfolio van de Boston Consulting Group. Bedrijfsactiviteiten worden in deze portfolio getypeerd als 'dog', 'problem child', 'star' of 'cash cow'.

5. Het bepalen van de weging door middel van een paneldiscussie door alle betrokken beleidsmakers.

Tevens wordt ingegaan op combinaties van wegingsstrategieën.

Het vierde deel van het boek, getiteld Toepassing, gaat in op specifieke problemen bij het gebruiken van de verschillende technieken. Aan de orde komen:

a. het in de praktijk identificeren van kosten;
b. de mogelijkheden om kosten door te belasten;
c. de problemen bij het invoeren van de diverse technieken uit de informatie-economie in een organisatie. Hierbij wordt ingegaan op de invloed van de organisatiecultuur, de omgeving van de organisatie en het kennisniveau van de organisatie met betrekking tot informatie-economie.

Er wordt een stappenplan gegeven voor het verbeteren van de besluitvorming met betrekking tot voorstellen voor informatiesystemen.

Verwarrende terminologie

Het boek leest bijzonder makkelijk, maar heeft, mijns inziens, één groot nadeel, namelijk de verwarrende terminologie. Men heeft de termen kosten en baten als uitgangspunt genomen en moet vervolgens onderscheid kunnen maken tussen financiële en niet-financiële voor- en nadelen van informatiesystemen. Met betrekking tot de financiële voor- en nadelen moet verder nog onderscheid kunnen worden gemaakt tussen de economische begrippen resultaat (in de vorm van winst of verlies) en kasstromen.

De auteurs gebruiken de term kosten voor alle nadelen, en baten voor alle voordelen (zowel financiële als niet-financiële) die aan het invoeren van een informatiesysteem zijn verbonden. Voor het aanduiden van de financiële consequenties worden de termen '(financiële) baten' en wederom kosten gebruikt. Voor het aanduiden van de niet-financiële consequenties worden de termen bijdrage en waarde gebruikt (waarde was de som van de gewogen bijdragen van een specifiek informatiesysteem).

De term waarde wordt nu gebruikt om niet-financiële consequenties aan te duiden. Baten worden wel uitgesplitst in '(financiële) baten' en (niet-financiële) bijdrage, maar kosten worden niet uitgesplitst. Door de termen kosten en baten als uitgangspunt te nemen, ontstaan er problemen bij de uitleg van de investeringsanalyse. Bij een investeringsanalyse wordt uitgegaan van kasstromen in plaats van kosten (kosten zijn de geldswaarde van de produktiemiddelen die men opoffert). Een andere consequentie van dit begrippenkader is dat met kosten soms offers, soms uitgaven en soms zowel financiële als niet-financiële nadelen worden bedoeld. Zaken zoals de verslechtering van de arbeidsomstandigheden zijn hierdoor moeilijk aan te duiden, want er bestaat geen term voor niet-financiële nadelen. De terminologie geeft eveneens aanleiding tot merkwaardige constructies. In het boek worden uitdrukkingen als 'batige kasstromen' en 'kosten in geld' gebruikt.

Men had bijvoorbeeld beter het begrippenkader van prof.drs. B.K. Brussaard kunnen hanteren (*Organisatie van de informatievoorziening*, T.U. Delft, 1993). Deze hanteert de begrippenparen baten en lasten voor alle voor- en nadelen, kosten en opbrengsten voor de financiële voor- en nadelen, en uitgaven en inkomsten voor alle positieve en negatieve kasstromen die aan een specifieke investering zijn verbonden.

Conclusie

Informatici die de besluitvorming rond automatiseringsprojecten in hun organisatie willen verbeteren, kunnen veel aan de informatie in het boek hebben. Men heeft met de scorecard-techniek een uitgebreid inschattings- en overlegmodel in handen om in een organisatie te kunnen discussiëren over de voor- en nadelen van voorstellen voor informatiesystemen. Het begrippenkader dat in het boek wordt gehanteerd, had beter moeten zijn. Nu blijft het risico aanwezig dat slecht-willenden, als excuus om een goede analyse achterwege te laten, blijven herhalen dat de baten van informatiesystemen toch te moeilijk te achterhalen zijn. Het feit dat het boek in plezierig Nederlands is geschreven en veel duidelijk herkenbare voorbeelden bevat, maakt veel goed.

