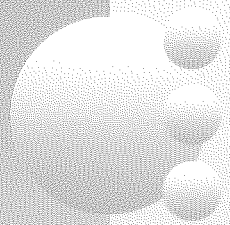
COMPACT

TIJDSCHRIFT EDP-AUDITING



INVESTEREN IN IT
BENCHMARKING
AS/400 NETWORKING

1996/2

Compact ®
Jaargang 23, nummer 2
Een uitgave van KPMG EDP Auditors NV en Samsom Bedrijfs-Informatie, werkmaatschappij van Wolters Kluwer NV.
Het blad verschijnt 6 x per jaar.
Redactie
Prof. A.W. Neisingh RE RA (hoofdredacteur)
J.C. Boer RE RA
Ir. J.A.M. Donkers RE
Drs. R.G.A. Fijneman RE RA
Drs. P. Veltman RE RA
Ir.drs. J. van der Vlugt
Adviesraad
Prof.dr. J.C. Arnbak
J.H. Buisman RA
Mr. P. van Dijken
Prof.mr. H. Franken
Dr. K.IJ. Mollema RA
Prof. H.B. Moonen RE RA
Prof.dr.ir. R. Paans RE
Redactiesecretariaat
Mw. I. de Koning, Samsom Bedrijfsinformatie, Postbus 4, 2400 MA Alphen aan den Rijn
Tel.: 0172 – 466 746
Fax : 0172 – 466 569
Vormgeving
Bureau Karakter, Delft
Opmaak
Sander Pinkse Boekproduktie, Amsterdam
Abonnementen
f 165,- per jaar incl. BTW. Losse nummers f 45,- incl. BTW. Studentenabonnement f 95,- incl. BTW. Abonnementen kunnen schriftelijk tot uiterlijk één maand voor de aanvang van een nieuw abonnementsjaar worden opgezegd. Bij niet tijdige opzegging wordt het abonnement automatisch met een jaar verlengd.
Abonnementsadministratie
Samsom Bedrijfsinformatie, Postbus 4, 2400 MA Alphen aan den Rijn
Tel.: 0172 – 466 800
Fax : 0172 – 475 933
Adreswijzigingen – ook tijdelijke – moeten minstens 8 weken voor de verschijningsdatum bekend zijn.
Overname artikelen
Het overnemen en vermenigvuldigen van artikelen en berichten is slechts geoorloofd na schriftelijke toestemming van de uitgever.
Overdrukken artikelen
Overdrukken van artikelen kunnen worden aangevraagd bij het redactiesecretariaat. Prijs per overdruk per artikel (inclusief omslag) f 5,-.

Uitgever
Drs. ing. O.A. Rouwendal

NOTU VAK
Lid van de Nederlandse organisatie van tijdschriftuitgevers NOTU

ISSN 0920 – 1645

INHOUDSOPGAVE

REDACTIONEEL

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

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

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

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

De besluitvorming over IT-aangelegenheden krijgt een steeds grotere reikwijdte en neemt toe in complexiteit. Dit wordt enerzijds veroorzaakt door de groei van de inzet van informatietechnologie, waardoor binnen het vakgebied steeds meer specialisaties moeten ontstaan met evenzoveel meer plaatsen waar vernieuwing kan optreden. Anderzijds wordt informatietechnologie steeds meer geïntegreerd met de overige ondersteunende werkzaamheden in organisaties. Hierdoor zullen de bestaande eisen voor de beheersbaarheid in toenemende mate ook aan informatietechnologie worden gesteld; de betrokken afdelingen verliezen hun geprivilegieerde positie.

Deze ontwikkelingen betekenen dat er op alle niveaus een toenemende behoefte bestaat aan structurering van de IT-management-werkzaamheden. Hiermee kunnen de verwachtingen en het beheer van IT-aangelegenheden beter in de hand worden gehouden.
In dit opzicht is het belangrijk om te onderkennen dat de IT-wereld geen statisch geheel is, maar een continue en snelle verandering ondergaat. Hierdoor is het niet goed mogelijk bestaande beheerstechnieken onveranderd te gebruiken.
Op managementniveau betekent dit in veel gevallen dat de besluitvorming ten aanzien van investeringen in informatietechnologie wordt gerationaliseerd.

In deze Compact treft u drie artikelen aan die zich richten op dit structureringsproces. Allereerst wordt de besluitvorming ten aanzien van IT-investeringen onder de loep genomen, waarna aandacht wordt besteed aan benchmarking van general IT controls. Een omvangrijk artikel gaat in op het opnemen van meerdere AS/400-systemen in een netwerk, waarbij zowel de eisen van interne controle als de audit op de implementatie ervan in zo'n omgeving worden besproken.
In het EDP Auditorium volgen ten slotte twee besprekingen van proefschriften waarin respectievelijk de relatie tussen technische normen en het recht, en de belangrijkste benaderingen voor informatiebeveiliging worden onderzocht.

Op deze wijze komt de beheersing van informatietechnologie door het management vanuit verschillende gezichtspunten aan de orde.

Ir. drs. J. van der Vlugt

TERUGTREDEN P. VELTMAN

Na een jarenlange intensieve betrokkenheid bij de totstandkoming van Compact heeft Piet Veltman besloten de redactie te verlaten. De redactie betreurt dit besluit, echter van zijn inbreng zal zeker 'langs de zijlijn' nog gebruik worden gemaakt.
De redactie is Piet Veltman veel dank verschuldigd voor de wijze waarop hij 'met de stofkam' door de aangeboden artikelen ging. Het doet de lezers en (potentiële) schrijvers wellicht deugd dat ook mederedactieleden deze procedure moesten ondergaan. Sommige artikelen van hen hebben het dan ook evenmin gehaald.
Piet, bedankt.

Dries Neisingh

Besluitvorming over IT-investeringen: gebruik de juiste criteria

Ing. E.M.H. Coorens BE MBA,
drs. P.J.C. van Bladel en
dr. M. Boogaard

Besluitvorming over IT-investeringen vergt een besluitvormingsproces dat geïntegreerd is in de algehele bedrijfsvoering en waarbij de analyse-inspanningen afgestemd zijn op het type IT-project. Probleem hierbij is vaak dat het algemeen management een IT-investering niet geheel kan overzien, met name als dit overzicht in relatie tot de totale projecten-portfolio nodig is. In dit artikel worden met name de samenstelling van de projecten-portfolio op basis van categorisering van projecten en de allocatie van middelen naar die categorieën besproken.

INLEIDING

Het (toenemende) belang van informatietechnologie hoeft geen nader betoog ([Nais90]).
Parallel aan het groeiende belang van informatietechnologie is de algehele informatievoorziening en bijbehorende gegevensverwerking een steeds belangrijker onderdeel van strategisch management geworden. Het daadwerkelijk strategische aspect is hoe informatie en informatievoorziening (en dus informatietechnologie) gebruikt kunnen worden om de algemene bedrijfsstrategie te ondersteunen. Dit is meer en meer een aspect van concurrentiekracht geworden.

John Rockart benadrukt het belang van de ontwikkeling van informatiesystemen die sleutelinformatie voor topbeslissers genereren om de kritieke succesfactoren van een organisatie te managen ([Rock79]). 'Business alignment' is een vereiste voor deze 'systems alignment'. Een bedrijf dat bijvoorbeeld net heeft besloten om het transport volledig uit te besteden, zal geen nieuwe trucks gaan aanschaffen. Net zo min zou een organisatie die met een ingrijpend proces-herontwerp-traject bezig is grote investeringen moeten doen in de automatisering van de oude processen. Toch blijkt deze afstemming in de praktijk nog verre van gerealiseerd. Onderzoeken van onder anderen Gianotten ([Gian91]) en Mantz ([Mant90]) geven dit duidelijk aan. Het belangrijkste aspect is dus niet het managen van de technologie, maar het managen van de informatievoorziening. Meyer en Boone beweren zelfs dat wanneer in organisaties informatiesystemen niet adequaat zijn afgestemd op de bedrijfsstrategie, informatiesystemen en informatietechnologie de organisatie alleen maar helpen om sneller in de verkeerde richting te gaan ([Meye89]). Het Strategic Alignment Model kan als vereenvoudiging van de essentiële onderdelen van een organisatie een goed hulpmiddel zijn voor het bereiken van deze zo noodzakelijke onderlinge afstemming ([Hend93]).

Diverse publikaties (onder andere [Park88], [Oirs93], [Swin92] en [Oost92]) behandelen modellen om besluitvorming over informatietechnologie te faciliteren. Ook het themanummer 1992/2 van Compact gaat hier uitvoerig op in.
In dit artikel wordt geen nieuwe methode of de grootste gemene deler van de beschikbare methoden aangereikt. Veeleer wordt gepoogd om de IT-investeringsanalyse in te passen in de algehele investeringsbesluitvorming binnen een bedrijf. Uitgaande van het investeringsprobleem wordt het algehele besluitvormingsproces beschreven. Als aanvulling op beschikbare methoden worden binnen dit raamwerk de relevante criteria voor de vier typen IT-projecten, met name *ondersteunend, direct noodzakelijk, strategisch* en *hoog potentieel,* bepaald, met de bijbehorende allocatie van middelen. Tot slot worden de kwaliteitseisen voor een goede besluitvorming over informatietechnologie gegeven.

HET INVESTERINGSPROBLEEM

Het investeringsprobleem – gerelateerd aan vrijwel elk project – is dat aan het begin van de periode waarbinnen de desbetreffende investering moet renderen, op het beslismoment, financiële en niet-financiële middelen beschikbaar worden gesteld voor projecten die een onzekere opbrengst genereren tijdens diezelfde periode. Vanuit een objectieve investeringsbenadering, zoals in een optimale kapitaalmarkt, heeft dit probleem twee aspecten: de strategische (markt)planning en de financiering. Wanneer we echter het investeringsprobleem vanuit een organisatorische benadering bezien, spelen er vele interne en externe factoren een rol die het besluitvormingsproces beïnvloeden. Deze subjectieve factoren zijn overigens geenszins negatief, maar benadrukken dat elke organisatie en haar marktpositie uniek zijn en derhalve een andere invulling van de besluitvorming (nodig) hebben. De achterliggende methodiek van besluitvorming zou echter voor elke organisatie gelijk moeten zijn.

De beslisser over een IT-investering zal zich niet als de volstrekt rationeel handelende homo economicus gedragen.

Een organisatorische factor die de effectiviteit van investeringsacties sterk beïnvloedt is de aanwezige competentie van de organisatie op het gebied waarin geïnvesteerd wordt. Investeren in een projectplanning-tool kan erg waardevol zijn in een organisatie waarin projectplanning plaatsvindt en herkend wordt als een belangrijke activiteit. Bij een organisatie waarin geen projectplanning plaatsvindt zou een dergelijke investering niet zo zinvol zijn, tenzij zij louter wordt gebruikt om enthousiasme en begrip voor de baten van planning te kweken (waarvoor veel geëigender projecten te bedenken zijn). Ook het zoekproces naar investeringsmogelijkheden wordt veelal door situationele factoren bepaald. Een innoverende en creatieve organisatie heeft wellicht een fundamenteel ander zoekproces voor projecten dan een conservatieve en rigide organisatie. Terwijl de eerste sterke culturele en organisatorische ondersteuning voor nieuwe en gedurfde projecten geeft, stimuleert de tweede gematigde projecten die in lijn zijn met historische ontwikkelingen. Tevens is een keuze zelden gebaseerd op puur objectieve maatstaven, maar wordt zij sterk beïnvloed door de organisatiecultuur, de besluitvormers en de beïnvloeders (lobbyisten) binnen een organisatie. De beslisser over een IT-investering zal zich niet als de volstrekt rationeel handelende homo economicus gedragen. Daarbij is er vaak niet één beslisser, maar zijn er meerdere partijen. De omgeving van de beslisser, het type beslissing en de karakteristieken van de beslisser(s) beïnvloeden dus ook de uiteindelijke beslissing.

De genoemde organisatorische aspecten ten aanzien van IT-besluitvorming blijven vaak buiten beschouwing door het waarderen van projecten in puur kwantitatieve, veelal financiële termen. Investeringsbeslissingen op basis van criteria als Return on Investment of Net Present Value gaan uit van een statische bedrijfsstrategie en een vaststaand scenario voor toekomstige ontwikkelingen. Aspecten als behoud of blijvend behoud van concurrentiekracht en strategische mogelijkheden door middel van investeringen worden dus niet meegewogen. Door de snelle veranderingen in de markt veranderen strategieën en doelstellingen ook steeds sneller, waardoor IT-beslissingen die uitgaan van een vast toekomstscenario vaak te weinig flexibiliteit bieden. Dit weegt met name zeer zwaar bij infrastructurele beslissingen. Voor een uitwerking van het specifieke probleem van infrastructurele IT-investeringen kan worden verwezen naar onder anderen Van Irsel en Fluitsma ([Irse92]) en Morrenhof en Schipper ([Morr95]). De niet-financiële aspecten aan een IT-investering rechtvaardigen geenszins een puur kwalitatieve benadering. Dit kan met name bij de opstart van een project of bij een complete verandering van informatievoorziening heel gevaarlijk zijn. Op zulke momenten is het in het oog houden van financiële aspecten van levensbelang. Waardering van projecten dient dus een juiste balans tussen kwalitatieve en kwantitatieve aspecten te bevatten.
In het proces van besluitvorming omtrent het al dan niet investeren mag niet worden uitgegaan van de veronderstelling dat alle alternatieven en alle gevolgen daarvan bekend zijn. Men kan gewoonweg niet beschikken over volledige informatie. Investeringsbeslissingen in informatietechnologie kunnen variëren van eenvoudig tot zeer complex. In de meer complexe situaties is er sprake van deelbeslissingen en onderlinge afhankelijkheid tussen de beslissingen. In deze situatie van hoge onzekerheid kunnen analyses geen *doorslaggevende* rol spelen. Doordat het afwegen van subjectieve factoren in de besluitvorming gaat overheersen, spelen de analyses vaak een *rituele* rol. In de meeste situaties echter is de rol van de analyses *ondersteunend*. Afhankelijk van de precieze situatie vormen de analyses een aanzet tot besluitvorming, discussie of onderhandeling.

HET BESLUITVORMINGSPROCES

De stappen die idealiter in een (IT-)besluitvormingsproces worden genomen, zijn in figuur 1 weergegeven. Dit traject wordt echter niet altijd lineair afgelegd, terwijl soms een beslissing reeds is genomen voordat het proces daadwerkelijk wordt ingezet, bijvoorbeeld vanuit politieke overwegingen. De cirkels in de figuur geven de uit te voeren stappen in het proces aan, de rechthoeken het resultaat van die stappen.

In het algehele proces van besluitvorming over informatietechnologie is het genereren van potentiële projecten de eerste stap. Projecten kunnen naar voren worden gebracht door IT-medewerkers,

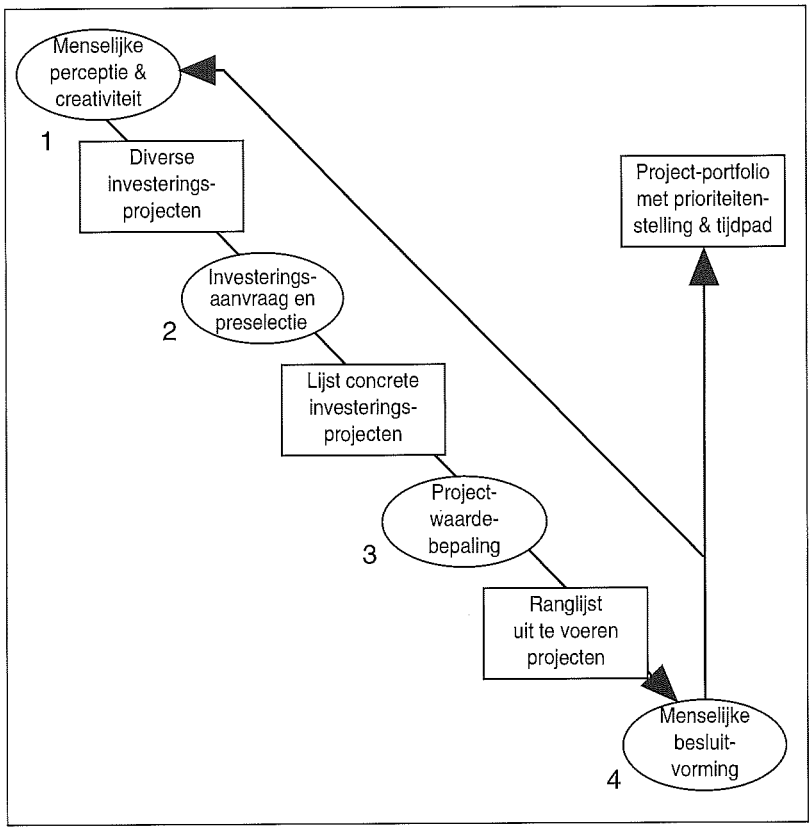
maar bij voorkeur komen deze vanuit alle geledingen binnen het bedrijf. In deze fase dient er (nog) geen waarde-oordeel te worden uitgesproken over de daadwerkelijke waarde van bepaalde ideeën of projecten. Dit genereren van potentiële projecten zou tot de strategische kerncompetenties van elke organisatie moeten behoren. Innovatie is immers een kritieke factor voor het behoud van continuïteit, de sine qua non voor elke organisatie. Het genereren van mogelijke projecten is een aspect van de creativiteit van een organisatie. De denkwijze over nieuwe projecten kan echter sterk verschillen per organisatie. Terwijl het ene bedrijf een grote mate van structurele en culturele ondersteuning geeft voor innovatie, verstikt een ander juist innovatieve gedachten en beloont het conservatisme.

Stap 1 eindigt met een lijst van alle potentiële projecten. Een volgende stap omvat het uitvoeren van een preselectie uit de lijst van potentiële projecten. Bepaalde ideeën kunnen vervallen voor verdere evaluatie, omdat ze te ver van de realiteit staan of omdat ze bijvoorbeeld politiek nooit haalbaar zullen zijn. Hierbij is echter voorzichtigheid geboden. Het is al te vaak voorgekomen dat echte 'winners' nooit in het daadwerkelijke besluitvormingstraject zijn terecht gekomen, omdat ze op het eerste oog onrealistisch of zelfs belachelijk leken. Anderzijds is preselectie wenselijk om onnodige inspanning in de evaluatie van grote aantallen doodgeboren projecten te voorkomen. Ook bij preselectie is de cultuur van een organisatie weer bepalend. De aanvraag van middelen voor elk project zou een globaal projectplan en ten minste de noodzakelijke input voor het evaluatietraject moeten bevatten, te zamen met randinformatie voor de besluitvormers. Geen project zou ooit goedgekeurd of verworpen moeten worden zonder mondelinge toelichting. Voor elk voorstel dat door de preselectie heen komt dient een soort investeringsaanvraag te worden opgesteld. De omvang en vorm van deze investeringsaanvraag moeten afgestemd zijn op de typen projecten (zoals verderop wordt toegelicht) en met name hun financieringsbehoefte. In principe kan worden gesteld: hoe groter het project, hoe gedetailleerder de investeringsaanvraag op de kritieke aspecten van dat project. Stap 2 levert dus een lijst met concrete investeringsprojecten, waarvoor een investeringsaanvraag is opgesteld.

Deze lijst dient als input voor de daadwerkelijke projectwaardering. Dit is ook de stap waar beslissingsondersteunende methoden en modellen hun waarde kunnen leveren. Voor een meer diepgaande bespreking van deze methoden wordt verwezen naar [Swin92].

Vanuit de eigenlijke projectwaardebepaling resulteert een rangschikking van de voor evaluatie aangeboden projecten per type project. Deze typering vindt plaats op basis van de noodzakelijkheid om een project uit te voeren en het concurrentievoordeel (of -behoud) dat erdoor gerealiseerd kan worden. De rangschikking bevat een weging van de aspecten kosten, baten, risico's en tijd.