Informatie-economie: investeringsstrategie voor de informatievoorziening, R. van Oirsouw, J. Spaanderman en H. de Vries, Academic Service, Schoonhoven 1993, ISBN 90-5261-052-5, prijs *f* 58/BF 1160.

BOEKBESPREKING

De weg naar kwaliteitsverbetering, Drs.ir. B. van Melle

Drs. P.P.M.G.G. Brouwers

Inleiding

In de praktijk wordt men bij de uitvoering van EDP-audit-opdrachten regelmatig geconfronteerd met diverse aspecten die een rol spelen bij de invoering van een kwaliteitssysteem. Dit is zeker niet opzienbarend daar ongeveer zestig procent van de IT-bedrijven werkt aan het verkrijgen van een certificaat voor een kwaliteitssysteem in de komende twee jaren. In Nederland zijn inmiddels tussen de vijftienhonderd en tweeduizend gecertificeerde bedrijven en dit aantal groeit met enkele per dag. Dat er iets aan de kwaliteitszorg van een organisatie moet worden gedaan, wordt meestal wel ingezien, maar op welke wijze hieraan praktische invulling kan worden gegeven, is dikwijls nog een openstaande vraag voor het management.

Dit boek geeft inzicht op welke manier invulling kan worden gegeven aan het kwaliteitsdenken. Het is tot stand gekomen op basis van praktijkervaringen die de auteur heeft opgedaan bij kwaliteitszorgprojecten bij Nederlandse bedrijven uit diverse branches. De auteur van het boek is als organisatie-adviseur verbonden aan KPMG Bywater Nederland (het samenwerkingsverband tussen

KPMG Klynveld Management Consultants en Bywater plc te Chertsey), dat zich bezighoudt met advisering op het gebied van kwaliteitszorg.

Over het boek

Het boek geeft geen diepgaande uiteenzetting van de theoretische principes achter het kwaliteitsdenken, maar geeft beknopt weer op welke wijze in de praktijk op een verantwoorde manier met kwaliteitszorg kan worden omgegaan. Met behulp van een case wordt een geheel kwaliteitsproject doorlopen: vanaf de aanleiding voor het besluit tot certificering, de motieven voor het inschakelen van een externe adviseur, een beschrijving van de te ondernemen activiteiten voor een kwaliteitszorgproject, de ondersteuning door hulpmiddelen tot de resultaten van de ondernomen activiteiten. In de case wordt de implementatie van de ISO-9002-norm bij een organisatie gevolgd. De case wordt afgewisseld met beknopte theoretische achtergronden van het kwaliteitsdenken. Het boek wordt ten slotte afgerond met tien stellingen over kwaliteitszorg.

Opbouw van het boek

In eerste instantie wordt de case beschreven die in het boek verder wordt gevolgd.
Hierbij worden enkele kerncijfers van de organisatie genoemd, wordt de marktsituatie toegelicht en wordt het organisatieschema gepresenteerd.
Tevens worden beknopt de interne en externe motieven aangegeven die de aanleiding vormen voor het opstarten van het kwaliteitsproject.
Hierna volgt een beknopte toelichting op de termen kwaliteit en kwaliteitszorg. Kwaliteit wordt in dit boek omschreven als 'het voldoen aan overeengekomen eisen ten aanzien van produkt, proces en organisatie'. Deze kwaliteit moet binnen een organisatie worden gewaarborgd via kwaliteitszorg, dat wordt omschreven als 'een benaderingswijze die als doel heeft de continue verbetering van de effectiviteit en efficiëntie van produkt, proces en organisatie'.
De auteur stelt vervolgens dat in succesvolle kwaliteitszorgprojecten op gebalanceerde wijze aandacht moet worden besteed aan drie kritische factoren van de kwaliteitszorg: het kwaliteitssysteem, de metingen en de mensen. Deze factoren worden verderop in het boek uitgebreid behandeld.

Eerst gaat de auteur in op welke wijze een kwaliteitszorgproject binnen een organisatie kan worden gelanceerd via een workshop. Hierna worden algemene uitgangspunten aangereikt waaraan een kwaliteitsaanpak moet voldoen :
- een planmatige aanpak;
- top-down implementatie;
- bottom-up participatie;
- het kennen van klanteneisen;
- communicatie.

Vervolgens wordt in de volgende hoofdstukken ingegaan op de onderkende kritische factoren van een kwaliteitsproject.
Het kwaliteitssysteem

In dit hoofdstuk worden de verschillende onderdelen van het kwaliteitssysteem toegelicht en de wijze waarop deze onderdelen in de praktijk kunnen worden gerealiseerd. Als belangrijkste onderdelen van een kwaliteitssysteem onderkent de auteur een kwaliteitshandboek, procedures en werkinstructies. Het kwaliteitshandboek bevat doorgaans onderdelen als het beleid en de doelstellingen van de organisatie, de organisatiestructuur, een samenvatting van het kwaliteitssysteem en een overzicht van procedures.
Vervolgens wordt ingegaan op de vraag voor welke activiteiten binnen een organisatie procedures moeten worden opgesteld of dat voor bepaalde activiteiten met werkinstructies of een gedegen training kan worden volstaan. Om dit te bepalen wordt de volgende matrix als hulpmiddel gehanteerd.

		Activiteit kritiek?	
		JA	NEE
Raakvlak? (Tussen afdelingen)	JA	Procedure Functie-omschrijving Training	Functie-omschrijving Training
	NEE	Werkinstructie Functie-omschrijving Training	Training

Aan de hand van de case wordt duidelijk toegelicht op welke manier procedures in de praktijk moeten worden opgesteld, welke onderdelen deel uitmaken van een procedure, wat aan bod komt tijdens een proceduretraining en op welke manier in de praktijk kan worden vastgesteld of ook volgens de procedures wordt gehandeld.

De metingen
Deze kritische factor is noodzakelijk om vast te stellen in welke mate wordt voldaan aan de overeengekomen eisen op een bepaald gebied: de zogenaamde kwaliteitsindicatoren. De metingen kunnen tevens worden gebruikt om de medewerkers te motiveren door de kwaliteitsgedachte in 'harde' guldens uit te drukken. In het boek wordt zeer uitgebreid ingegaan op een speciale groep kwaliteitsindicatoren, namelijk de faalkosten. Hiermee worden bedoeld de kosten die ontstaan ten gevolge van afwijkingen en fouten in de dagelijkse gang van zaken.
In het resterende deel van het hoofdstuk worden technieken en mogelijke analysevormen aangereikt op basis waarvan een faalkostenonderzoek in een organisatie kan worden uitgevoerd.
Vervolgens kunnen op basis van de resultaten van een faalkostenonderzoek verbeterprojecten in een organisatie worden geïdentificeerd.

Opvallend zijn nog enkele statistische cijfers die de auteur op basis van een onderzoek van het ministerie van Economische Zaken noemt. Enige tijd geleden bedroegen de faalkosten in het Nederlandse

bedrijfsleven circa twintig miljard gulden. Deze twintig miljard zijn er eigenlijk veertig. Aangenomen wordt namelijk dat de helft van het bedrag relatief gemakkelijk vermijdbaar is. Twintig miljard is dan het verbeterpotentieel. Tevens wordt aangegeven dat bij de meeste industriële concerns de faalkosten tussen de tien en twintig procent van de omzet lagen. Het bedrag wordt ondersteund door een onderzoek van McKinsey bij vijfhonderd Europese bedrijven. Dit bureau komt op een gemiddelde van zeventien procent faalkosten over de totale kosten.

De mensen
Bij de laatste kritische factor worden de belangrijkste punten behandeld die een rol spelen bij de kwaliteitsbewustwording bij de mensen in een organisatie, namelijk:
- de betrokkenheid op alle niveaus in de organisatie;
- opleiding en training;
- het belang van het management;
- open communicatie.

Het boek wordt afgesloten met tien stellingen over kwaliteitszorg, waarvan enkele EDP-auditors zeker tot nadenken zullen stemmen.