De laatste stap (4) in het gehele traject is het eigenlijke beslissen op basis van de in stap 3 gegenereerde informatie. De besluitvorming dient idealiter



Figuur 1. Het IT-besluitvormingsproces.

plaats te vinden op het laagste niveau noodzakelijk om objectief de aspecten van coherentie tussen projecten en de allocatie van de middelen naar de verschillende typen te kunnen overwegen. In de meeste organisaties zal het hiërarchisch niveau van besluitvorming worden bepaald door de organisatiestructuur. Zelfs in deze eindfase zou additionele informatie van specialisten de keuze nog moeten kunnen beïnvloeden.

Het voorliggende raamwerk is een hulpmiddel voor besluitvorming over (IT)-investeringen. Waardevolle informatie kan worden verkregen bij het toepassen van modellen en tools en de gegenereerde rangschikking is zeer behulpzaam wanneer de onderliggende procedures van het model duidelijk zijn. Per definitie zijn de middelen van een organisatie echter beperkt, hetgeen betekent dat elke investeringsbeslissing – en de bijbehorende allocatie van middelen – een verdere beperking van de flexibiliteit van die organisatie betekent. Vanwege het soort en de (relatieve) omvang van IT-investeringsbeslissingen zou geen enkel model gezien of gebruikt moeten worden als substituut voor menselijke besluitvorming en gezond verstand. Daarbij komt dat geen model ooit de werkelijkheid kan vervangen. Derhalve is de laatste stap bij het toepassen van elk model de voorzichtige evaluatie van de resultaten en de uiteindelijke weging van alle harde en zachte criteria om tot een goed afgewogen beslissing te komen.

BASEER DE BESLISSING OP CRITERIA DIE ECHT TELLEN

Beslissingen nemen betekent altijd omgaan met een bepaalde mate van onzekerheid. Vaak kenmerken investeringsanalyses zich dan ook door een grote inspanning in het proberen terug te dringen van die onzekerheid. Vaak wordt hierbij echter onnodig veel tijd besteed aan het proberen te prognotiseren van factoren die ofwel niet te prognotiseren zijn, ofwel niet relevant voor de beslissing. Naar onze mening zijn de criteria met name afhankelijk van het type project waarover beslist wordt (maar ook deels van de beslisser). Op basis van onderzoeken van McFarlan ([Farl81]) en Edwards et al. ([Edwa91]) is voor die projecttypering het VIZIER ontwikkeld (zie figuur 2). Hierbij worden projecten voorafgaand aan de analyse van de criteria gecategoriseerd naar hun strategische betekenis. Het VIZIER is op basis van concurrentievoordeel en de noodzakelijkheid van een project verdeeld in vier sectoren: strategisch, hoog potentieel, noodzakelijk en ondersteunend.

Inzicht in het type project of investeringsbeslissing is essentieel voor een adequate vergelijking van projecten. Niet alleen kan worden aangegeven waarop de keuze gebaseerd moet zijn, maar tevens kan de analyse-inspanning gericht worden op die criteria die tellen. Deze criteria zijn bijvoorbeeld het rendement op geïnvesteerd vermogen, de mate van toekomstig concurrentievoordeel en de mate van onzekerheid in het gebruik van de benodigde technische hulpmiddelen. Binnen het totaal aan mogelijke criteria (voor een overzicht van deze criteria wordt verwezen naar [Park88] en [Coor92]) is er een aantal waar afhankelijk van het type project de nadruk meer op moet liggen. De insteek hiervoor is weergegeven in figuur 4. Het zodanig focusseren voorkomt dat men door de bomen het bos niet meer ziet, terwijl tevens de meeste inspanning kan worden gestoken in het prognotiseren van deze sleutelcriteria. Een goede beslissing is in veel gevallen immers ook een snelle beslissing.
Zoals gezegd worden de investeringen/projecten op basis van twee dimensies ingeschaald:

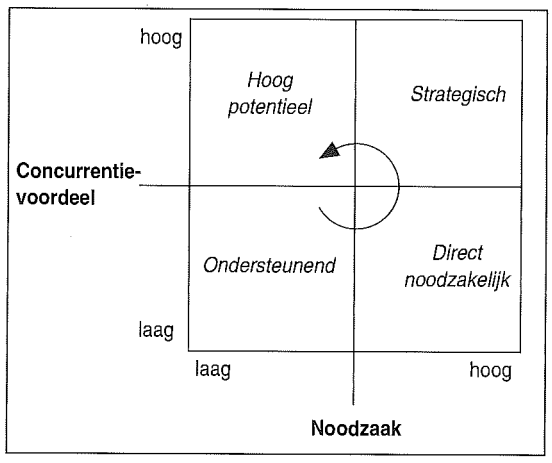
1. de mate van concurrentievoordeel die zij (potentieel) levert;
2. de mate van noodzakelijkheid. Sommige investeringen zijn noodzakelijk omdat anders het dagelijkse functioneren van de organisatie in gevaar komt (direct noodzakelijk) of het betreft een hoog wenselijke investering in een richting die niet noodzakelijk is voor het functioneren van de organisatie op korte termijn (hoog potentieel). Correctief onderhoud van een bedrijfskritiek systeem is een voorbeeld van een 'direct noodzakelijk'-investering.

De draaiende pijl in het midden van het model geeft de toename in complexiteit van de investeringsbeslissingen weer. Het typeren van een project kan een lastige taak zijn. De basisvragen die bij een typering beantwoord moeten worden, zijn:

1. Levert het project me *alleen* efficiencyvoordeel op: ja = ondersteunend.
2. Heb ik het absoluut nodig om nu te 'overleven': ja = direct noodzakelijk.
3. Levert het project me nu concurrentievoordeel op: ja = strategisch.
4. Kan het project me in de toekomst concurrentievoordeel opleveren: ja = hoog potentieel.

Doordat voor elk project of bestaand systeem maximaal één van deze vragen met 'ja' te beantwoorden is, kunnen ze helpen bij de categorisering. Overigens treedt er een extra complicerende factor op wanneer een project eigenlijk meerdere projecten omvat van een ander type. De deelprojecten kunnen dan wel afzonderlijk worden ingedeeld in de vier typen, maar bij de uiteindelijke besluitvorming moet de onderlinge samenhang van de deelprojecten niet uit het oog worden verloren.

Figuur 2. Het VIZIER.

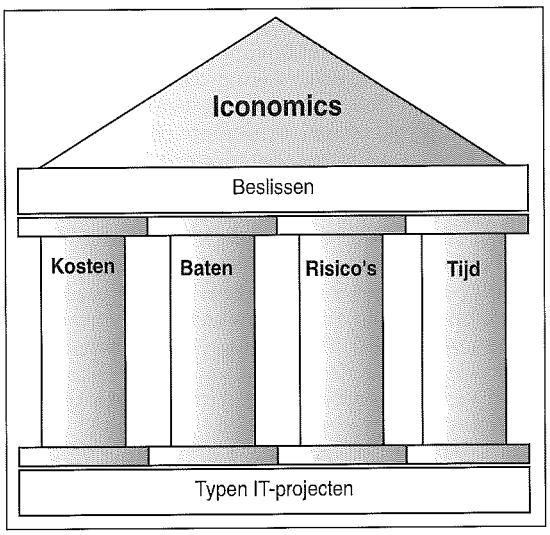


ICONOMICS

Zoals gesteld, is er een groot aantal criteria die bij de waardebepaling van IT-projecten kunnen worden meegewogen. Deze criteria zijn alle gerelateerd aan één of meer van de vier elementen van deze waardebepaling: kosten, baten, risico's en tijd. De auteurs hebben op basis hiervan de Iconomics-aanpak ontwikkeld. Hierin wordt gebaseerd op het fundament van de vier IT-typen (ondersteunend, direct noodzakelijk, strategisch en hoog potentieel) en gedragen door de vier elementen van waardebepaling (kosten, baten, risico's en tijd) besluitvorming over IT-projecten gefaciliteerd. Hierbij dekt Iconomics het totale besluitvormingstraject af, waarbij het voorziet in eigen beslissingsmodellen voor de projectwaardebepaling ([Coor92]), maar waarbij ook andere modellen kunnen worden toegepast.

Het fundament: De typen IT-projecten

Vanuit de noodzakelijkheid en het te behalen concurrentievoordeel worden projecten onderverdeeld. Dit voorkomt het vergelijken van appels met



Figuur 3. De Iconomics-aanpak met de vier pijlers voor IT-besluitvorming.

peren en richt de aandacht op die criteria die echt meetellen. Een bijkomend voordeel van gerichte allocatie van middelen wordt later besproken.

Pijler 1: Kosten

Met name op dit aspect worden tot op heden de investeringen beoordeeld. Deze lijken ook het meest eenvoudig te bepalen, waarbij verborgen en indirecte kosten vaak vergeten worden. Kosten omvatten overigens niet alleen financiële middelen, maar kunnen ook kwalitatieve aspecten omvatten, zoals imagoverlies bij een project dat nadelige milieu-effecten heeft. Bij de discussie omtrent het investeringsprobleem is de rol van het kostenaspect in de besluitvorming reeds genoemd.

Pijler 2: Baten

Voor baten gelden in principe dezelfde overwegingen als voor kosten. Bijkomend probleem is dat baten vaak pas in een later stadium behaald (kunnen) worden, terwijl kosten direct gemaakt moeten worden. Ten aanzien van de aloude kosten/baten-analyses kan worden opgemerkt dat deze de kwalitatieve baten (en deels de kwalitatieve kosten) buiten beschouwing laten en zodoende een onvolledig beeld geven.

Pijler 3: Risico's

Een derde element dat bij de waardebepaling wordt betrokken, zijn de risico's die aan een bepaalde optie kleven. Een project kan een zeer voordelige kosten/baten-verhouding hebben, maar wanneer de risico's die aan het project kleven zo groot zijn dat de baten waarschijnlijk nooit gehaald worden, zal het project waarschijnlijk niet geselecteerd worden (afhankelijk van type en daarmee de risico-geaardheid van de beslisser).

Pijler 4: Tijd

Tijd wordt meer en meer een essentieel onderdeel van de besluitvorming over informatietechnologie. Een project of systeem dat vandaag strategisch voordeel biedt kan morgen tot de direct noodzakelijke systemen behoren. Ook kan een project dat geweldige voordelen biedt maar één jaar ontwikkeling vergt, vaak minder aantrekkelijk zijn dan een minder voordelig project dat in drie maanden kan worden afgerond.

Wanneer men de pijlers vanuit een bepaalde abstractie bekijkt zou men kunnen stellen dat risico's en tijd toegerekend kunnen worden naar kosten en baten. Bij een voldoende hoog abstractieniveau zijn zo alle criteria en aspecten aan een project terug te brengen tot positieve (baten) en negatieve (kosten) argumenten voor dat project. Deze vereenvoudiging gaat echter voorbij aan het feit dat een bepaald projectrisico afhankelijk van de situatie zowel voordelige als nadelige gevolgen kan hebben voor de waarde van een project. Een zelfde argumentatie kan voor tijd worden gegeven: een systeem kan vandaag van onschatbare waarde zijn en concurrentievoordeel geven, terwijl het over enkele jaren oud nieuws is en geen enkel voordeel meer genereert.

De top: Beslissen

Boven op het fundament en de pijlers komt het beslissen zelf. Hierbij worden op basis van de typering de aspecten van kosten, baten, risico en tijd van een project in samenhang gezien en worden deze gerelateerd aan de kwalificaties van andere projecten.

Overkoepelend: Iconomics

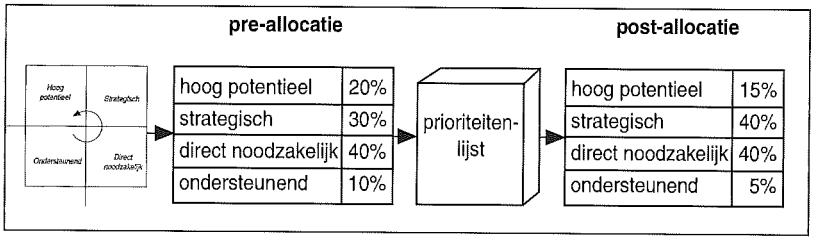
Uitgaande van vier pijlers van IT-besluitvorming en dit combinerend met de typen projecten (het VIZIER) kunnen we de gewenste focussering bepalen in de criteria die de doorslag moeten geven bij de besluitvorming.

'Ondersteunend'	'Direct noodzakelijk'	'Hoog potentieel'	'Strategisch'
Focus op financieel rendement (ROI) en laag risico	Focus op lage kosten, laag risico en snelle uitvoering	Focus op kwalitatieve baten en markt-risico	Focus op kwalitatieve baten en timing (voorop blijven)

Figuur 4. De doorslaggevende criteria voor de verschillende projecttypen.

ENKELE ORGANISATORISCHE ASPECTEN

Zoals naar voren gekomen bij de bespreking van het besluitvormingsproces speelt een groot aantal organisatorisch bepaalde aspecten een rol bij die



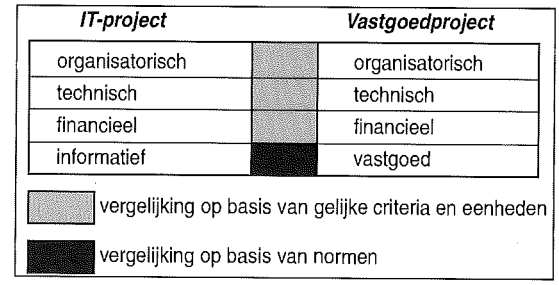
Figuur 5. Allocatie van middelen naar de verschillende projecttypen.

besluitvorming. Door de verdeling van de IT-projecten in vier klassen lijkt er een specifiek organisatorisch aspect bij te komen, namelijk de toekenning van schaarse middelen aan de verschillende projecttypen. Dit aspect wordt echter niet toegevoegd door het classificeren, maar expliciet gemaakt. Elke organisatie neemt immers impliciet beslissingen over de vraag of middelen worden toegekend aan optimalisatie van bestaande systemen of aan de ontwikkeling van nieuwe zaken.

Door de classificatie van projecten komt de vraag naar voren welk deel van het beschikbare budget in geld, mensen en andere middelen er moet worden toegekend aan strategische, hoog potentiële, direct noodzakelijke of ondersteunende projecten. Deze toekenning (zie figuur 5) kan vooraf (*pre-allocatie*) of achteraf (*post-allocatie*) plaatsvinden.

Deze keuze gaat dieper dan het in eerste instantie lijkt. Het volledig weglaten van pre-allocatie zou in het slechtste geval bijvoorbeeld kunnen resulteren in een projectportefeuille die alleen gevuld is met ondersteunende projecten, hetgeen de organisatie op korte termijn kostenreductie en efficiency-verbetering kan opleveren. Op de middellange termijn zouden de kaarten echter slecht gestoken zijn voor deze organisatie, omdat de concurrentiepositie ondermijnd zou kunnen worden door het gebrek aan direct noodzakelijke projecten. Op langere termijn zou deze positie nog verder teruglopen door gebrek aan strategische en hoog potentiële projecten. Deze situatie is overigens lang niet denkbeeldig, daar gebleken is dat het merendeel van de mensen die gevraagd worden om nieuwe projecten te bedenken vaak ondersteunende projecten oplevert. Efficiency-verbeteringen zijn vaak sneller te ontdekken dan effectiviteitsverbeteringen die een breder inzicht van de betrokkene vragen.
Hoewel de gevaren die verbonden zijn aan volledige pre-allocatie geringer zijn dan die van het geheel achterwege laten, kan volledige pre-allocatie wel resulteren in het uitvoeren van zeer slechte projecten uit het ene kwadrant, terwijl zeer goede projecten uit een ander kwadrant worden losgelaten onder invloed van te beperkte middelen.

Een zelfde problematiek maar van een hogere orde betreft het alloceren van middelen naar IT-projecten en andere investeringsprojecten. De meeste organisaties stellen investeringsbudgetten op om deze problematiek te omzeilen. Dit dekt echter niet de specifieke situatie die zich voordoet wanneer een bepaald probleem of een bepaalde opportuniteit kan worden ingevuld door een IT-project of een ander soort project. Stel bijvoorbeeld dat een supermarkt een snellere afhandeling bij de checkout wil bereiken. Dit kan worden bewerkstelligd door meerdere kassiers aan te nemen en wellicht het aantal kassa's uit te breiden, door de routing in de winkel te verleggen of door een volledig geïntegreerd point-of-sale-systeem aan te schaffen. Om deze verschillende opties onderling te kunnen vergelijken is het noodzakelijk om vergelijkbare criteria te creëren. Een mogelijkheid hiertoe biedt een aanvulling op de drie domeinen van Parker en Benson ([Park88]): financieel, organisatorisch en technisch. Dit vierde domein, dat specifiek is voor het investeringsgebied (bijvoorbeeld informatietechnologie, onroerend goed, personeel, etc.), vormt dan het domein dat de onderlinge vergelijking tussen die geheel verschillende projecten mogelijk moet maken. Voor dit vierde domein moeten dan normen worden gesteld: bijvoorbeeld voor een IT-project de mate waarin het voorziet in de informatiebehoefte, en voor een vastgoedproject de mate waarin het de werkomgeving van de medewerkers verbetert.



Figuur 6. Vergelijking van projecten uit verschillende vakgebieden door middel van domeinen.

Bijkomend voordeel is dat de beslissingen over de verschillende delen van het investeringsprobleem (technisch, organisatorisch, etc.) door de specialist op dat gebied kunnen worden genomen, waarna het algemeen management de overall-beslissing neemt. Voor verdere toelichting op deze materie wordt verwezen naar [Coor92].

CONCLUSIES

Op basis van het investeringsprobleem en de genoemde aspecten die een rol spelen in de besluitvorming is er een aantal kwaliteitseisen aan het besluitvormingsproces te stellen:
- in de besluitvorming dienen zowel kwantitatieve als kwalitatieve criteria te worden gewogen;
- de subjectieve aspecten in de besluitvorming gerelateerd aan de organisatie en de besluitvormers dienen in het proces erkend te worden;
- de keuze dient gericht te zijn op de criteria die daadwerkelijk van belang zijn voor dat project (zie figuur 4);

- pre- en post-allocatie van middelen dient plaats te vinden op basis van de strategie van de onderneming (defensief, innovatief, etc.);
- de verschillende investeringsprojecten dienen te worden vergeleken op vergelijkbare aspecten (bijvoorbeeld technisch domein) op basis van cijfers, en op verschillende aspecten (bijvoorbeeld informatietechnologie en procedureel) op basis van standaardnormen;
- een investeringsbeslissing in informatietechnologie moet een totaalaanpak omvatten. Alle factoren moeten afzonderlijk, maar ook in samenhang met elkaar onderzocht en beoordeeld worden.

Besluitvorming over investeringen in IT-projecten handelt niet over technologie, maar over de organisatie. De moeilijkheid ligt niet meer zozeer bij de technologie, maar bij de besluitvorming over hoe die technologie en de bijbehorende concepten een zo maximaal mogelijke waarde voor de organisatie kunnen genereren.

Bevreesd voor deze moeilijke beslissingen en afgeschrikt door de steeds complexere techniek heeft het algemeen management de besluitvorming over informatietechnologie te lang overgelaten aan de automatiseringsstaf. Soms resulteerde dit vluchtgedrag in het delegeren van de besliskracht naar technisch personeel, meestal komt het tot uiting in de focus op technische moeilijkheden in het besluitvormingstraject. Mede dankzij dit tekort aan algemene managementsturing zijn betrokkenheid bij en beheersbaarheid van IT-projecten laag gebleven.
In dit artikel is een aantal methoden weergegeven om het oppakken van die beslissingen door de betrokkenen te faciliteren. Zo kan de besluitvorming over de (strategische) inzet van informatietechnologie plaatsvinden op het niveau waar zij hoort: dat van het algemeen management.

LITERATUUR

[Coor92] E.M.H. Coorens, *Assessing the value of information and information handling as a competitive strength*, PUC Press, 1992.

[Edwa91] C. Edwards, J. Ward en A. Bytheway, *The essence of information systems*, Prentice-Hall International, 1991.

[Farl81] F.W. McFarlan, *Portfolio approach to information systems*, Harvard Business Review, no. 5, 1981.

[Gian91] M. Gianotten, *Topmanagers, succesvol ondernemen en informatietechnologie*, Giarte Management & Informatie, 1991.

[Hend93] J.C. Henderson en N. Venkatraman, *Strategic Alignment: Leveraging information technology for transforming organizations*, IBM Systems Journal, Vol. 32, no. 1, 1993.

[Irse92] H.G.P. van Irsel en P. Fluitsma, *Het plannen en rechtvaardigen van infrastructurele IT-investeringen*, Compact 1992/2.

[Mant90] E.A. Mantz, J.T.H.C. van Lieshout en F.A.P. van der Zijden, *Omgaan met informatiebeleid en informatieplanning: bevindingen van een vijfde praktijkonderzoek*, Informatie, jaargang 32, no. 1, 1990.

[Meye89] N.D. Meyer en M.E. Boone, *The information edge*, Gage Educational Publishing, 1989.

[Morr95] M.J. Morrenhof en R. Schipper, *Identificatie en legitimatie van investeringen in de informatie-infrastructuur*, Management & Informatie, juni 1995.

[Nais90] J. Naisbitt en P. Aburdene, *Megatrends 2000: Ten new directions for the 1990's*, Morrow, 1990.

[Oirs93] R.R. van Oirsouw, J. Spaanderman en H. de Vries, *Informatie-economie, investeringsstrategie voor de informatievoorziening*, Academic Service, 1993.

[Oost92] A. Oosterhaven, *Het beoordelen van investeringen in informatietechnologie*, Informatie, themanummer, jaargang 34, 1992.

[Park88] M.M. Parker, R.J. Benson en H.E. Trainor, *Information Economics, Linking Business Performance to Information Technology*, Prentice-Hall International, 1988.

[Rock79] J.F. Rockart, *Chief executives define their own data needs*, Harvard Business Review, no. 2, 1979.

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

Ing. E.M.H. Coorens BE MBA
Is werkzaam bij Macintosh Retail Group. Zijn werkzaamheden zijn overwegend gericht op de bedrijfskundige toepassing van IT in de retail, waarbij onder andere informatieplanning, IT-besluitvorming (information economics) en IT-synergie belangrijke aandachtspunten zijn.

Drs. P.J.C. van Bladel en dr. M. Boogaard
Zijn werkzaam bij KPMG Management Consulting en als zodanig sterk betrokken bij de vakontwikkeling op het gebied van information economics.

Benchmarking, een hulpmiddel voor de EDP-auditor?

Ir. J.A.M. Donkers RE en
mw. ir. E.R. van Sommeren

De toenemende belangstelling voor benchmarking komt voort uit een behoefte bij het management aan spiegelinformatie. De auteurs behandelen de voor- en nadelen van het toepassen van benchmarking bij EDP-audits. Als voorbeeld worden de verschillende stappen voor benchmarking van de general IT controls ingevuld.

INLEIDING

Benchmarking staat in Nederland steeds meer in de belangstelling. Door onder meer de kritische opstelling van de afnemers van bedrijven en instellingen en de toegenomen concurrentie tussen organisaties onderling wordt continu druk uitgeoefend om zich te verbeteren. Hierbij is het essentieel dat men vast kan stellen hoe men ervoor staat ten opzichte van andere organisaties. Door zich te 'meten' en deze metingen te vergelijken, is het mogelijk de sterkte(n) en/of zwakte(n) ten opzichte van andere organisaties te bepalen. Dit proces wordt aangeduid met de term benchmarking.

De werkzaamheden van de EDP-auditor bestaan voor een belangrijk deel uit het beoordelen van automatiseringssituaties. Veel bedrijven en instellingen zijn afhankelijk van automatisering en de werking daarvan. Een goede beheersing en controle van de automatisering en het gebruik hiervan kunnen bij grote afhankelijkheid als een kritieke factor worden beschouwd door het management. Organisaties zijn steeds meer op zoek naar spiegelinformatie. Wie wordt niet bij werkzaamheden geconfronteerd met vragen als: Hoe doen andere bedrijven en/of instellingen... ? Op basis van kennis en ervaring kan natuurlijk antwoord worden gegeven op dergelijke vragen. Het is dan echter niet mogelijk de vergelijking te ondersteunen met benchmark-gegevens (bijvoorbeeld cijfermateriaal). Een EDP-auditor kan deze gegevens leveren.

In dit artikel wordt ingegaan op benchmarking in het algemeen en vervolgens op benchmarking van een belangrijk onderdeel van de audits: de general IT controls. De voor- en nadelen van het toepassen van benchmarking bij EDP-audits worden vervolgens besproken. Aan de hand van het benchmarking-proces van Camp ([Camp89]) worden de verschillende stappen voor benchmarking van de general IT controls ingevuld.

BENCHMARKING

Benchmarking kan kortweg worden gedefinieerd als het vergelijken van organisaties of organisatie-onderdelen ([Pryo89]). Het is een continu, systematisch proces waarbij de resultaten van de vergelijking worden geëvalueerd en dat veelal wordt gebruikt als instrument om de performance van een organisatie te verhogen. Benchmarking kan in verschillende typen worden ingedeeld ([Pryo89]):

- *strategic benchmarking*, de vergelijking van verschillende marktstrategieën en de verbanden tussen deze strategieën en hun succes in de markt;
- *operational benchmarking*, de vergelijking van een specifiek onderdeel van de bestaande functionele onderdelen van een organisatie met die van andere organisaties. De analyse concentreert zich in het algemeen op een beperkt aantal variabelen, waaronder kosten;
- *business management benchmarking*, de vergelijking van ondersteunde functies van organisaties. De analyse richt zich op het bepalen van de huidige waarde van de desbetreffende functie voor de onderneming in vergelijking met andere organisaties.

Een tweede indeling van typen benchmarking kan worden gemaakt op basis van de groep organisaties waarmee men zich wil (laten) vergelijken. Er is een aantal mogelijkheden:

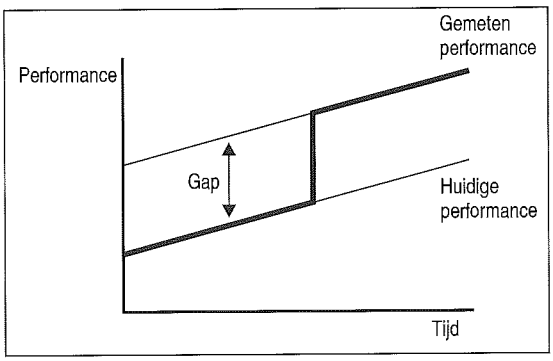
- intern, vergelijking vindt binnen de organisatie plaats, bijvoorbeeld tussen business units;
- branche, vergelijking vindt plaats met organisaties uit dezelfde branche;
- algemeen, vergelijking vindt plaats met 'alle' organisaties.

Binnen de genoemde typeringen kan de vergelijkingspopulatie aanvullend worden afgebakend door het beperken aan de hand van variabelen zoals de omzet en/of het aantal medewerkers.
De keuze voor het type vergelijking is afhankelijk van de eisen en wensen van het bedrijf en/of de instelling dat (die) het benchmarking-proces doorloopt. Grotere organisaties zijn vaak benieuwd naar het functioneren van de verschillende organisatie-onderdelen (interne benchmarking). Door echter alleen intern vergelijkingen uit te voeren, ontbreekt een externe spiegel: er vindt geen vergelijking plaats met bijvoorbeeld branchegenoten.

Naast een vergelijking met soortgelijke bedrijven of instellingen kan het ook wenselijk zijn om een vergelijking te maken met de 'best presterende' organisatie. Op deze manier ontstaat er inzicht in de gebieden waar men zich zou kunnen verbeteren om het 'best' te presteren van allemaal. Vergelijking kan in dit geval met zowel organisaties binnen als buiten de branche plaatsvinden.

Waarin verschilt benchmarking van andere managementtechnieken?

De kern van benchmarking wordt gevormd door het in kaart brengen van de huidige performance en van de gemeten performance (zie figuur 1). Op het eerste gezicht is dit concept weinig vernieuwend ten opzichte van andere managementtechnieken. Het belangrijkste onderscheidende kenmerk van benchmarking wordt gevormd door de gegevens waarmee de huidige performance wordt vergeleken. Naast een vergelijking tussen de *ist-* en *soll-positie* wordt de ist-positie vergeleken met die van andere (soortgelijke) organisaties.



Figuur 1. Benchmarking-gap.

Interpretatie van een benchmarking-gap

Het is belangrijk dat de interpretatie van de benchmarking-resultaten voor alle bij het benchmarking-proces betrokken partijen duidelijk is. Zo zijn de volgende twee formuleringen mogelijk:

1. na constatering van de gap worden actieplannen ontwikkeld om de bij andere organisaties gemeten (gewenste) performance te bereiken;
2. na constatering van de gap wordt de herkomst van het verschil ten opzichte van andere organisaties geëvalueerd. Op basis van de evaluatie worden verdere actieplannen ontwikkeld.

Het gevaar van de eerste formulering, die in de praktijk nogal eens wordt aangetroffen, is dat te snel conclusies worden getrokken. Hierdoor zou een onjuiste actie kunnen worden geïnitieerd. Een voorbeeld hiervan kan zijn dat een organisatie met andere wordt vergeleken op het aspect automatiseringskosten. Uit de vergelijking blijkt dat de organisatie meer aan automatisering besteedt dan gemiddeld in de referentiegroep. Uit nadere analyse blijkt dat de desbetreffende organisatie een hogere graad van automatisering heeft dan de organisaties waarmee is vergeleken. Daarnaast zouden incidentele kostenverhogende factoren zoals de verbetering van de IT-infrastructuur eveneens een oorzaak van de hoge automatiseringskosten kunnen zijn. Dit eenvoudige voorbeeld geeft aan dat de resultaten van de vergelijking nader geanalyseerd zullen moeten worden. De auteurs zijn dan ook van mening dat actieplannen die voortkomen uit benchmarking altijd gebaseerd moeten zijn op een nadere analyse van de geconstateerde verschillen.

HET BENCHMARKING-PROCES

Om benchmarking succesvol te kunnen toepassen is het van belang dat het proces en de bijbehorende

produkten voldoen aan bepaalde eisen. Van der Zee ([Zee94]) geeft de volgende spelregels voor een IT-meet- en regelsysteem weer:
- een uniform begrippenkader;
- een juiste afgesproken timing;
- een bepaalde frequentie van meting;
- een onafhankelijk rapporteur;
- inbedding in de reguliere managementrapportage.

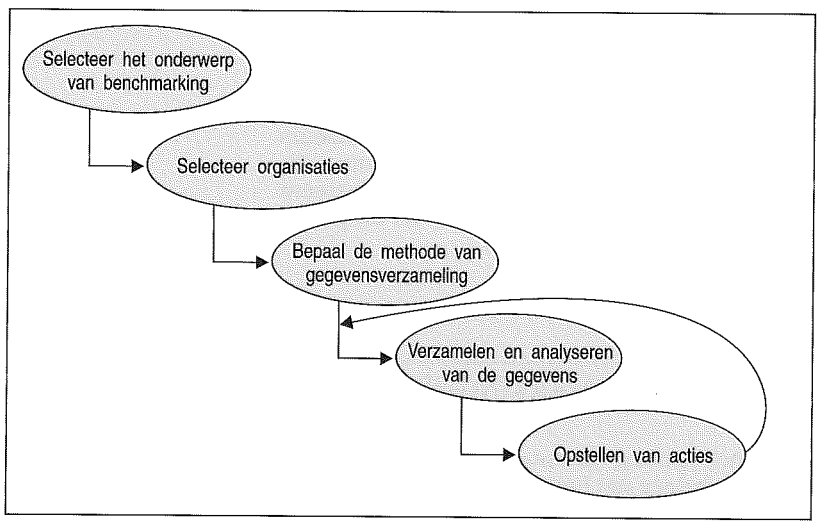
Naast genoemde spelregels is het voor de organisatie die het benchmarking-proces ondergaat van belang dat men sterk betrokken is bij het proces en bereid is te leren en te veranderen. Benchmarking is een onderdeel van een bewustwordingsproces. Degene(n) die het benchmarking-proces uitvoert, moet beschikken over kennis van en ervaring met benchmarking en het object van benchmarking, bijvoorbeeld informatietechnologie. Dit is noodzakelijk om tot een goede afbakening van de te benchmarken objecten te komen.

Een ander belangrijk aspect is dat een voldoende grote hoeveelheid vergelijkingsgegevens verzameld wordt om zinvolle vergelijkingen te kunnen maken. Het verzamelen van deze gegevens kan in de praktijk nogal wat problemen opleveren. Als een bedrijf of instelling gegevens wil verzamelen van soortgelijke organisaties betreft het in veel gevallen concurrenten. Het verkrijgen van de benodigde informatie kan in dergelijke gevallen problematisch zijn. In Nederland is reeds een aantal organisaties ingesprongen op dit probleem door als 'onafhankelijke' organisatie (een deel van) het benchmarking-proces voor een bedrijf of instelling uit te voeren.

Het proces

De eerste fase van een benchmarking-proces bestaat uit het definiëren van de toegevoegde waarde van benchmarking en het selecteren van de methode van benchmarking: Strategic, Operation of Business management. Vanaf deze keuze kan het benchmarking-proces vereenvoudigd worden weergegeven door middel van vijf stappen ([Camp89]):

Figuur 2.
Benchmarking-proces.



1. Wat? Selecteer het onderwerp van benchmarking.
2. Wie? Selecteer bedrijven en/of instellingen waarmee men zichzelf wil vergelijken.
3. Waar? Bepaal de methode van gegevensverzameling.
4. Hoe? Verzamel en analyseer de gegevens.
5. Actie. Opstellen van acties en eventueel implementeren van verbeteringen.

Selecteer het benchmarking-onderwerp
Er zijn voor bedrijven en instellingen vele onderwerpen interessant om te benchmarken. Deze kunnen bijvoorbeeld betrekking hebben op de financiële functie, de produktie- en/of logistieke functie en de automatiseringsfunctie van een organisatie. De praktijk heeft geleerd dat een goede afbakening van het benchmarking-onderwerp noodzakelijk is. Dit mede om te voorkomen dat het onderzoek een te omvangrijk en tijdrovend proces wordt.

Selecteer bedrijven en/of instellingen waarmee men zichzelf wil vergelijken
Het selecteren van bedrijven of instellingen kan worden gestart met het beantwoorden van de vraag: met wie wil de organisatie worden vergeleken? Er is al aangegeven dat kan worden gekozen voor een interne of een externe vergelijking. De te selecteren organisaties kunnen bijvoorbeeld ook aan een aantal eisen moeten voldoen: ze moeten alle actief zijn in dezelfde branche, een ongeveer overeenkomende omzet en een vergelijkbaar aantal medewerkers hebben.

Bepaal de methode van gegevensverzameling
Het verzamelen van gegevens kan op verschillende manieren plaatsvinden. Hierbij kan worden gedacht aan het versturen van vragenlijsten, het afnemen van interviews en/of het organiseren van workshops waaraan alle belanghebbenden deelnemen.

Ongeacht de methode van gegevensverzameling is het altijd van belang dat de verzamelde gegevens worden gecontroleerd op kwaliteit. Deze bewaking van de kwaliteit vormt naar de mening van de auteurs wellicht één van de belangrijkste onderdelen van het benchmarking-proces. Indien de verzamelde gegevens niet van voldoende kwaliteit zijn, is het gevolg dat kwaliteit van de database onvoldoende is en daarmee ook de benchmark die wordt uitgevoerd. Om te waarborgen dat kwalitatief goede informatie wordt verzameld, is het van belang om in het verzamel- en verwerkingsproces kwaliteitsborgingen in te bouwen. Voorbeelden hiervan kunnen zijn:
- het inbouwen van controlevragen in de vragenlijst. Met behulp van controlevragen kunnen onjuistheden en/of inconsistenties worden gedetecteerd;
- het beoordelen van de verzamelde informatie op basis van kennis en ervaring van het onderwerp en de organisatie.

Verzamelen en analyseren van de gegevens
De bepaling van de methode van gegevensverzameling wordt gevolgd door de daadwerkelijke verzameling van de gegevens. Na voltooiing van dit proces zullen de gegevens moeten worden verwerkt. De resultaten van deze verwerking kunnen vervolgens worden geanalyseerd (zie subparagraaf Interpretatie van een benchmarking-gap).

Opstellen van acties (implementeren van verbeteringen)
Op basis van de verzamelde gegevens, de vergelijking van die gegevens met die van het bedrijf of instelling en de analyse van de resultaten van de vergelijking kunnen actiepunten worden opgesteld. Wegen tot verbetering moeten naar de mening van de auteurs niet worden gezocht in het kopiëren (klonen) van 'beter' presterende organisaties. Het is vrijwel uitgesloten dat twee organisaties identiek aan elkaar zijn. Het is dan ook vaak zinvoller om de performance van andere organisaties als uitgangspunt voor evaluatie te nemen en om de tijd die het zou kosten om een andere organisatie te kopiëren, te gebruiken om de 'eigen' organisatie door te lichten.

Deze stappen geven slechts een kader aan voor het uitvoeren van het benchmarking-proces. Dit kader is abstract gedefinieerd waardoor het mogelijk en noodzakelijk is om nog een aantal keuzen te maken. Om de general IT controls te kunnen benchmarken zullen deze stappen nogmaals worden doorlopen. In het vervolg van het artikel zal een beschrijving hiervan worden gegeven.

Is vergelijking met een normenstelsel ook benchmarking?

Het is mogelijk organisaties te vergelijken met normenstelsels zoals de Code voor Informatiebeveiliging. De Code voor Informatiebeveiliging is een naslagdocument voor bedrijven en instellingen voor het opzetten, implementeren en onderhouden van informatiebeveiliging. Niet alle maatregelen zijn van toepassing op elke automatiseringsomgeving maar een klein aantal maatregelen is *essentieel* (bijvoorbeeld wettelijke eisen) of *fundamenteel* voor informatiebeveiliging ([NEN94]). Gemeten kan worden in hoeverre een organisatie voldoet aan de in de documenten gestelde normen.

Kan een onderzoek met als doel het toetsen aan een normenstelsel benchmarking worden genoemd? Indien wordt vergeleken met een normenstelsel vindt geen vergelijking plaats met soortgelijke organisaties, dus kan volgens de definitie niet worden gesproken van benchmarking. In geval van de Code voor Informatiebeveiliging gaat dit niet in zijn geheel op. De Code is gebaseerd op een verzameling van de beste praktijkmethoden van informatiebeveiliging, in algemeen gebruik in vele toonaangevende internationale bedrijven ([NEN94, Krol96]).

Indien de situatie binnen een organisatie niet overeenkomt met die van deze referentiegroep, kan zeker niet worden gesproken van benchmarking. Voor organisaties die soortgelijk zijn aan de bedrijven die hebben meegewerkt aan de Code, kan een vergelijking meer informatie verschaffen over de positie die wordt ingenomen ten opzichte van de Code (en indirect ten opzichte van genoemde internationale bedrijven). Volgens de eerder gegeven definitie in dit artikel zou een dergelijke vergelijking benchmarking kunnen worden genoemd.

Het 'klonen' van beter presterende organisaties is geen weg tot verbetering.

Naar de mening van de auteurs kan wederom niet worden gesproken van benchmarking, omdat vergelijking niet direct met andere organisaties plaatsvindt maar met de 'beste' praktijkmethoden van een aantal organisaties. Vergelijking vindt in dit geval plaats met een soort ideaaltype bedrijf.

Is er bij benchmarking sprake van een norm?

Het is beter om te spreken van referentie-informatie (spiegel) dan van een norm. De benchmarkinformatie dient gebruikt te worden voor bewust maken van bedrijven en instellingen van het bestaan van verschillen tussen organisaties onderling, waarbij er in eerste instantie niet kan worden gesproken over 'goed' of 'fout'. Het advies is om te spreken van 'hoger' of 'lager' ten opzichte van de vergelijkingsmaatstaf. Nadere analyse moet uitwijzen of de geconstateerde verschillen door het benchmarking-proces daadwerkelijk acties tot gevolg moeten hebben.