Tot slot

Het is een vlot geschreven boek. Met name de casebeschrijving zorgt ervoor dat men van een kwaliteitsproject een zeer praktische voorstelling van zaken krijgt. De casebeschrijving is natuurlijk zo ingericht dat de toegevoegde waarde van het kwaliteitssysteem overduidelijk wordt aangetoond. Dit leidt soms tot een wel zeer simpele voorstelling van zaken. Met name op het gebied van de kwantificering van de faalkosten is dit het geval. Tevens zou naar mijn mening een kort overzicht wenselijk zijn geweest inzake certificering in zijn algemeenheid (welke standaarden inzake certificering worden onderkend, wat zijn de verschillen tussen die standaarden en waarop hebben die standaarden specifiek betrekking).

Het boek geeft duidelijk aan op welke wijze externe deskundigen ondersteuning kunnen geven aan organisaties bij het behalen van een kwaliteitscertificaat. Tevens geeft het boek voor managers een uitstekend overzicht van activiteiten en de wijze waarop deze moeten worden uitgevoerd om een kwaliteitsproject succesvol te implementeren. Het boek benadrukt nogmaals dat certificering slechts het begin van kwaliteitszorg is. Het betreft namelijk een certificaat aangaande het kwaliteitssysteem en niet ten aanzien van de aangeboden produkten of de verleende diensten. Een certificaat geeft dus nog zeker geen garanties dat de produkten of diensten voldoen aan de eisen van de afnemers.

Het dient bij de certificering om het proces te gaan en niet om het behalen van het papiertje aan de wand!! (Hoewel in de praktijk ...)

De weg naar kwaliteitsverbetering, B. van Melle, met bijdragen van H.J. Hagenberg en J.J.M. Laan, KPMG Klynveld Management Consultants, Kluwer VNO, 1991, ISBN 90 200 1380 7.

CUMULATIEF

Overzicht van eerder verschenen artikelen in Compact

Een selectie van geactualiseerde artikelen uit de $12^1/_2$ jaar Compact 1974 - 1986 is opgenomen in het boek *24 over EDP-auditing*. 24 auteurs over EDP-auditing in theorie en praktijk: visies, ontwikkelingen, werkwijzen en oplossingen.
Het boek is verkrijgbaar via de boekhandel onder nummer: ISBN 90 14 03648 5.

2 19e jaargang 92/2 zomer 1992

Investeren in informatietechnologie:
take IT or leave IT
drs.ing. G.J.P. Swinkels en drs. H.G.P. van Irsel

Managing with Information Technology
- a decade of wasted money?
ir. M.C.A. van Nievelt

Informatietechnologie in een kantooromgeving:
produktiviteitsmanagement van kantoorarbeid en kantoorautomatisering
drs. F.R.E. Lekanne Deprez

Het plannen en rechtvaardigen van infrastructurele IT-investeringen
drs. H.G.P. van Irsel en P. Fluitsma

Uitbesteding van automatisering:
more than make or buy
mw. drs. H.W.A. van den Heuvel en mw. mr. A.M.Ch. Kemna MBA

3 19e jaargang 92/3 herfst 1992

De EDI-infrastructuur bij de Kas-Associatie
P. van Berge

Beheersbaarheid van het EDI-verkeer in de praktijk
G.J. Endenburg RI

EDI bij de Rijksdienst voor het Wegverkeer
J.W.J. Laan

EDI, een strategisch perspectief voor het bankwezen
drs. M.A. Bongers RE en mw.drs. M. Steeman

Beheersing van inzet en gebruik IT:
van kopzorg tot hoofdzaak
drs. G.C.M. Mol en drs. J.F.H. Vrins

4 19e jaargang 92/4 winter 1992

De veiligheid van betaalautomaten
E.R. Fekkes

S.W.I.F.T. and Security
This article was produced by S.W.I.F.T. s.c. Marketing and the Chief Inspector's Office

Het binnenlandse traject van SWIFT-posten;
het SWIFT-8007-circuit
drs. F.G. Knaack

Betrouwbaarheid van het FA-systeem
drs. R. Oudega

Een Nederlandse standaard voor de elektronische handtekening
mw.drs. M.C. van Lith

De beveiliging van elektronisch bankieren
mw.drs. M.C. van Lith

Secure Cash Management; a case study
H. Roos RA and H. Veenman MBT

Beveiligingsaspecten en juridische aspecten als communicerende vaten
ir. G.J. Schuringa en mr. R.E. van Esch

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