DE BRUIKBAARHEID VAN BENCHMARKING BIJ EDP-AUDITS

Benchmarking kan op een aantal wijzen worden gebruikt bij EDP-audits:
- benchmarking als onderzoek. Het benchmarking-proces wordt in samenwerking met een bedrijf of instelling uitgevoerd;
- benchmarks als extra hulpmiddel bij de audits.

Indien een organisatie wil weten hoe haar positie is ten opzichte van andere soortgelijke organisaties, kan een benchmarking-onderzoek worden uitgevoerd. Eerder is reeds aangegeven dat het voor een organisatie vaak moeilijk is om het benchmarking-proces zelfstandig uit te voeren. De onafhankelijke positie van EDP-auditors ten opzichte van organisaties en hun concurrenten vormt voor hen een uitstekend uitgangspunt voor het uitvoeren van een dergelijk benchmarking-proces.

Behalve bij het uitvoeren van het benchmarking-proces kunnen de benchmarks als extra hulpmiddel worden gebruikt bij EDP-audits. Een belangrijk voordeel hiervan is dat een organisatie tevens informatie kan worden verschaft over andere (soortgelijke) ondernemingen: de externe spiegel.

Ook kunnen de benchmarks een aantal andere doelen dienen, zoals:
- referentiemateriaal. Door het gebruik van benchmarks kunnen uitgangspunten voor onderzoek worden opgesteld door de sterkte(n) en zwakte(n) ten opzichte van andere organisaties in kaart te brengen. Dit overzicht kan behulpzaam zijn bij het opstellen van de aandachtspunten van onderzoek en mogelijk kunnen prioriteiten van de te ondernemen activiteiten worden aangegeven.
- ondersteuning van aanbevelingen. Als op basis van onderzoek aanbevelingen zijn opgesteld, kunnen de benchmarks worden gebruikt als ondersteunende gegevens;
- 'eye-opener'. Benchmarks kunnen zeer goed als aanknopingspunten worden gebruikt voor het leveren van aanvullende diensten. Het feit dat andere organisaties een hogere score bereiken zal een organisatie er meer van overtuigen dat wegen tot verbetering bestaan.

Tevens leveren de benchmarks de klanten een aanzienlijke hoeveelheid marktinformatie op waardoor het gebruik ervan in zijn algemeenheid als een aan de audit toegevoegde waarde kan worden gezien.

BENCHMARKING VAN DE GENERAL IT CONTROLS

Gezien de toenemende afhankelijkheid van organisaties van automatisering wordt de beheersing van automatisering steeds belangrijker. Al jaren lang worden door EDP-auditors de sterkte(n) en zwakte(n) van de general IT controls in kaart gebracht. Op basis van de beoordeling wordt aan de opdrachtgever een aantal aanbevelingen gedaan hoe verbeteringen kunnen worden aangebracht. In dit proces wordt de desbetreffende organisatie vergeleken met een vooraf vastgesteld (op basis van professional judgement) stelsel van normen. Op basis van deze werkwijze is het echter niet mogelijk de opdrachtgever een beeld te geven van zijn performance ten opzichte van andere (soortgelijke) organisaties.

Door de general IT control-gegevens op een consistente en systematische wijze in een database te verzamelen is het mogelijk benchmarks samen te stellen. Aan de hand van de eerder genoemde benchmarking-processtappen wordt deze methode weergegeven.

Selecteer het onderwerp van benchmarking: general IT controls

De betrouwbaarheid van een IT-systeem wordt beheerst door computercontroles met een algemeen karakter (de general IT controls of algemene computercontroles) en computercontroles die zich richten op de betrouwbare werking van een specifieke applicatie (de application controls of toepassingscontroles, [Munc95]). Bij voortschrijdende automatisering worden onder meer uit efficiëntieoogpunt in toenemende mate controles in de applicatie geïmplementeerd. Om ervoor te zorgen dat deze application controls bij voortduring effectief zijn, worden hogere eisen gesteld aan de general IT controls. De general IT controls dienen te voldoen aan de steeds hogere eisen die de administratieve organisatie en de applicaties stellen.

Op basis van de aandachtsgebieden van de general IT controls zijn de volgende belangrijke beheersgebieden te onderscheiden met de doelstellingen voor de te nemen maatregelen:

- *Beleid en management*

Deze maatregelen zijn gericht op het vaststellen dat het beleid van een organisatie en de managementprocedures effectief zijn in de beheersing van de automatiseringsfunctie.

- *Informatiebeveiliging*

Hieronder vallen maatregelen die zijn gericht op de beveiliging van de (kritieke) informatie. De logische toegangsbeveiliging vormt hier een onderdeel van. In toenemende mate wordt informatie opgenomen in geïntegreerde informatiesystemen zodat gezamenlijk gebruik van gegevens mogelijk is. Om de in de administratieve organisatie opgenomen functiescheidingen ook in deze informatiesystemen te kunnen realiseren wordt gebruik gemaakt van logische toegangsbeveiliging.

- *Fysieke beveiliging*

Deze maatregelen zijn gericht op het minimaliseren van het risico van bewust of per ongeluk veroorzaken van schade aan of diefstal van bijvoorbeeld computerapparatuur, programmatuur en gegevens. Tevens spelen omgevingsomstandigheden zoals de stroomvoorziening een rol.

- *Continuïteit*

De maatregelen omtrent continuïteit zijn gericht op het bewerkstelligen van een ongestoorde voortgang van de gegevensverwerking.

- *Change management*

Dit betreft maatregelen inzake technische en organisatorische veranderingen die binnen een organisatie plaatsvinden. Change management is het proces van evalueren, plannen en coördineren van de implementatie en van de wijzigingen in de informatiesystemen en de verwerkingsorganisatie. Omdat elke verandering in principe bedreigingen met zich meebrengt, is het belangrijk maatregelen te nemen.

- *Systeemontwikkeling/aankoop van systemen*

Deze maatregelen zijn gericht op het zeker stellen dat ontwikkelde of standaardsystemen en wijzigingen in programmatuur geautoriseerd, getest, gedocumenteerd en gerealiseerd worden. Dit om ervoor te zorgen dat de systemen voldoen aan de wensen van de gebruikers.

- *Beoordeling van automatisering*

Organisaties zijn voortdurend in beweging. Om te controleren of de huidige automatiseringssituatie nog steeds voldoet aan de eisen en wensen van de organisatie, moeten maatregelen zijn getroffen die

waarborgen dat de automatisering periodiek wordt beoordeeld.

Selecteer bedrijven en/of instellingen waarmee vergelijkingen plaatsvinden

De vergelijking van de general IT controls kan met verschillende organisaties worden uitgevoerd. Om zinvolle vergelijkingen te kunnen maken, vindt vergelijking plaats met gegevens van soortgelijke organisaties. Soortgelijke organisaties kunnen worden getypeerd op punten als:
- het soort organisatie;
- de automatiseringsorganisatie;
- de afhankelijkheid en betrouwbaarheid van automatisering.

Typering organisatie
Bedrijven en instellingen verschillen ten opzichte van elkaar in onder meer branche en omvang. De omvang van een organisatie kan nader worden gespecificeerd door de omzet, het aantal medewerkers, het aantal automatiseringsmedewerkers en het IT-budget (de IT-kosten).

Typering automatiseringsorganisatie
De organisatie van automatisering heeft met name invloed op de inrichting van de te treffen (beveiligings)maatregelen. Naar een onderzoek van Spruit en Looijen ([Spru94]) naar de beveiliging van de informatievoorziening kan de automatiseringsorganisatie grofweg als volgt worden getypeerd:
- *geconcentreerd:* de automatiseringsmiddelen zijn gegroepeerd in een cluster (concentratie), zoals in een reken-, computer- of servicecentrum;
- *gespreid:* de automatiseringsmiddelen zijn in zekere mate gespreid (bijvoorbeeld opgesteld bij de gebruikers of op gebruikersafdelingen) en zijn al of niet gekoppeld aan elkaar of aan geconcentreerde middelen.

Bij benchmarking van de general IT controls kan een dergelijke typering van automatisering worden gebruikt. Er kan bijvoorbeeld onderscheid worden gemaakt naar geconcentreerd (een centrale omgeving, bijvoorbeeld een mainframe-omgeving), gespreid (een decentrale omgeving, bijvoorbeeld een PC-LAN-omgeving) en een tussenvorm (bijvoorbeeld een midrange-omgeving). Genoemde omgevingen worden in de praktijk vaak in combinatie met elkaar aangetroffen. De typering kan dan plaatsvinden door aan te geven waar het zwaartepunt van gegevensverwerking ligt.

Afhankelijkheid en betrouwbaarheid
Een derde typering kan plaatsvinden aan de hand van de afhankelijkheid van de beschikbaarheid van de automatisering en de betrouwbaarheid. Indien hogere eisen worden gesteld aan de beschikbaarheid en de betrouwbaarheid van automatisering, zal de inrichting en beheersing van de automatiseringssituatie verschillen met die van een situatie waarin langere tijd zonder automatisering kan worden gewerkt en/of minder hoge eisen worden gesteld aan de betrouwbaarheid.

Bepaal de methode van gegevensverzameling

De gegevens kunnen worden verzameld met behulp van vragenlijsten, interviews, documentatie of workshops. Naast het stellen van gerichte vragen aan de juiste personen is het voor het verwerken van de gegevens van belang dat deze onderling vergelijkbaar zijn. Dit betekent dat voor het verzamelen van de gegevens een bepaalde methodiek moet worden gebruikt waardoor de verzamelde informatie onderling vergelijkbaar is. Om deze onderlinge vergelijkbaarheid te bewerkstelligen moeten de vragen zodanig zijn geformuleerd dat de beantwoorder weinig ruimte wordt gegeven voor het formuleren van 'eigen' antwoorden. Voorbeelden van dergelijke vragen zijn de leeftijd van een persoon (dus één antwoord mogelijk) en of deze persoon in het bezit is van een rijbewijs (alleen ja of nee mogelijk).

Een andere mogelijkheid is het vooraf definiëren van antwoorden. De vraag kan bijvoorbeeld worden beantwoord door één van de vijf mogelijkheden aan te geven, waarbij elke mogelijkheid een eigen betekenis heeft (zie kader 1). Belangrijk bij deze aanpak is dat de beantwoorder de ruimte moet krijgen om opmerkingen of alternatieven te vermelden bij de desbetreffende vraag.

Alleen als de antwoorden en daarmee de verzamelde gegevens van hetzelfde formaat zijn, is het mogelijk de benchmarks (gegevens) onderling te vergelijken (eventueel aangevuld met het relateren van de gegevens aan bepaalde grootheden).

Een tweede aandachtspunt dat speelt bij het benchmarken van maatregelen is het inhoudelijke aspect dat wordt gemeten. De general IT controls kunnen

Kader 1. Voorbeeld definiëring mogelijke antwoorden.

Vraag: Zijn er maatregelen getroffen omtrent de fysieke beveiliging van computerapparatuur?

Antwoord:
1 = Geen maatregelen.
2 = Informele maatregelen.
3 = Formele maatregelen. De maatregelen worden consequent gehanteerd/toegepast.
4 = Formele maatregelen. De maatregelen worden consequent gehanteerd/toegepast. De sterkte(n) en zwakte(n) van de maatregelen worden gemeten. Resultaten worden gerapporteerd waarop vervolgens actie wordt ondernomen.
5 = Gelijk aan 4. Aansluitend vindt feedback van de metingen plaats (aan eindverantwoordelijke) met als doel het verbeteren van de performance. Verbetering vindt daadwerkelijk plaats.

met verschillende mate van diepgang worden gemeten op de volgende aspecten:
- opzet: de maatregel wordt in opzet beoordeeld;
- bestaan: het bestaan (aanwezigheid) van de maatregel wordt beoordeeld;
- werking: de werking (toepassing) van de maatregel wordt beoordeeld.

Door naast de opzet het bestaan en de werking te toetsen, kan worden geconstateerd dat de maatregelen niet alleen op papier bestaan maar ook zijn geïmplementeerd en effectief werken in de praktijk. De keuze voor een of meer aspecten is afhankelijk van de eisen en wensen van een organisatie.

Verzamelen en analyseren van de gegevens

De general IT controls die worden aangetroffen in een organisatie kunnen van een verschillend kwaliteitsniveau zijn. Het is dan ook van belang om naast het meten van de aanwezigheid van de maatregel, de kwaliteit van de maatregel in kwestie te meten. Om een dergelijke meting uit te voeren, kan niet worden volstaan met een ja- of nee-antwoord. Als een vraag met ja wordt beantwoord, is niet duidelijk wat de kwaliteit van de maatregel is. Dit probleem kan worden ondervangen door de antwoorden in te delen in categorieën zoals in kader 1 is gedaan. Door de general IT controls op deze wijze te meten, met behulp van de daartoe geschikte hulpmiddelen, kunnen de gegevens daadwerkelijk worden verzameld en vastgelegd in een database.

Database
In de database moeten de typeringsgegevens en automatiseringsgegevens van de organisaties zodanig zijn opgeslagen dat het mogelijk is met de gegevens bewerkingen en/of berekeningen uit te voeren. Om voldoende vergelijkbare bedrijven of instellingen te kunnen selecteren, dient de database niet alleen de gegevens van een groot aantal bedrijven te bevatten maar dient deze ook voldoende te zijn gesegmenteerd. Beide overwegingen leiden tot de noodzaak van het opbouwen en onderhouden van een relatief grote database. Het zal voor een organisatie vrijwel ondoenlijk zijn voor elke benchmark opnieuw relevante gegevens van andere organisaties te verkrijgen. Reeds eerder in dit artikel is aangegeven dat een oplossing voor een dergelijk probleem wordt geboden door de vergelijkingsgegevens te betrekken van een in benchmark-databases gespecialiseerde organisatie.

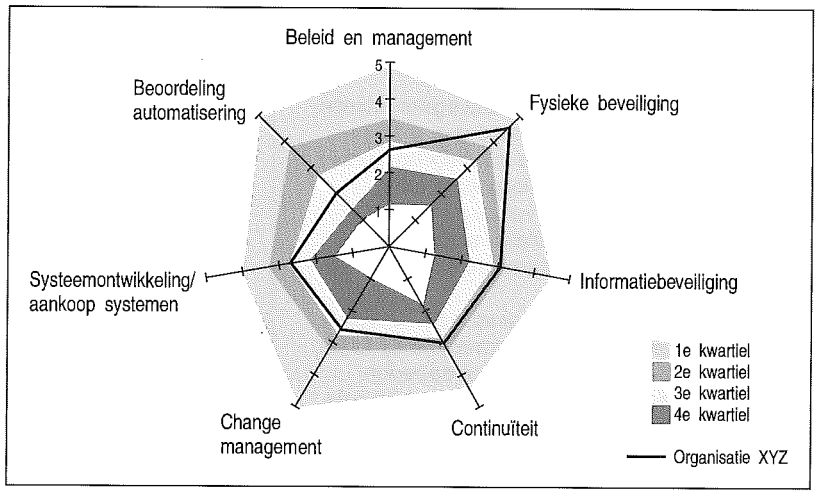
Beveiliging en onderhoud van de database
Naast het opzetten en het vullen van de database zijn het onderhoud en de beveiliging van een dergelijke database van groot belang voor de kwaliteit van het referentiemateriaal en de bescherming van de gegevens. Het beveiligen van de gegevens in de database dient een tweeledig doel. Enerzijds is het belangrijk dat de database voldoende is beveiligd tegen ongeautoriseerde raadplegingen of wijzigingen door onbevoegden. Anderzijds moet anonimiteit van de gegevens zijn gewaarborgd. Het moet voor organisaties niet mogelijk zijn andere organisaties te 'herkennen' in de resultaten. Vergelijking moet derhalve plaatsvinden met een minimum aantal bedrijven en instellingen zodat de herkomst van de gegevens niet herleidbaar is. Het is belangrijk organisaties toestemming te vragen voor het opnemen van de gegevens in de database. Tevens zal de waarborg van de anonimiteit van de gegevens duidelijk aan de desbetreffende organisatie kenbaar moeten worden gemaakt.

Het onderhoud van de database betreft het verwerken en updaten (aanpassen en verwijderen) van de gegevens. Het updaten van de database vormt een belangrijk onderdeel omdat op het gebied van automatisering ontwikkelingen elkaar in een hoog tempo opvolgen waardoor gegevens snel verouderen. Verouderde gegevens moeten dan ook uit de database worden verwijderd, zodat deze gegevens de bepaling van de benchmarks niet kunnen beïnvloeden. Behalve dit verwijderen is het van belang dat de benchmarks en daarmee ook de te verzamelen gegevens inhoudelijk periodiek worden geëvalueerd en aangepast aan de laatste ontwikkelingen.

Analyseren van de gegevens
Door een selectie te maken uit de database van de scores van bijvoorbeeld organisatie XYZ en de organisaties waar deze mee zal worden vergeleken (bijvoorbeeld dezelfde branche), kan vergelijking plaatsvinden. Het resultaat van de vergelijking kan op een aantal manieren worden weergegeven. In figuur 3 staat een voorbeeld van een mogelijke presentatie.

De zwarte lijn in figuur 3 geeft de (gemiddelde) score van organisatie XYZ weer. Deze score is vergeleken met de voor onderneming XYZ relevante organisaties (populatie). De scores van de populatie zijn weergegeven in kwartielen (25-procentsintervallen) waardoor de spreiding van de scores binnen deze populatie beter zichtbaar is. Belangrijk aandachtspunt bij de vergelijking is dat de scores van de opdrachtgever niet zijn opgenomen in het vergelijkingsmateriaal. Een reden die hieraan ten grondslag ligt is dat het voor een organisatie anders onmogelijk wordt om 'hoger' (of 'lager') te scoren dan de populatie. De figuur geeft slechts de situatie van een organisatie weer voor dat moment.

Figuur 3. Voorbeeld benchmark general IT controls.



In de terugkoppeling zal de datum derhalve duidelijk moeten worden aangegeven.

Door de general IT controls op deze wijze terug te koppelen aan een organisatie is in één oogopslag zichtbaar waar de zwakte(n) liggen ten opzichte van de geselecteerde populatie. Tevens wordt een gebalanceerde presentatie van general IT controls weergegeven, immers, naast de afwijkingen in negatieve zin zijn ook de afwijkingen in positieve zin van de organisatie af te lezen.

Actie naar aanleiding van de vergelijking

Op basis van de analyse kunnen actiepunten worden opgesteld. Voordat daadwerkelijk kan worden overgegaan tot het ondernemen van actie naar aanleiding van de resultaten is het van belang om de resultaten van het benchmarking-proces te evalueren. Evaluatie kan voor de general IT controls op twee manieren plaatsvinden:

- constateren en evalueren van verschillen ten opzichte van soortgelijke organisaties;
- evalueren sterkten en zwakten van de organisatie ten opzichte van het 'eigen' risicoprofiel (afhankelijkheid van de beschikbaarheid van automatisering en de betrouwbaarheid van automatisering).

Het is volgens de auteurs noodzakelijk om minstens deze twee vergelijkingen te maken omdat het risico bestaat dat de populatie bestaat uit 'laag' scorende organisaties waardoor het benchmarking-proces geen zwakke plekken weergeeft terwijl deze wel degelijk aanwezig zijn. Door tevens een vergelijking te trekken naar de risico's omtrent automatisering, het gewenste profiel van de organisatie en de kennis en ervaring van de EDP-auditor wordt het genoemde gevaar bestreden. Indien duidelijk is waar de knelpunten voor de organisatie liggen kan een actieplan worden ontwikkeld.

TOT SLOT

Door het gebruik van benchmarks, zoals de IT controls benchmark, krijgen organisaties naast marktinformatie (hoe doet een organisatie het ten opzichte van andere organisaties) een gebalanceerder beeld van de getroffen maatregelen omtrent de beheersing en controls van automatisering gepresenteerd. Naast de afwijkingen in negatieve zin worden ook de (eventuele) afwijkingen in positieve zin teruggekoppeld.

Voor het analyseren van de uitkomsten van benchmarking, op het gebied van de geautomatiseerde gegevensverwerking, moeten de resultaten kunnen worden geïnterpreteerd en geëvalueerd. Hierbij kan de EDP-auditor een belangrijke rol spelen. Benchmarking moet in een samenhangend geheel worden toegepast, dat wil zeggen of als proces of als extra hulpmiddel bij EDP-audits. Het gevaar dat wordt vergeleken met 'slecht' scorende organisaties is reeds besproken, maar geeft duidelijk aan hoe belangrijk het is om naast benchmarks de normen van de EDP-auditor tegen een organisatie aan te leggen. Nogmaals wordt benadrukt dat benchmarks geen normen maar slechts indicatoren zijn: spiegelinformatie. Deze spiegel heeft als belangrijkste doel het laten zien van afwijkingen ten opzichte van andere organisaties.

LITERATUUR

[Camp89] R.C. Camp, *Benchmarking: The search for Industry Best Practices That Lead to Superior Performance*, Milwaukee WI, Quality Press, 1989.

[Donk95] J.A.M. Donkers, M. Groesz en J.A. Verstelle, *Informatietechnologie: Management control van de geautomatiseerde informatievoorziening*, Controlling in de praktijk 11, Kluwer Bedrijfswetenschappen, 1995.

[Krol96] W.S.C. Krol en M.M. Smits, *De Code voor Informatiebeveiliging als norm voor de EDP-auditor*, Compact 96/1.

[Looi89] M. Looijen, *Management en organisatie van automatiseringsmiddelen*, Kluwer Bedrijfswetenschappen, 1989.

[Mana94] Management Team, *Business Topics: Benchmarking, spiegelen aan de beste in class*, nummer 4, november 1994.

[Munc95] W.A. de Munck, *Informatietechnologie als beoordelingsobject in de hedendaagse controlebenadering*, Compact 95/3.

[NEN94] *Code voor Informatiebeveiliging, Een leidraad voor beleid en implementatie*, Nederlands Normalisatie-Instituut, 1994.

[Pryo89] L.S. Pryor, *Benchmarking: A Self-Improvement Strategy, The Journal of Business strategy*, November/December 1989.

[Spru94] M.E.M. Spruit en M. Looijen, *Beveiliging van de informatievoorziening*, Onderzoek op basis van een landelijke enquête '93-'94 door de sectie Beheer van Informatiesystemen van de Technische Universiteit Delft, oktober 1994.

[Vrie95] G.K. de Vriend en A. Timmerman, *Benchmarking, een strategie om concurrentievoordeel te behalen*, Controlling in de praktijk 12, Kluwer Bedrijfswetenschappen, 1995.

[Zee94] H.T.M. van der Zee, *Kwantitatieve kwaliteitsverbetering en benchmarking van de informatievoorziening*, Praktijkgids De Controller & Informatiemanagement, afl. 8, maart 1994.

Ir. J.A.M. Donkers RE
Is als EDP Audit Manager werkzaam bij KPMG EDP Auditors. Hij is tevens als docent betrokken bij de post-doctorale opleiding EDP-auditing van de Erasmus Universiteit Rotterdam.

Mw. ir. E.R. van Sommeren
Is afgestudeerd aan de Technische Universiteit Twente in de Technische Bedrijfskunde op een onderzoek naar de mogelijkheden voor het gebruik van benchmarking door EDP-auditors. Sinds 1995 is zij werkzaam bij KPMG EDP Auditors. Zij neemt momenteel deel in een internationaal KPMG-project ten behoeve van de verdere invoering van benchmarking van general IT controls binnen KPMG.

AS/400-networking

Mw. drs. A.L. Hristova RE

Een basisprobleem bij het uitvoeren van een audit op de AS/400 in een netwerkomgeving is het expliciteren van de eisen van interne controle. Daarnaast is het vaak moeilijk de eisen op een juiste wijze te vertalen naar specifieke systeeminstellingen. De auteur geeft een gestructureerde aanpak van deze vertaalslag en behandelt tot slot de audit ervan.

INLEIDING

De verhandelingen over AS/400-audits bevatten vaak geen analyse van de concepten achter de AS/400, maar beperken zich of tot auditvragen op hoog abstractieniveau (en dus nauwelijks meer specifiek voor de AS/400), of tot security-risico's op laag detailleringsniveau. Dit komt overeen met de algemene trend in de technische EDP-auditliteratuur.

De reden daarvan zou kunnen zijn dat deze verhandelingen niet door specialisten in de desbetreffende materie zijn geschreven, maar door daarin geïnteresseerde onafhankelijke derden, die de voorkeur geven aan algemene stellingen.
De invalshoek is immers anders. Waar de specialist schrijft voor vakgenoten, schrijft de EDP-auditor voor het management, dat meestal geen specialist is.

In dit artikel wordt vooral gepoogd de 'missing link' tussen de abstractie en het detail te geven, namelijk het concept achter en de analyse van de AS/400-datacommunicatie-aspecten, die hier met het begrip AS/400-networking worden aangeduid. Hiertoe worden in deel 1 de achtergronden van AS/400 toegelicht. Daarbij zal de nadruk liggen op de (netwerk-)architectuurconcepten, netwerkattributen, -objecten en -parameterinstellingen van de AS/400.

Deel 2 bespreekt de functionaliteit en de beveiligingsrisico's van de netwerkfuncties en -software van de AS/400, te weten: APPC/APPN (Advanced Program-to-Program Communication/Advanced Peer-to-Peer Networking), DSPT (Display Station Pass-Through), DDM (Distributed Data Management), SNADS (SNA Distribution Services) en PC Support, een PC-AS/400-datacommunicatiepakket.

In deel 3 zullen de specifiek voor de technische audits van belang zijnde onderwerpen worden behandeld.
Dit soort audits wordt vooralsnog met meer kunde uitgevoerd door dienstverlenende automatiseringsbedrijven dan door (interne of externe) EDP-auditors of door de gebruikersorganisaties zelf. De laatste twee categorieën zijn over het algemeen minder goed in staat AS/400-auditinformatie met voldoende relevantie en diepgang te verzamelen, terwijl de mogelijkheden daarvoor de laatste tijd juist groter worden, in de vorm van nieuwe audittools en functies voor de geavanceerde AS/400-modellen.

DEEL 1: ACHTERGRONDEN VAN DE AS/400-NETWORKING

In dit deel zullen achtereenvolgens worden behandeld:
- de bouwstenen voor de AS/400-networking, te weten:
  - het OS/400-besturingssysteem;
  - de IBM-netwerkarchitecturen;
- de belangrijkste aspecten van de AS/400-networking, zoals:
  - de AS/400-netwerkattributen;
  - de AS/400-communicatie-objecten;
  - de implementatie van de IBM-netwerkarchitecturen op de AS/400;
- de AS/400-netwerkservices in SNA, te weten:
  - de AS/400-netwerkservices (per SNA-laag), met nadruk op
  - de services van de applicatielaag;
- het configureren van de AS/400 voor netwerkgebruik.

Het OS/400-besturingssysteem

De AS/400 is een IBM-midrangecomputer die evenals de andere IBM-hardwareplatformen (MVS, VM en OS/2) ondersteund wordt door de System Applications Architecture (SAA) van IBM. SAA bewerkstelligt de onderlinge consistentie, connectiviteit en applicatie-overdraagbaarheid tussen de verschillende IBM-systemen.

De AS/400 opereert onder het OS/400-besturingssysteem (Operating System/400)[1]. Dit is een object-georiënteerd systeem. Alles wat op het systeem is gedefinieerd (gebruikers, bestanden, programma's, systeemcommando's, apparatuur), is een object. De consistentie van alle AS/400-objecten wordt bewaakt door een in het besturingssysteem geïntegreerde database, die vanaf versie 3 van het OS/400-besturingssysteem expliciet DB/400 wordt genoemd. Een apart database-managementsysteem (DBMS) is voor de AS/400 niet nodig.

De AS/400 wordt geconfigureerd door middel van *systeemparameters*. Qua functies vallen de AS/400-systeemparameters uiteen in twee hoofdgroepen:
- operationele parameters, die zaken regelen op het gebied van het work-, storage- en memory-management;
- beveiligingsparameters.

De tweede groep systeemparameters, namelijk de beveiligingsparameters, kan weer worden ingedeeld in twee groepen:
- parameters die betrekking hebben op de AS/400-systeembeveiliging;
- parameters die betrekking hebben op de AS/400-gebruikersbeveiliging.

De parameters die betrekking hebben op de AS/400-gebruikersbeveiliging zijn ten slotte nader te verdelen in:
- password management-parameters;
- autorisatieparameters.

Van de eerste groep beveiligingsparameters, te weten de parameters met betrekking tot de AS/400-systeembeveiliging, is het *beveiligingsniveau* (QSECURITY) de belangrijkste parameter. In dit artikel wordt uitgegaan van niveau 30 of hoger, omdat alleen dan de AS/400-objectbeveiliging actief is en de hieronder beschreven autorisatiestructuur geldig is.

De bevoegdheden van de gebruikers voor het systeem worden vastgelegd in *gebruikersprofielen*. Een deel van de parameters in de gebruikersprofielen is gekoppeld aan de autorisatieparameters op systeemniveau. In het gebruikersprofiel kunnen deze waarden echter individueel worden gewijzigd.

De gebruikersprofielen kunnen *individuele profielen* of *groepsprofielen* zijn. In de groepsprofielen worden bevoegdheden voor een hele groep gebruikers gedefinieerd. Technisch wordt dit gerealiseerd door de profielen van de individuele gebruikers aan het groepsprofiel te koppelen.
Daarnaast kunnen per gebruiker in diens individuele gebruikersprofiel bevoegdheden worden gedefinieerd, die afwijken van de voor hem geldende groepsbevoegdheden. De individuele bevoegdheden hebben dan prioriteit boven de groepsbevoegdheden; de groepsbevoegdheden op hun beurt hebben weer prioriteit boven de bevoegdheden die op systeemniveau zijn gedefinieerd.

De AS/400 is menugestuurd. Dit houdt in dat de meeste systeemcommando's in menu's zijn opgenomen. Daarnaast is het mogelijk vanaf een commandoregel OS/400-systeemcommando's te geven. In het gebruikersprofiel wordt aangegeven of de gebruiker hiertoe bevoegd is.

Alle objecten van de AS/400 zijn ondergebracht in bibliotheken. Dit kunnen systeembibliotheken of gebruikersbibliotheken zijn. Bibliotheken zijn ook objecten. De gebruikers kunnen beschikken over rechten tot bibliotheken en tot de daarin aanwezige objecten. Deze rechten heten 'specific authorities', nader te verdelen in:
- 'object authorities': bevoegdheden tot manipulaties met een object als geheel;
- 'data authorities': bevoegdheden tot manipulaties met de gegevens van een object.

Daarnaast kunnen aan de gebruikers ook 'special authorities' worden toegekend. Deze bevoegdheden geven recht tot het uitvoeren van systeemfuncties. Dit zijn administratieve, operationele en managementfuncties. Vanaf versie 3 van het OS/400-besturingssysteem zijn hieraan ook auditfuncties toegevoegd.

De kenmerken van objecten worden vastgelegd in objectbeschrijvingen. Daarin staat ook welke gebruikers tot dat object zijn toegelaten. Tegelijkertijd wordt in het gebruikersprofiel vastgelegd tot welke objecten de gebruiker is geautoriseerd.

De toekenning van bevoegdheden aan gebruikers tot objecten kan ook groepsgewijs geschieden, door middel van de zogenaamde 'autorisatielijsten'. In een autorisatielijst wordt per individueel object aangegeven welke gebruikers over welke bevoegdheden tot dat object beschikken.

1. De functies van het OS/400-besturingssysteem worden hier niet beschreven omdat ze in essentie niet verschillen van de functies van andere besturingssystemen (CPU-besturing, I/O en command processing, storage access, etc.).

De IBM-netwerkarchitecturen

De AS/400 is een IBM-produkt en kan als zodanig deel uitmaken van een SNA-netwerk. Het kan ook gebruik maken van de SNA-netwerkservices.

SNA
SNA (Systems Network Architecture) is de netwerkarchitectuur van IBM. Zij definieert standaard-datacommunicatiefuncties en protocollen voor de hele produktlijn van IBM-computers.
In zijn klassieke vorm is SNA een gelaagde architectuur, gebaseerd op hiërarchische verhoudingen tussen een centraal mainframe (master) en mainframe-afhankelijke apparatuur zoals terminals en printers (slaves).
In deze communicatie speelde het mainframe de leidende rol. Communicatie tussen slaves onderling, zonder tussenkomst van het mainframe, was niet mogelijk.

Wijziging van één netwerkattribuut heeft implicaties voor alle gerelateerde systeemparameters.

Een SNA-netwerkcomponent vormt een knooppunt ('node') in het netwerk. Elke component is een PU (Physical Unit). De functies van de PU zijn vastgelegd in een logische definitie, de LU (Logical Unit). Een netwerkcomponent is volledig beschreven door de PU/LU-combinatie.
Een LU kan behalve fysieke hardwarefuncties ook softwarefuncties beschrijven. Zo kan bijvoorbeeld een netwerkverbinding of een verbinding tussen twee 'remote' applicaties worden beschreven aan de hand van LU/LU-combinaties.

Met de komst van de gedistribueerde gegevensverwerking, alsmede van intelligente kleinere systemen zoals de IBM 3X/400-midrangelijn (S/36, S/38 en AS/400) en PC's, ontstond de behoefte aan directe communicatie tussen intelligente netwerkcomponenten onderling (zoals gedistribueerde applicaties of intelligente 3X/400's en PC's), zonder tussenkomst van de master. In de klassieke SNA-opzet waren alleen de slave-functies voor deze componenten beschikbaar.

APPC
Om directe communicatie tussen intelligente netwerkcomponenten mogelijk te maken, ontstond de SNA-uitbreiding APPC (Advanced Program-to-Program Communication). In APPC vindt er communicatie plaats tussen gelijkwaardige partners (zoals tussen applicaties op twee verschillende remote systemen), in plaats van communicatie tussen masters en slaves.
APPC werkt op basis van de LU6.2/PU2.1-combinatie. Dit zijn intelligente LU- en PU-typen. LU6.2 staat voor APPC-communicatie tussen applicaties op twee remote systemen. Met PU2.1 worden de 3X/400-systemen aangeduid.
Omdat bij APPC verbindingen tussen PU's en LU's worden gelegd zonder tussenkomst van het mainframe, heet dit soort networking Low Entry Networking (LEN).
De APPC-communicatie kent de beperking dat alleen communicatie tussen direct aan elkaar grenzende systemen ('adjacent nodes') mogelijk is.

APPN
Later is APPN (Advanced Peer-to-Peer Networking) ontstaan. APPN is een uitbreiding van APPC. Het is ontstaan uit de behoefte netwerkmanagementfaciliteiten aan te bieden voor de APPC-netwerken.
Met APPN is ook communicatie tussen niet direct aan elkaar grenzende systemen ('intermediate nodes') mogelijk. De netwerkadressen van gebruikers worden in netwerk-directories bijgehouden. Op basis daarvan kunnen de eindbestemming en de route van berichten over het netwerk worden bepaald. De directories en de routes kunnen centraal worden beheerd.

AS/400-networking

De datacommunicatiefuncties van de AS/400 zijn gebaseerd op de APPC- en APPN-uitbreidingen van SNA. AS/400 kan alleen met APPC werken dan wel voor APPN worden geconfigureerd. De AS/400 wordt geconfigureerd voor netwerkgebruik met de AS/400-netwerkattributen en -communicatie-objecten.

AS/400-netwerkattributen
In de netwerkattributen worden kenmerken vastgelegd die betrekking hebben op de systeem- en netwerkidentificatie, alsmede op het gebruik van APPN en van de AS/400-netwerkservices. De netwerkattributen hebben net als de systeemparameters een 'system-wide' werking. Dit houdt in dat de wijziging van één attribuut implicaties heeft voor alle gerelateerde systeemparameters.
De AS/400-netwerkattributen bevinden zich in de Network Attributes Table *NETATR. Deze tabel kan worden bekeken met het Display Network Attributes (DSPNETA)-commando en worden gewijzigd met het Change Network Attributes (CHGNETA)-commando.

AS/400-communicatie-objecten
Om de AS/400 in een netwerk op te nemen, moeten de AS/400-communicatie-objecten worden gedefinieerd. De belangrijkste AS/400-communicatie-objecten zijn:
- line description (LIND);
- controller description (CTLD);
- mode description (MODD);
- device description (DEVD).

De functie en de onderlinge samenhang van de vier AS/400-communicatieparameters zijn afgebeeld in figuur 1.

De mode description (MODD) is zowel bij APPC als bij APPN nodig. Een vijfde object, de class-of-service (COS)-parameter, wordt alleen gebruikt

bij APPN. MODD en COS zijn niet van toepassing op niet-SNA-aansluitingen, zoals bijvoorbeeld TCP/IP of Novell.
Bij aansluiting op een ISDN-netwerk moeten aanvullend nog twee communicatie-objecten worden gedefinieerd. Dit zijn de network interface description (NWID) en de connection list (CNNL).

AS/400 en de IBM-netwerkarchitecturen

In deze paragraaf worden kort de benodigde definities voor controllers en devices voor IBM-netwerkarchitecturen aangegeven.

AS/400 en SNA
SNA (en als gevolg daarvan ook APPN en APPC) kent geen 'high level' adressen[2] en kan om die reden geen gebruik maken van routers. In plaats daarvan fungeren de computers in een SNA/APPC/APPN-netwerk zelf als router. Ze houden zowel de lokale als de remote netwerk- en locatie-id's bij, alsmede de id's van de lokale en remote controllers en devices.

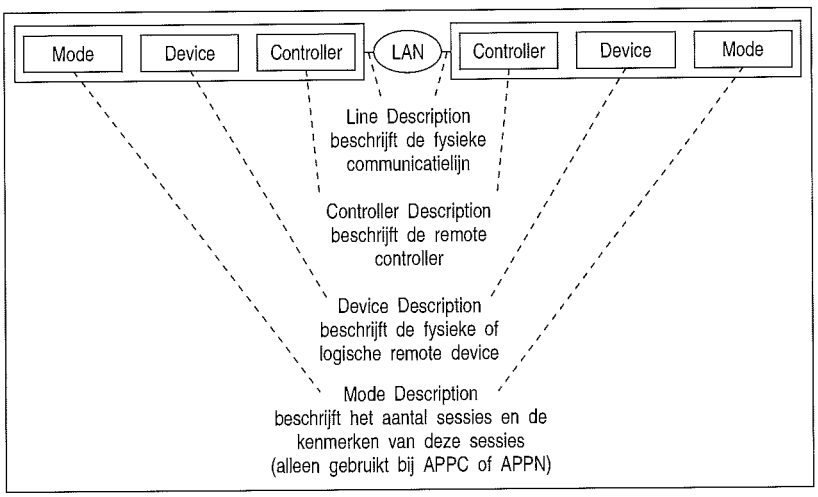
Ook de AS/400 wordt op deze wijze geconfigureerd. Dit houdt in dat op alle in een netwerk opgenomen systemen er definities moeten bestaan zowel van het individuele systeem (de lokale AS/400) als van alle overige (remote) systemen. Dit hoeven niet per se andere AS/400's te zijn, als het maar systemen zijn die over SNA-, APPC- of APPN-functies beschikken.

AS/400 en APPC
In de AS/400-controller- en -device-definities wordt vastgelegd of de AS/400-configuratie gebruik maakt van APPC of van APPN.

APPC wordt toegepast bij datacommunicatie tussen AS/400's onderling en in lokale netwerken, zoals Token-Ring, Ethernet of PC-LAN. Wanneer gebruik wordt gemaakt van APPC, moeten er overeenkomstige APPC-controllers en -devices worden gedefinieerd.
Voor niet-APPC-aansluitingen (zoals een verbinding met een SNA-mainframe master) of voor niet SNA-aansluitingen (zoals TCP/IP of Novell), zijn niet-APPC-controller- en -device-definities nodig.

In de line, controller en device descriptions moet vastliggen welke rol de AS/400-node in het netwerk vervult als PU2.1 in een PU2.1/LU6.2-(APPC)-combinatie (met of zonder APPN):
- primary (*PRI);
- secondary (*SEC);
- negotiable (*NEG).

De primary role is bestemd voor de centrale AS/400 (de server) die de secondary AS/400's (de clients) in het netwerk bestuurt. De negotiable role wordt gebruikt voor gateway-computers, welke aan de grens tussen twee netwerken (bijvoorbeeld APPC en APPN) worden geplaatst.



Figuur 1. As/400-communicatie-objecten

AS/400 en APPN
Indien behalve van APPC ook van APPN gebruik wordt gemaakt, moeten de APPC-controllers en -devices tevens als 'APPN-capable' worden gedefinieerd. Dit wordt aangegeven door APPN(*YES) te definiëren in de APPC-device en -controller descriptions.
Daarnaast moet de controller als APPN-node worden gedefinieerd. Dit vindt plaats in de NODE-TYPE-parameter van de controller description.

Ten slotte moeten zowel op de lokale als op de remote AS/400's lokale respectievelijk remote configuration lists (QAPPNLCL en QAPPNRMT) worden aangemaakt. Op basis van deze lijsten wordt de route tussen niet-aangrenzende nodes in het APPN-netwerk bepaald. In de lijsten zijn alle op het APPN-netwerk aangesloten systemen opgenomen.

De AS/400-netwerkservices in SNA

De SNA-netwerkservices zijn ondergebracht in zeven hiërarchische lagen. Dit zijn de physical control layer, de data link control layer, de path control layer, de transmission control layer, de data flow control layer, de presentation services layer en de transaction services layer.
Op elk SNA-niveau zijn netwerkdiensten voor de AS/400 beschikbaar. De belangrijkste services zijn in tabel 1 afgebeeld.

De AS/400-netwerkservices van de SNA-applicatielaag

De AS/400-netwerkservices maken gebruik van de netwerkmanagement-functies van de IBM Network Management Architecture (NMA).
De NMA-functies zijn gerealiseerd in Netview, het IBM-produkt voor gecentraliseerd netwerkbeheer (primair ontwikkeld voor de S/370-systemen) en in SystemView, de netwerkmanagement-uitbreiding voor open systemen.

Netview
De Netview-functionaliteiten zijn opgenomen in de 3X/400-produkten die de basis-SNA-netwerk-

2. Dit zijn adressen op netwerk protocol-niveau, in tegenstelling tot de 'low level' LAN-adressen op access protocol-niveau.

AS/400

Transaction (Application) Services Layer

3X/400-services:
- Display Station Pass-Through (DSPT)
- Distributed Data Management (DDM)
- SNA Distributed Services (SNADS)
- APPC Communication programming interfaces (ICF, CPI-C, FTS)

APPC Layer (LU6.2)

VMC Layer (APPN, PU2.1)

Data Link Control Layer:
- SDLC
- X.25
- Token-Ring

Tabel 1. De belangrijkste AS/400-netwerk- services in SNA.

services bewerkstelligen. Dit zijn de APPC/APPN-functies, DSPT (Display Station Pass-Through), DDM (Distributed Data Management), SNADS (SNA Distribution Services) en de Alert Facility.

De 3X/400-netwerkservices van Netview
DSPT is een remote login service. DDM is een tool voor gedistribueerd bestandsbeheer. SNADS is een netwerkservice voor de distributie van objecten over het netwerk.

De Alert Facility is een toepassing van de IBM Open Network Architecture (ONA), waarmee ook niet-SNA-elementen in het netwerk kunnen worden beheerd. Dit vindt plaats door het definiëren van de systemen als een focal point (de master), een entry point (de slave) of een service point (de poort naar heterogene netwerken). Tussen deze punten wordt netwerkbeheer-informatie en beveiligingsinformatie uitgewisseld via 'alert messages'. De Alert Facility is alleen mogelijk in combinatie met APPN, omdat het gebruik maakt van de APPN-routes.

De 3X/400-netwerkservices van Netview bieden een beperkte subset van Netview-functionaliteiten, namelijk alleen die op het gebied van het configuratie-, problem en change management.
De reden daarvoor is dat SNA de midrangesystemen niet als volwaardige subarea nodes (met een SSCP op een PU5-mainframe) ziet. Ze zijn ook niet uitgerust met alle functies die nodig zijn voor het besturen van een SSCP(PU5)-subarea node. De verbinding tussen SNA en APPC/APPN-netwerken loopt daarom vooralsnog over SNA-subarea-netwerken.

De 3X/400-netwerkservices van SystemView
De SystemView-functionaliteiten voor de AS/400 zijn geïmplementeerd in System Manager/400 en in de System Management Tools (SMT). Hiermee kan gecentraliseerd netwerkmanagement plaatsvinden vanuit één centrale AS/400. Alle parameters en objecten die te maken hebben met het netwerk worden op één centraal systeem opgeslagen en vanuit dit systeem beheerd.

Hoewel de system management tools een verbetering vormen ten opzichte van de basis-3X/400-netwerkservices, is er zowel bij NMA als bij SystemView sprake van netwerkbesturing vanuit een centraal systeem. Hiermee ontstaat een 'single point of failure', hetgeen het grootste nadeel is van een hiërarchisch netwerk zoals SNA.

PC Support (PCS)
Los van de AS/400-netwerkservices van SNA staat PC Support (PCS), een AS/400-datacommunicatiepakket voor onder andere terminal-emulatie, up- en download van bestanden tussen een PC(-LAN) en een AS/400.

Het configureren van de AS/400 voor netwerkgebruik

Bij het configureren van de AS/400 voor netwerkgebruik zijn de inhoud en de beschrijving van de AS/400-communicatie-objecten sterk afhankelijk van de kenmerken van de fysieke netwerkcomponenten. De beschrijving van een Token-Ring-lijn of -controller verschilt wezenlijk van die van een SDLC-lijn of -controller, evenals van die van een APPC-controller en een SNA-host controller.

Slechts een deel van de kenmerken van de AS/400-communicatie-objecten blijft constant ongeacht de fysieke netwerkcomponenten. Dit zijn de parameters voor object-, systeem- en netwerkidentificatie. In een AS/400-netwerkconfiguratie moeten deze parameters naar elkaar verwijzen als volgt. Ten eerste moeten de volgende definities van AS/400-datacommunicatie-objecten naar elkaar verwijzen:
- de lokale mode description en de remote device description;
- de remote device description en de remote controller description;
- de remote controller description en de remote line description.

Ten tweede moeten er verbanden worden gelegd tussen de lokale en de remote id's van communicatie-objecten van de aangesloten AS/400's. Namen en andere identificatieparameters van de communicatie-objecten van het remote systeem, waaraan het lokale systeem is gekoppeld, moeten als lokaal te boek staan op het remote systeem, en omgekeerd.

Nadat de communicatie-objecten, netwerkattributen en -services zijn gedefinieerd, moet de netwerkconfiguratie worden opgestart, ofwel 'varied on'. Dit kan met het commando Vary Configuration (*ON/*OFF). De nieuwe configuratie wordt geldig bij de eerstvolgende IPL (Initial Program Load) van het systeem.

Gebruik van de AS/400-netwerkservices

Het activeren van de AS/400-netwerkservices gebeurt via de AS/400-systeemparameters en -netwerkattributen. Dit zijn de systeemparameter Remote Sign-on Control (QRMTSIGN) voor DSPT, alsmede de netwerkattributen: Job Action (JOBACN) voor SNADS, DDM Access (DDMACC) voor DDM en PC Support Access (PCSACC) voor PC Support.

Om de bovenstaande services te kunnen gebruiken, moeten de genoemde attributen een andere waarde hebben dan *REJECT. Met *REJECT wordt de toegang tot de desbetreffende netwerkservice geweigerd.

Om de Alert Facility te kunnen gebruiken, moet het netwerkattribuut Alert Status aanstaan: ALRSTS (*ON), en moet het systeem 'APPN-capable' zijn: APPN(*YES).

Om van een service gebruik te kunnen maken, moet de netwerkconfiguratie zijn geïnitialiseerd ('varied on') en moet elke service worden gekoppeld aan een bestaand *subsysteem*. Dit kan door een *communications entry*.[3]

Een 'subsysteem' is een voorgedefinieerde werkomgeving die tot doel heeft de verschillende gebruikersactiviteiten in het systeem te scheiden. In de AS/400 zijn standaard-subsystemen aanwezig voor onder meer:
- interactieve jobs (QINTER);
- batch jobs (QBATCH);
- printtaken (QSPL);
- datacommunicatie (QCMN).

In een subsysteem worden 'subsystem entries' gedefinieerd voor de jobs die van het subsysteem gebruik maken. Per subsystem entry zijn de devices en de modes aangegeven die door een job worden gebruikt.

Subsystemen worden geactiveerd tijdens het IPL'en van de AS/400. DDM en PC Support maken initieel gebruik van het standaard AS/400-communications subsystem QCMN. SNADS maakt gebruik van het standaard QSNADS-subsysteem. De gebruiker kan zelf andere dan deze standaard AS/400-subsystemen definiëren.

Afsluiting

In deel 1 van dit artikel is gepoogd inzicht te verstrekken in de achtergronden van de AS/400-networking. Achtereenvolgens zijn de volgende onderwerpen de revue gepasseerd: het OS/400-besturingssysteem, de IBM-netwerkarchitecturen en de implementatie daarvan in de AS/400, de AS/400-netwerkservices, de AS/400-netwerkparameters en -datacommunicatie-objecten, alsmede het configureren van de AS/400 voor aansluiting in een netwerk en voor het gebruik van de AS/400-netwerkservices.

DEEL 2: DE AS/400-NETWERKSERVICES

In deel 2 zullen de afzonderlijke AS/400-netwerkservices worden besproken in termen van functionaliteit, beveiligingsrisico's en -maatregelen. De volgende services zullen de revue passeren:
- APPC/APPN;
- Display Station Pass-Through (DSPT);
- SNA Distribution Services (SNADS);
- Distributed Data Management (DDM);
- het PC-AS/400-datacommunicatiepakket PC Support.

APPC/APPN

De APPC/APPN-beveiliging wordt met twee *security levels* geïmplementeerd.

Functionaliteit en beveiliging
De APPC/APPN-beveiliging bestaat uit 'session level security' en 'conversation level security'.

Een *sessie* is de LU/LU-verbinding die tussen twee systemen bij datacommunicatie moet worden opgezet. Er kunnen tussen dezelfde LU's meerdere parallelle sessies tegelijk plaatsvinden.

Een *conversatie* is een tijdelijke verbinding tussen twee programma's tijdens een sessie. Binnen één sessie kunnen meerdere conversaties serieel (achter elkaar) plaatsvinden.

De *session level security* wordt gerealiseerd door het instellen van een Location Password (LOCPWD)-parameter. Het location password is vooral van belang voor de beveiliging van X.25-netwerken en van 'switched' communicatielijnen, omdat deze normaliter openstaan voor dial-up-toegang vanuit allerlei systemen.

De *conversation level security* komt tot stand door een 'secure location (*YES/*NO)' te definiëren.
Wanneer secure location(*YES) is gedefinieerd, betekent dit dat de lokale en remote systemen elkaar vertrouwen. Ze volstaan dan met het verzenden van de user-id. In plaats van het password wordt een code verzonden die aangeeft dat het password al is gecontroleerd. Deze code is de AVI (Already Verified Identifier). Dit heeft tot gevolg dat de lokale gebruikers op het remote systeem mogen werken onder het gezamenlijke gebruikersprofiel van een 'default user'.
De default user is een standaardinstelling voor de work entries van een (communicatie-)subsysteem. Het aanloggen als default user heeft tot gevolg dat gebruikersactiviteiten niet meer individueel kunnen worden gevolgd.

In APPC worden de Location Password- en Secure Location-parameters vastgelegd in de APPC-device description. In APPN worden deze parameters per remote systeem in de APPN-configuration list gedefinieerd.

De 'session level security' en 'conversation level security' hebben betrekking op het remote systeem.

3. Een 'communications entry' is een subsystem entry die bestemd is voor datacommunicatie, te definiëren in het desbetreffende subsysteem.

De controle van beide soorten beveiliging vindt plaats op het lokale systeem. Eerst wordt de session level security gecontroleerd, en daarna de conversation level security.

Bij bepaalde uitkomsten van beide controles mogen user-id's en passwords over de lijn naar het remote systeem worden verzonden. Dan is er sprake van een 'secure bind', hetgeen tevens inhoudt dat de 'session level security' geactiveerd is.
Een *bind* is het statement waarmee een sessie wordt opgezet. Er is sprake van een 'secure bind', wanneer de location passwords van zowel de lokale als de remote machine ingesteld zijn en dezelfde waarde hebben en het AS/400-beveiligingsniveau hoger is dan 10.
Dit maakt de sessie nog niet veilig omdat dan de machine-passwords wel afzonderlijk gecontroleerd worden op elke lokatie (en bij ongelijke waarde op de remote machine access wordt geweigerd) maar ten behoeve van deze controle onversleuteld over de lijn gaan, met het risico dat ze kunnen worden afgeluisterd. Een dergelijke 'secure bind' resulteert in een schijnbaar in plaats van feitelijk veilige toegangscontrole.

Wanneer de conversation level security actief is, worden eveneens user-id's en (onversleutelde) passwords over de lijn verzonden. Dit vindt plaats wanneer Secure Location (SECURELOC(*NO)) is gedefinieerd, of wanneer batch jobs, voorzien van de user-id's en passwords van de eigenaren, door applicaties worden verzonden.

Beveiligingsrisico's

1 Het ten onrechte definiëren van de AS/400-site als 'secure location': SECURELOC(*YES), omdat dan de passwords van de remote gebruikers lokaal niet worden gecontroleerd.
2 Passwords worden onversleuteld over de lijn verzonden.
3 Gebruik van generieke gebruikersprofielen: DFTUSR(*QUSER).
4 Gebruik van generieke modes en devices in de subsystem communications entries: MODE(*ANY) en DEVICE(*ANY).
5 Geen beveiliging van de AS/400-communicatie-objecten en -commando's, zoals Create/Change/Delete/Work met:
   – Line/Controller/Device/Mode Description (en de variaties daarvan per soort lijn, controller of device);
   – APPN Configuration List (Local/Remote).

Beveiligingsmaatregelen

1a SECURELOC(*NO) en location passwords voor de remote gebruikers;
1b Identieke gebruikersprofielen, user-id's en passwords op de lokale en remote systemen.
2 V3.R1 van OS/400 en Enhanced Security (*SAME) op de lokale en remote systemen.
3 Gebruik van specifieke gebruikersprofielen met beperkte bevoegdheden en DFTUSR(*NONE).
4 Specifieke verwijzing naar modes en devices in de subsystem communications entries: MODE(-naam) en DEVICE(-naam).
5 PUBLIC(*EXCLUDE) of (*USE) voor de AS/400-communicatie-objecten en commando's.

Kader 1. Beveiligingsrisico's en -maatregelen bij APPC/APPN.

Protected password
Wanneer user-id's en passwords over de lijn worden verzonden, zijn de passwords onversleuteld wanneer OS/400-versies ouder dan versie 3 en/of PC Support worden gebruikt. In OS/400 versie 3 worden passwords tijdens de verzending vervangen door een versleuteld 'protected password'. Dit is een functie van de Enhanced Security(*SAME)-faciliteit.
Om met een protected password op het remote systeem aan te loggen, moet op het remote systeem een gebruikersprofiel met een zelfde user-id en password bestaan. Daarnaast moet zowel het lokale als het remote systeem Enhanced Security(*SAME) ondersteunen. Indien dit bij een van beide systemen niet het geval is, worden de passwords alsnog in clear text over de lijn verzonden.

Beveiligingsrisico's en -maatregelen
De beveiligingsrisico's en -maatregelen bij APPC/APPN zijn afgebeeld in kader 1.

Display Station Pass-Through

De beveiliging van Display Station Pass-Through (DSPT) wordt met *virtual devices* en 'remote' parameterdefinities gerealiseerd.

Functionaliteit en beveiliging
Met DSPT kan vanuit een lokaal systeem op een remote systeem worden aangelogd en toegang worden verkregen tot programma's en gegevens op het remote systeem. Simultane sessies met meerdere systemen tegelijk zijn niet mogelijk.

DSPT maakt gebruik van *virtual devices*. Dit zijn emulaties van fysieke devices (bijvoorbeeld een virtuele versie van een IBM-terminal van een bepaald model). Met behulp van virtual devices stuurt het remote systeem de output naar de fysieke devices van het lokale systeem.
Virtual devices worden automatisch aangemaakt door het remote systeem op het moment dat het lokale systeem om toegang vraagt. Dit is alleen mogelijk als de waarde van systeemparameter Automatic Configuration of Virtual Devices (QAUTVRT) groter is dan de standaardwaarde 0.
De eenmaal gecreëerde virtual devices kunnen niet weer automatisch worden verwijderd. Dit moet handmatig gebeuren.

Om DSPT te kunnen gebruiken, moet de systeemparameter Remote Sign-on Control (QRMTSIGN) op de lokale en remote machines ongelijk zijn aan *REJECT. Daarnaast moet bij het opstarten van DSPT op de lokale machine een remote gebruikersprofiel worden opgegeven. Wanneer voor dit profiel geen user-id is gedefinieerd (RMTUSER (*NONE)), gelden alleen de instellingen van de remote sign-on parameter.
Een gebruiker kan op het remote systeem aanloggen op twee manieren:
– onder hetzelfde gebruikersprofiel als op het lokale systeem, met RMTUSER(*CURRENT);
– onder een ander gebruikersprofiel, met RMTUSER(-profielnaam).

Als onder een ander gebruikersprofiel wordt aangelogd, wordt dit gesignaleerd wanneer de Remote Sign-on-parameter is ingesteld op QRMTSIGN (*SAMEPRF, 'same profile').

Om de route naar het remote systeem te bepalen, moeten op het lokale systeem minimaal een 'local location name', 'remote location name' en 'remote network identifier' worden gedefinieerd.
Wanneer geen gebruik wordt gemaakt van APPN, moet worden aangegeven dat de route via een non-networking APPC-device verloopt, het 'connection device'. Dit wordt opgegeven met de remote location name-parameter (RMTLOCNAME (*CNNDEV)).
Bij gebruik van APPN moet aanvullend ook een mode worden gedefinieerd.

Voor de DSPT-gebruikers moeten op de lokale machine behalve de remote user-id ook het 'remote password', 'initial program' en 'initial menu' worden gedefinieerd. Het remote initial program en menu zijn nodig om remote applicaties op te kunnen starten.

Door voor het remote initial menu *SIGNOFF te definiëren, kan ervoor worden gezorgd dat de gebruiker na beëindiging van de applicatie automatisch aflogt.

DSPT kan worden geconfigureerd en opgestart met het commando Start Pass-Through. Tijdens een remote sessie kan tijdelijk worden teruggeschakeld naar het lokale systeem met Transfer Pass-Through.
De DSPT-sessie moet na *SIGNOFF met het commando End Pass-Through definitief worden beëindigd. Het zich beperken tot *SIGNOFF sluit alleen de conversatie, niet de sessie.

Beveiligingsrisico's en -maatregelen
De beveiligingsrisico's en -maatregelen bij DSPT zijn afgebeeld in kader 2.

Beveiligingsrisico's

1 Het is mogelijk zonder geldig password op het remote systeem aan te loggen, indien:
   - SECURELOC(*YES) is ingesteld, in combinatie met:
   - de waarden *VERIFY of *SAMEPRF (Same Profile) voor de Remote Sign-on Control (QRMTSIGN)-parameter, en
   - de Remote User (RMTUSER)-parameter tevens de waarde *CURRENT heeft.
2 DFTUSR(*QUSER): als bij APPC/APPN.
3 Bij het interactief beëindigen van DSPT met het SIGNOFF-commando wordt alleen de conversatie beëindigd, maar niet de DSPT-sessie.
4 Bij het automatisch configureren van virtual devices (QAUTVRT>0):
   - wordt het totale aantal toegestane aanlogpogingen vermenigvuldigd met het aantal automatisch te configureren virtual devices: QMAXSIGN x QAUTVRT;
   - worden bij een combinatie van QAUTVRT>0 met Limit Security Officer (QLMTSECOFR)=0 de bevoegdheden van de security officer of van elke andere gebruiker die over de *ALLOBJ- of *SERVICE-speciale bevoegdheden beschikt, niet beperkt tot de voor hem toegestane devices op het remote systeem.
5 Het toekennen van default systeemnamen aan de automatisch geconfigureerde virtual devices en controllers, welke in de AS/400-handboeken zijn gepubliceerd (QPADEVnnnn en QPACTLnn voor respectievelijk de device en de controller, waarbij nnnn = volgnummer).
6 Geen beveiliging van de DSPT-objecten en commando's, waaronder ook de commando's voor het handmatig aanmaken van virtual devices en controllers, namelijk:
   - Create Controller Description Virtual Workstation;
   - Create Device Description Display Device Class (Virtual).

Beveiligingsmaatregelen

1 SECURELOC(*NO) in combinatie met QRMTSIGN(*FRCSIGNON), of een toegangsvalidatieprogramma voor deze parameter.
2 DFTUSR(*NONE).
3 DSPT afsluiten met End Pass-Through of *SIGNOFF DROP(*YES).
4 QAUTVRT(0) en QLMTSECOFR(1) instellen (na het configureren van het systeem en het netwerk).
5 Wijzigen van de standaardnamen van devices en controllers in zelf gedefinieerde namen.
6 PUBLIC(*EXCLUDE) voor de genoemde commando's, alsmede voor de gecreëerde virtual devices en controllers.

Kader 2. Beveiligingsrisico's en -maatregelen bij DSPT.

SNA Distribution Services

SNA Distribution Services (SNADS) is een service die het verzenden van objecten (berichten, jobs, programmatuur of gegevens) over het netwerk verzorgt.

Functionaliteit en beveiliging
De distributie vindt plaats naar aanleiding van aanvragen die *originating agents* (clients) bij *receiving agents* (servers) plaatsen. SNADS werkt volgens het *store-and-forward*-principe. Als een bericht niet direct kan worden verzonden, komt het in een wachtrij en wacht daar totdat verzending mogelijk is.
De verzending wordt afgehandeld door *router*- en *sender*-processen. De wachtrijen worden op de *distributiepunten* (de DSU, of Distribution Service Unit) afgehandeld door een queue manager.

De communicatie tussen de verschillende services vindt plaats via *protocol boundaries*. Ze definiëren de functies die een SNADS-component levert, alsmede de functies die naar verwachting aan de andere kant aanwezig zijn. Zo worden protocol boundaries onderscheiden tussen DSU-agents, DSU-servers, DSU-queue managers en DSU-LU6.2, die de feitelijke verzending verzorgen.
SNADS maakt geen gebruik van definities van SNA-nodes en -routes, maar van eigen componenten. Zo worden de adressen van agenten door de DSU in een directory geplaatst en de routing-informatie in een *routing table*. Elke DSU houdt zijn eigen informatie bij. Daarnaast zijn er ook knooppunt-DSU's, die als systeem-administrators fungeren en de directories en routing tables van alle DSU's in het netwerk bijhouden.

Om SNADS te kunnen gebruiken, moet het systeem 'APPN-capable' zijn en moet het AS/400-netwerkattribuut Job Action (JOBACN) een andere waarde hebben dan *REJECT.
Ten behoeve van SNADS moeten op de AS/400,

naast het SNADS-subsysteem en de communications entries van de aangesloten remote systemen, SNADS-specifieke objecten worden aangemaakt. Dit zijn:
- de distribution queue;
- de system distribution directory;
- de routing table;
- (eventueel) een secondary system name table met alternatieve systeemnamen.

Per gebruiker moet in de *system distribution directory* een *directory entry* worden gedefinieerd, waarin de user-id en het adres van de gebruiker moeten worden aangegeven. Ze vormen samen een identifier die uniek moet zijn in het netwerk.

Als een gebruiker als *indirect user* is gedefinieerd, kan hij objecten ontvangen zonder aan te hoeven loggen. De indirect user-optie wordt gebruikt om een ontvanger aan te wijzen. Zo'n ontvanger kan bijvoorbeeld een gebruikersprofiel-eigenaar zijn van een applicatie die batch jobs moet kunnen ontvangen.

Voor de afhandeling van de verzendingen moet op het lokale systeem één directory entry bestaan voor het gebruikersprofiel dat objecten verzendt. Op het remote systeem moet één directory entry bestaan voor het gebruikersprofiel dat ontvangt.

Tevens moet op het lokale systeem een *recipient*-gebruikersprofiel worden gedefinieerd voor de ontvangst van de zendingen vanuit het remote systeem. Op het remote systeem dient ten slotte een *originator*-gebruikersprofiel van de gebruiker-eigenaar van de verzonden objecten te worden gedefinieerd.

Kader 3. Beveiligingsrisico's en -maatregelen bij SNADS.

Beveiligingsrisico's
1 SECURELOC(*YES): als bij APPC/APPN.
2 DFTUSR(*QUSER): als bij APPC/APPN.
3 Bij de waarde *FILE of *SUBMIT van de Job Action (JOBACN)-systeemparameter kunnen ook niet-geautoriseerde remote jobs op het lokale systeem worden binnengelaten.
4 *ANY-global entries in de SNADS-directories, waardoor individuele verzenders en ontvangers niet meer kunnen worden geïdentificeerd.
5 Geen beveiliging van de SNADS-objecten en commando's.

Beveiligingsmaatregelen
1 SECURELOC(*NO).
2 DFTUSR(*NONE).
3a Het definiëren van een *network job table* en het toelaten van alleen de remote jobs die daarin zijn gespecificeerd; dit kan met JOBACN(*SEARCH);
3b Jobs van niet-geïdentificeerde gebruikers vanuit niet-geïdentificeerde systemen weigeren; dit wordt bewerkstelligd door in de network job table een entry te definiëren voor de user *ANY met adres *ANY met JOBACN(*REJECT).
4 In de SNADS-directories voor elke (geautoriseerde) gebruiker een user-id en adres definiëren.
5 PUBLIC(*EXCLUDE) voor de SNADS-objecten en commando's.

In een directory entry kan in plaats van de individuele user-id de waarde *ANY worden gedefinieerd. Dan wordt de entry een 'global entry' voor alle SNADS-gebruikers, waardoor individuele verzenders en ontvangers niet meer kunnen worden geïdentificeerd.
In de *system distribution directory* zijn ook default directory entries aanwezig. Deze entries worden gebruikt door systeemtaken en mogen niet worden gewijzigd.

SNADS heeft een eigen *logging*, waarin het verloop van de objectdistributie wordt vastgelegd. Deze logging maakt gebruik van het standaard-systeemjournaal QSNADSJRN. De SNADS-logging kan worden bekeken met het Display Distribution Log-commando.

Beveiligingsrisico's en -maatregelen
De beveiligingsrisico's en -maatregelen bij SNADS zijn afgebeeld in kader 3.

Distributed Data Management

Voor bestandsbeheer over netwerken wordt Distributed Data Management (DDM) gebruikt.

Functionaliteit en beveiliging
DDM is de IBM-architectuur voor gezamenlijke data management interfaces ten behoeve van de gegevensuitwisseling tussen homogene (bijvoorbeeld alleen mainframes of midranges) en heterogene (mainframe-midrange) (IBM-)systemen.

In feite is DDM een middel voor gedistribueerd bestandsbeheer. Dit beheer vindt plaats op fileniveau. Gegevens kunnen worden benaderd tot op record-niveau. Benadering van de afzonderlijke velden van een record is niet mogelijk.

Het is ook niet mogelijk de operaties op files op het remote systeem uit te voeren en alleen de uitkomsten naar het lokale systeem te transporteren ('set-at-a-time processing'). Voor elke operatie (add, update, delete) moeten de applicatieprogramma's afzonderlijke I/O-requests naar het remote systeem sturen. Dit zorgt voor veel overhead en heeft een nadelige invloed op de performance.
Read-only set-at-a-time I/O-requests zijn wel mogelijk met het commando Open Query File (OPNQRYF) van Query/400 (de AS/400-databasetaal).

DDM heeft een eigen expliciete *commit protocol*. Ten opzichte van het 'echte' gedistribueerde protocol ('two-phase commit', of 2PC) heeft het DDM-protocol de volgende beperkingen:
- commitment control kan niet worden gebruikt indien de lokale database-file en de (lokale) DDM-file tegelijk zijn geopend;
- wanneer meerdere remote files tegelijk zijn geopend, moeten deze files zich op hetzelfde remote systeem bevinden en door dezelfde applicatie zijn geopend;
- de transacties van alle remote files, geopend door een bepaalde applicatie onder commit-

ment control, moeten worden vastgelegd in hetzelfde journal;
- het remote systeem voor DDM-files onder commitment control moet een andere AS/400 zijn;
- bij een communicatiestoring tijdens een commit-operatie wordt zowel op het lokale als op het remote systeem een roll-back uitgevoerd. Deze roll-backs zijn echter niet gesynchroniseerd. Wanneer het remote systeem net vóór de storing een commit heeft afgerond, zal het lokale systeem alsnog een roll-back uitvoeren.

De DDM-implementatie op de AS/400 is een integraal deel van het besturingssysteem. Om DDM te kunnen gebruiken, moet het netwerkattribuut DDM Access (DDMACC) zowel op de lokale als op de remote machine een andere waarde hebben dan *REJECT.
Bij het benaderen van remote files door lokale applicaties met behulp van DDM is de plaats van de bestanden transparant voor de applicatie. De identificatie van een bestand op het remote systeem en van het pad naar dit bestand vindt plaats met behulp van *DDM-files*. DDM-files zijn een soort pointers die naar de remote files verwijzen. De lokale applicatie ziet dan de remote file als een lokale file. DDM-files moeten op het lokale systeem worden aangemaakt (met het Create DDM-file commando). Voor elke remote file die men wil benaderen, moet een DDM-file bestaan.

DDM benadert remote files met het commando Submit Remote Command (SBMRMTCMD). Met behulp daarvan kunnen AS/400-commando's naar het remote systeem worden gestuurd. De primaire functie van Submit Remote Command is bestandsbeheer ten behoeve van DDM. Dit commando kan echter ook worden gebruikt om allerlei andere commando's op te sturen die niets met DDM te maken hebben. Dit is mogelijk zolang geen beeldschermuitvoer geproduceerd hoeft te worden. Daarnaast moet de DDM-gebruiker beschikken over bevoegdheden op het lokale systeem tot het Submit Remote Command en tot de commando's die daarmee moeten worden verzonden, alsmede over bevoegdheden om files op het remote systeem te benaderen.

De interactie tussen de lokale en remote systemen gebeurt aan de hand van een *DDM-conversatie* (binnen een LU/LU-sessie). In de mode description van de DDM-sessie worden sessie-eigenschappen vastgelegd, zoals het maximum aantal sessies en het maximum aantal conversaties binnen een sessie.
Een DDM-conversatie heeft drie statussen: actief (*ACTIVE), niet gebruikt (*KEEP) en beëindigd (*DROP).
De status *KEEP wordt gebruikt bij transactie-intensieve toepassingen, om te voorkomen dat per transactie telkens weer een nieuwe conversatie moet worden geopend.
Om DDM te kunnen gebruiken, moeten minstens twee DDM-jobs worden geopend: een job op het lokale systeem en een job op het remote systeem. Voor elke lokale DDM-job moet een aparte DDM-conversatie worden opgestart met de remote DDM-job. Wanneer meerdere DDM-files vanuit een lokale DDM-job dezelfde remote locatie benaderen, wordt de conversatie door de actieve files gedeeld.

Beveiligingsrisico's
1 SECURELOC(*YES): als bij APPC/APPN.
2 DFTUSR(*QUSER): als bij APPC/APPN.
3 De default-waarde *OBJAUT van de DDM Access-parameter (DDMACC) houdt in dat de DDM-verzoeken worden afgehandeld volgens de object-bevoegdheden van de DDM-gebruiker voor het remote systeem.
4 Het geven van AS/400-commando's op het remote systeem met behulp van het Submit Remote Command (SBMRMTCMD).
5 Bij een DDM-conversatie met status *KEEP:
   - geldt bij 'shared' conversaties dezelfde security check voor de verschillende soorten transacties binnen één conversatie;
   - vindt geen controle plaats van de user-id en het password van de applicatie of de gebruiker wanneer de conversatie door een andere applicatie (transactie) opnieuw wordt gebruikt.
6 Onvoldoende beveiliging van DDM-files op het lokale systeem.

Beveiligingsmaatregelen
1 SECURELOC(*NO).
2 DFTUSR(*NONE).
3 De gebruikersbevoegdheden op het remote systeem beperken en een toegangsvalidatieprogramma definiëren voor de DDMACC-parameter.
4 Het Submit Remote Command (SBMRMTCMD) beveiligen met PUBLIC(*EXCLUDE).
5a Risicovolle DDM-applicaties ook op het lokale systeem beveiligen;
5b Risicovolle DDM-applicaties niet binnen shared conversaties (met status *KEEP) opstarten.
6 Lokale DDM-files ook op het remote systeem beveiligen.

Kader 4. Beveiligingsrisico's en -maatregelen bij DDM.

Beveiligingsrisico's en -maatregelen
De beveiligingsrisico's en -maatregelen bij DDM zijn afgebeeld in kader 4.

PC Support

Met PC Support (PCS) is het mogelijk PC-gebruikers aan AS/400's te koppelen.

Functionaliteit
Met PC Support (vanaf OS/400 V3.R1 Client Access/400 genoemd) kunnen PC-gebruikers beschikken over AS/400-resources en -functies. PC Support biedt niet alleen eenvoudige terminal-emulaties, maar ook andere connectivity-functies tussen de PC en de AS/400, zoals:
- het up- en downloaden van bestanden tussen de PC en de AS/400;
- het opslaan van PC-bestanden op de AS/400 (in directories 'shared folders' genaamd);
- het geven van AS/400- en SQL-commando's vanuit de PC naar de AS/400 (met behulp van de Remote Command- en Remote SQL-functies);
- het aansturen van PC-printers door de AS/400 en omgekeerd;
- functies voor systeembeheer en inrichting van gebruikersomgevingen.

Beveiligingsrisico's

1 Passwords worden altijd onversleuteld naar de AS/400 verzonden, omdat de Enhanced Security(*SAME)-facility onder PC Support niet werkt.
2 Geen expiratie van het PCS-password in de oudere OS/400-versies, omdat de AS/400-systeemparameters PWDEXPITV, Password Expiration Interval, en PWDEXP, Set Password to Expired, niet werken.
3 In PC Support bestaat de mogelijkheid een eenmaal ingetypt password in clear text op te slaan in een ASCII-bestand op de PC en dit bij de volgende sessie op te roepen, zodat het opgeven van user-id's en passwords niet meer nodig is. Dit is mogelijk dankzij de 'pipeline facility' van het Start Router (STARTRTR)-commando van PC Support.
4 Indien er in PC Support een common user-id is gedefinieerd, worden de individuele user-id's niet meer gecheckt.
5 Indien in het PCS-subsysteem op de AS/400 een default user aanwezig is (DFTUSER(*USER)), kunnen ongeautoriseerde gebruikers in PC Support aanloggen.
6a Bij de (default) waarde *OBJAUT van het AS/400-netwerkattribuut PC Access (PCSACC) wordt de gebruiker tot PC Support toegelaten op basis van zijn bevoegdheden tot de PC Support-functies, terwijl zijn AS/400-objectbevoegdheden niet worden gecontroleerd;
6b Bij PCSACC(*REJECT) wordt de gebruiker niet toegelaten tot de AS/400, maar wel tot PC Support, zonder controle van user-id en password.
7 Met de Remote Command-functie van PC Support, identiek aan het AS/400-commando Submit Remote Command (SBMRMTCMD), kunnen vanuit de DOS-shell AS/400-commando's worden gegeven.
8 Binnen een PCS-sessie kunnen meerdere jobs en meerdere conversaties tussen de PC en de AS/400 plaatsvinden, zonder dat er opnieuw een user-id en password hoeven te worden aangegeven. Op die manier kunnen ook risicovolle applicaties zonder toegangscontrole binnen dezelfde sessie worden opgestart.
9 Inactieve werkstations, waar andere PCS-functies dan de PC Organizer (PCO) of de Work Station Function (WSF) zijn opgestart, worden niet afgelogd, ongeacht de ingestelde waarde voor de systeemparameter Inactive Job Time-Out Interval (QINACTITV).
10 Optie 1 (werkstation blokkeren) van de AS/400-systeemparameter Action When Maximum Sign-On Attempts Reached (QMAXSIGNACN) werkt niet samen met PC Support, omdat deze parameter geen invloed heeft op de LU/LU-sessie tussen de PCS-router en de AS/400.
11 De AS/400-systeemparameter Limit Device Sessions (LMTDEVSSN) werkt niet bij PC Support. Dit houdt in dat de PCS-gebruikers vanuit meerdere werkstations met dezelfde user-id en password in PC Support kunnen aanloggen.
12 De Limit Capabilities (LMTCPB)-parameter van het AS/400-gebruikersprofiel, waarmee het geven van systeemcommando's wordt afgeschermd, geldt niet voor de PCS Organizer (PCO)-functie, waarmee onder meer AS/400-systeemtaken kunnen worden uitgevoerd.
13 Voor bestanden en berichten, ge-download vanuit de AS/400 naar de PC of geplaatst in shared folders op de AS/400, geldt alleen de PC-beveiliging.
14 Geen beveiliging van de PC Support-programmatuur op de PC's.

Kader 5. Beveiligingsrisico's PCS.

De PC/AS/400-verbinding is op twee manieren mogelijk:
- de gewone terminal-emulatie, waarbij de PC als 'domme' terminal fungeert (en derhalve geen gebruik kan maken van de 'intelligente' PC Support-functies);
- verbindingen waarbij naast de terminal-emulatie ook de overige PC Support-functies actief zijn.

In alle gevallen vindt de communicatie tussen PC en AS/400 plaats via APPC/LU6.2.

PC Support en AS/400

PC Support kan worden geïnstalleerd vanuit de AS/400 of vanuit de PC. Per gebruiker moet worden aangegeven welke PCS-functies deze mag gebruiken. Ook moeten de communicatielijnen naar de AS/400 worden gedefinieerd.

Ten slotte moeten de gebruikersprofielen van de PCS-gebruikers worden aangemaakt. Dit wordt bewerkstelligd door de PCS Administration Function. Net als in de AS/400 kan de gebruiker worden gekoppeld aan een groepsprofiel (de 'model configuration'), of kan voor elke gebruiker een individueel profiel worden aangemaakt (de 'user configuration'). De identificatiekenmerken van het PCS-gebruikersprofiel bestaan uit user-id, password en netwerkadres van de gebruiker.

Voor de PCS Administration Function (PCSADM) moet de gebruiker beschikken over de Security Administrator (*SECADM)-speciale bevoegdheid op de AS/400. Gebruikers die op de AS/400 over deze bevoegdheid beschikken, krijgen automatisch toegang tot de PCSADM-functie. Alleen iemand met de *SECADM-bevoegdheid kan een PCS-administrator aanwijzen.

PCS-beheerfuncties

Via de PCS-administratiefunctie PCSADM kan worden aangegeven of de gebruiker zijn eigen PCS-configuratie mag wijzigen of dat deze configuratie centraal wordt geadministreerd. In dit laatste geval worden alle door de gebruiker ingebrachte wijzigingen ongedaan gemaakt bij de volgende PCS-sessie. PCSADM is daarom een goed beheersingsmiddel.

PC Support beschikt ook over een update-functie, die constant de PC Support-versies op de PC en op de AS/400 op elkaar afstemt. De update-functie is een goed middel voor versiebeheer.

Toegangsbeveiliging

De toegang tot PC Support wordt verleend aan de hand van een common user-id, een specifieke user-id en een password. De common user-id verleent toegang tot alle PCS-functies. De specifieke user-id verleent toegang tot geselecteerde PCS-functies.

Bij het opstarten van PC Support wordt eerst naar de common user-id gevraagd. Wanneer in PC Support al een common user-id is gedefinieerd (in de configuratie file CONFIG.PCS), wordt niet meer naar de specifieke user-id maar direct naar het password gevraagd.

Wanneer geen common user-id is gedefinieerd, wordt er gevraagd naar de specifieke user-id en naar het password van de gebruiker. Wanneer deze niet worden verstrekt, wordt gekeken in de communications entry van het PC Support-subsysteem op de AS/400 (de QCMNE-default of een user-defined subsysteem) of er een default user bestaat. Bij de aanwezigheid van een default user kan de gebruiker alsnog in die hoedanigheid aanloggen.

Gegevensbeveiliging
De gegevens, opgeslagen op de AS/400 onder PC Support (zoals ge-uploade PC-files of AS/400-files), komen terecht in de PC Support-directories genaamd 'shared folders'. De daarin geplaatste objecten, alsmede de shared folders zelf, kunnen met AS/400-middelen worden beveiligd.
Bij het downloaden van gegevens van de AS/400 naar de PC geldt voor deze gegevens alleen de PC-beveiliging, en niet de AS/400-objectbeveiliging.

Beveiligingsrisico's en -maatregelen
De beveiligingsrisico's en -maatregelen bij PCS zijn afgebeeld in de kaders 5 en 6.

Afsluiting

In dit deel zijn de afzonderlijke AS/400-netwerk-services besproken in termen van functionaliteit, beveiligingsrisico's en -maatregelen.
In het laatste, derde deel zullen de auditmiddelen voor de AS/400 worden besproken, alsmede de aandachtsgebieden die van belang zijn voor de technische AS/400-audit.

DEEL 3: DE TECHNISCHE AS/400-AUDIT

De technische AS/400-audit is afhankelijk van de AS/400-mogelijkheden voor het verzamelen van auditinformatie (audit-trail), maar nog belangrijker is of de gebruikersorganisatie van al deze mogelijkheden gebruik maakt. De praktijk leert dat dit zelden het geval is.

De externe of interne auditor is afhankelijk van deze informatie. Indien de gebruikersorganisatie geen auditinformatie over het verleden heeft verzameld, is de waarde van de technische AS/400-audit letterlijk een momentopname van de stand van de AS/400-parameters. Zo'n opname is wel aardig, maar zeker onvoldoende, indien men aan de audit hogere eisen stelt dan louter de controle van de gebruikersbevoegdheden op het moment van onderzoek.

Helaas beperken veel auditors zich tot dit soort werkzaamheden. Ze laten zich verleiden tot korte-termijnbevindingen, die op een eenvoudige wijze door de gebruikersorganisatie kunnen worden verholpen, bijvoorbeeld het wijzigen van een aantal beveiligingsparameters naar de door de auditor aanbevolen waarden.
Daarna gaan auditor en gebruikersorganisatie tevreden naar huis, met de geruststelling dat de AS/400 veilig is. De vraag is of dit op lange termijn voldoet. Het doel van een AS/400-audit is immers de beheersbaarheid van de AS/400-gegevensverwerking! Daarvoor zijn zowel de inrichting en de efficiëntie van de machine (dus de wijze waarop de AS/400 wordt beheerd) als het gebruikersgedrag van belang. Om daar iets zinvols over te kunnen zeggen, moet over een langere periode auditinformatie worden verzameld.

Beveiligingsmaatregelen

1 Het AS/400-aanlogscherm overslaan. Dit kan door 'Bypass sign-on display: Yes' te definiëren in het WSF (Workstation Function)-profiel voor terminal-emulatie. Daarnaast moet voor de Remote Sign-on (QRMTSIGN)-parameter de waarde *VERIFY of een toegangsvalidatieprogramma worden ingesteld.
2 Hogere OS/400-versies gebruiken.
3 De 'pipeline facility' buiten gebruik stellen.
4 Geen common user-id in PC Support definiëren.
5 DFTUSR(*NONE) definiëren in het PCS-subsysteem op de AS/400.
6a AS/400-bevoegdheden voor de PC Support-gebruikers op de AS/400 definiëren;
6b AS/400-bevoegdheden tot de PC Support-objecten (zoals de QIWS*-folders met PCS-programmatuur en folders met gebruikersbestanden) op de AS/400 definiëren;
6c Een toegangsvalidatieprogramma voor PCSACC definiëren.
7a Het PCS-programma dat de Remote Command-functie op de PC uitvoert, te weten RMTCMD.EXE in de QIWS*-folders, op de AS/400 beveiligen;
7b Op de AS/400 het PCS-serverprogramma QCNTEDDM (in de QSYS-bibliotheek), dat de Remote Command-functie op de AS/400 uitvoert, beveiligen;
7c Voor Limit Capabilities (LMTCPB) de waarde *YES instellen om het gebruik van de PCS Remote Command-functie af te schermen.
8 Na afloop van de gebruikersjob moeten de sessie, de conversatie en de PC Support-router direct worden beëindigd (met het commando STOPRTR/F, 'force all to stop').
9 Dit risico organisatorisch opvangen.
10 Eén van de overige opties van QMAXSIGNACN instellen.
11 Als 9.
12 Voor de PCS Organizer (PCO)-functie in de Allow Limited User (ALWLMTUSR)-parameter de defaultwaarde *YES wijzigen naar *NO.
13a De shared folders en daarin geplaatste objecten op de AS/400 beveiligen;
13b De directories en bestanden op de PC beveiligen.
14 De PCS-programma's op de AS/400 (de zgn. 'serverprogramma's') beveiligen, omdat daarmee ook de desbetreffende PC Support-functies worden beveiligd.

Kader 6. Beveiligingsmaatregelen PCS.

Voor het verzamelen van dit soort informatie zijn er voor de AS/400 verschillende mogelijkheden. In de eerste plaats zijn dit de AS/400-logging en -journaling. Deze worden besproken in de volgende twee paragrafen. Daarnaast komen nog de veredeling van de auditinformatie en de audits van de netwerktopologie en -beveiliging aan de orde.

Logging

De AS/400-logging valt uiteen in systeem-logging en netwerk-logging.

Systeem-logging
De systeem-logging kan zijn:
- *security-logging*, vastgelegd in de history log-file QHST;
- andere logging, zoals job logging, operations logging, problem logging, transactie-logging, etc.

De *transactie-logging* is gericht op beheersing van het primaire gegevensverwerkende proces van de

organisatie. De overige soorten systeem-logging, alsmede de netwerk-logging, zijn bedoeld voor systeembeheer.

Netwerk-logging
De netwerk-logging wordt gegenereerd door het systeem of door de verschillende AS/400-netwerkservices (van Netview of van SystemView) en (netwerk-)management-tools.
De netwerk-logging gegenereerd door het *systeem* bestaat uit:
- de APPN-logging met informatie over de topologie, location directories en nodes in het APPN-netwerk (verkrijgbaar met het commando Display APPN Information, DSPAPPNINF);
- het Verify Communications-menu met informatie over het fysieke netwerk;
- de Communications Protocol Trace met logging-informatie over protocollen en fysieke lijnen (SDLC, Ethernet, Token-Ring, etc.);
- de Communication Applications Trace met logging van standaard AS/400-netwerk applicatie-interfaces CPI-C (Common Program Interface-Communications) en ICF (Interactive Command Facility).

De netwerk-logging gegenereerd door de verschillende AS/400-netwerkservices en (netwerk)-management-tools betreft:
- in Netview:
  - de alert-logging (van de Alert Facility);
  - de SNADS-logging;
- in SystemView:
  - de System Manager/400-logging;
  - de System Management Tools (SMT)-logging;
- in andere tools, bijvoorbeeld:
  - de AS/400 Performance Tools;
  - de System Administration Tools (SAT).

Tabel 2. Logging-informatie per AS/400-(netwerk)-management-tool.

	AS/400-(netwerk)management-tools		
Logging-informatie	SM/400	SMT	SAT
PTF	x		x
Alerts	x		x
Problems	x		x
Gebruikersprofielen		x	
Objectdistributie		x	x
Bibliotheekdistributie		x	x
Distributie van commando's		x	x
Job scheduling			x
Systeemparameters		x	
Netwerkattributen		x	
Error logging		x	
Resource management			x
Statistieken over systeemgebruik			x

In tabel 2 is de verzamelde informatie per AS/400-(netwerk)management-tool weergegeven.

Journaling

De AS/400-logging-informatie wordt gegenereerd in log-files, message queues of journals. Deze laatste methode wordt 'journaling' genoemd. Journals bestaan uit aparte bestanden, *'journal receivers'* genaamd. Elk gelogd gegeven vormt een *'journal entry'*, een record in de journal receiver.

Journal receivers hebben een bepaalde omvang, welke vooraf moet worden gedefinieerd. Als een receiver vol is, wordt deze losgekoppeld van het journal. Een nieuwe, lege receiver moet aan het journal worden gekoppeld, wil men doorgaan met de journaling. Daarom moet de AS/400 zodanig worden ingesteld, dat de verwisseling van journal receivers automatisch plaatsvindt. Als dit niet is geregeld, begint het systeem opnieuw aan het begin van de volle receiver te schrijven. Daarmee gaat de reeds gelogde informatie verloren.

De default AS/400-security loggimg wordt behalve in de QHST-history log-file ook in de security audit journal QAUDJRN gegenereerd. Om deze te kunnen gebruiken, moet eerst op systeemniveau de security audit functie worden geactiveerd met de Auditing Control (QAUDCTL)-parameter.

Daarnaast moet in de Auditing Level (QAUDLVL)-parameter worden aangegeven welke security-informatie zal worden gelogd. De mogelijkheden zijn onder andere:
- geen security audit logging;
- autorisatie-overtredingen;
- security-overtredingen;
- 'create'- en 'delete'-handelingen;
- wijziging van de ingestelde beveiliging tijdens 'save'-en 'restore'-procedures.

Per soort overtreding worden vaste journal entries verzameld. Een journal entry is vergelijkbaar met een recordtype en staat voor een bepaald soort overtreding.
Indien bijvoorbeeld de Autorisation Failures (*AUTFAIL)-waarde is ingesteld, dan worden gelogd:
- in de AF-journal entry (Authority Failure): het overschrijden van objectautorisaties;
- in de PW-journal entry (Password and User Profile): de pogingen om met een ongeldig password aan te loggen.

Daarnaast kunnen vanaf OS/400 V3.R1 zowel op systeemniveau als op gebruikersniveau de zogenaamde 'user action auditing' en 'object action auditing' worden ingesteld.
De *user action auditing* geeft aan welke security-overtredingen van de gebruiker worden gelogd. Deze logging wordt geactiveerd door middel van de AUDLVL-parameter (Auditing Level) van het gebruikersprofiel (gekoppeld aan de systeemwaarde QAUDLVL).
In de *object action auditing* worden per object de autorisatie-overtredingen van de gebruikers tot dit object gelogd. Deze logging wordt geactiveerd

door middel van de OBJAUD-parameter van het gebruikersprofiel.
Indien in het gebruikersprofiel de *AUDIT-speciale bevoegdheid is gedefinieerd, kan de gebruiker zijn eigen security auditing wijzigen.

Het auditen van de AS/400

De informatie, gegenereerd door de AS/400-logging en -journaling, is erg gedetailleerd en niet direct bruikbaar. Om deze informatie zinvol te kunnen gebruiken, moeten de ruwe records worden bewerkt. Dit houdt in dat de auditor van tevoren moet weten welke auditinformatie voor hem van belang is. Slechts een klein gedeelte van deze informatie kan direct worden opgevraagd met systeemcommando's, maar zelfs dan zijn de verkregen overzichten omvangrijk en gebruikersonvriendelijk. Wil men bepaalde gegevens sorteren en cumuleren, dat moeten er met behulp van query's, CL-programma's of andere tools rapporten op een hoger aggregatieniveau worden samengesteld. De AS/400-(audit) tools zoals PDM (Program Development Manager), Query/400 en Secur/400 bieden iets meer rapportagemogelijkheden dan de standaard AS/400-functies. Maar zelfs daarmee moet de auditor veel meer van tevoren dan anders nadenken welke auditinformatie voor hem van belang is, ofwel tijdig zijn eigen informatiebehoefte definiëren.

Dit is ook van belang voor de nadere invulling van de auditopdracht voor de cliënt. De cliënt verzamelt normaliter nauwelijks andere gegevens dan transactie-logging, accounting- en performancegegevens. Wegens de omvang en detaillering van de standaard AS/400-logging zijn de log-files en de journal receivers snel vol.
Geen enkele organisatie kan het zich permitteren dit soort informatie online te bewaren (wegens het nadelige effect op de performance), of er zelfs maar backups van te maken (het kost te veel opslagruimte). Maar zelfs al zou de organisatie dit doen, dan zou ze later worden geconfronteerd met grote hoeveelheden gegevens die doorgespit moeten worden om iets zinvols te kunnen zeggen over misschien maar één aspect (bijvoorbeeld security-overtredingen).

Om dit te voorkomen, moet de auditor in een vroeg stadium precies aangeven welke rapportages hij nodig heeft voor zijn audit en deze rapporten tijdig laten genereren. Voor de gebruiker is dit om praktische redenen de enig mogelijke manier om de AS/400-logging te gebruiken. Omdat dit tevens betekent dat de gebruiker zijn informatiebehoefte moet bepalen en extra werkzaamheden moet verrichten om deze informatie te verkrijgen (hetgeen al gauw een paar weken programmeerwerk betekent), worden dergelijke werkzaamheden weggeschoven om plaats te maken voor andere IT-prioriteiten.
De systeembeheerder weet dan echter nog steeds niet veel over de mogelijke indringers op zijn systeem, en de auditor moet zich dan bij gebrek aan informatie beperken tot het geijkte rijtje AS/400-beveiligingsparameters. Omdat daar wel een aantal gebreken in te signaleren is, kan de auditor op het oog wezenlijke bevindingen rapporteren, en heeft de systeembeheerder (voorlopig) rust.

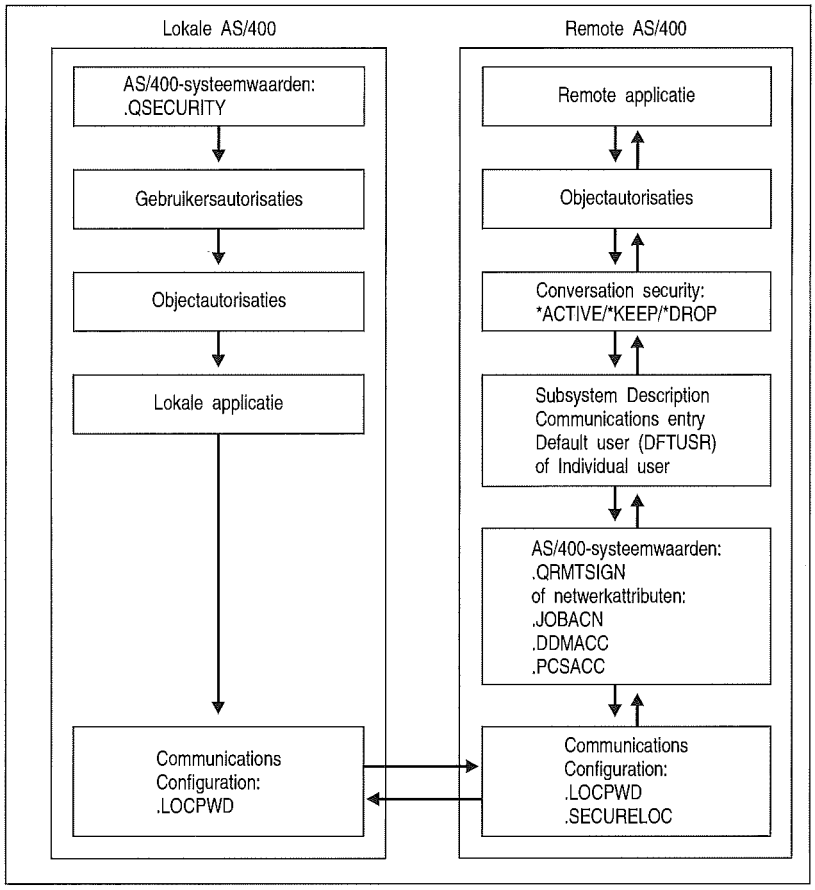
Daarom bij dezen een pleidooi voor een professionalisering van de technische AS/400-audit (en überhaupt van de audit van besturingssystemen!), ten wederzijdse bate van de auditor en de cliënt. Hieronder volgt een eerste aanzet voor de onderwerpen die aan bod moeten komen in een technische AS/400-netwerk-audit.
De aandachtsgebieden daarbij zijn:
- de AS/400-netwerktopologie met haar karakteristieke kenmerken;
- de gelaagdheid van de algehele logische toegangsbeveiliging van de AS/400 (van netwerk via netwerkservices tot individuele AS/400's);
- de specifieke risico's van de verschillende AS/400-netwerkservices (uiteraard zowel in onderlinge samenhang als ten opzichte van het AS/400-besturingssysteem).

Deze drie aandachtsgebieden vormen de bouwstenen waarop de AS/400-netwerkaudit moet worden ingericht. Ze worden achtereenvolgens in de onderstaande drie subparagrafen behandeld.

Audit van de AS/400-netwerktopologie
Wil de auditor inzicht verkrijgen in de algehele (AS/400-)netwerktopologie, dan moet hij informatie verkrijgen over de volgende auditobjecten:
- netwerkattributen;
- datacommunicatielijnen (Line Descriptions, LIND);
- remote controllers (Controller Descriptions, CTLD);
- APPC-devices (Device Descriptions, DEVD);
- communicatiesessies (Mode Descriptions, MODD);
- communicatie-subsystemen, te zamen met de daarin gedefinieerde network job entries en (default) users;
- lokale en remote APPN-configuratielijsten;
- APPN-system directories;
- SNADS-routing tables, -system distribution directories, -gebruikers en -logging;
- DDM-files, -conversaties en -gebruikersbevoegdheden;
- ICF-files;
- CPI-C operation calls.

De security-overtredingen inzake vitale AS/400-objecten worden standaard verzameld in de history log file QHST en in de security audit journal QAUDJRN (indien geactiveerd). De informatie betreft alle AS/400-objecten. De auditor moet daaruit een selectie kunnen maken afhankelijk van:
- hoe belangrijk deze objecten zijn voor de informatieverstrekkende processen in de organisatie;
- hoe belangrijk ze zijn voor de beheersbaarheid van de AS/400 (-networking).

Als de Alert Facility is geactiveerd, kan de informatie uit de history log files van de verschillende systemen op het netwerk in alerts worden geplaatst en verzonden naar één centraal systeem. Om informatie van de security audit journal QAUDJRN te loggen, moet de security audit journaling op alle aan-



Figuur 2. Communicatiepad tussen lokale en remote AS/400's

gesloten AS/400's actief zijn. Zowel voor de alert logging als voor de security audit journaling geldt dat de informatie over de netwerkattributen en over de objecten van de remote systemen moet worden gedestilleerd uit de totale logging. Vervolgens moet ze in afzonderlijke rapporten worden vastgelegd voor nadere analyse.

Audit van de algehele AS/400-logische toegangsbeveiliging

De gelaagdheid van de logische toegangsbeveiliging wordt geïllustreerd in figuur 2, waarin de hiërarchie van beveiligingselementen langs het communicatiepad tussen een lokale en een remote AS/400 staat weergegeven.

De samenhang tussen de beveiligingsfuncties in figuur 2 geeft tevens de reikwijdte van de AS/400-netwerk security audit. De hiërarchie in de audit moet betrekking hebben op de volgende beveiligingslagen:

- De APPC/APPN-beveiliging:
  - de location password-parameter (LOCPWD);
  - de secure location-parameter (SECURELOC);
  - de beveiliging van de LU6.2/APPC-conversatie.

  De beveiligingsrisico's, opgesomd in kader 1, kunnen als een basis-checklist voor de audit van de APPC/APPN-beveiliging worden gebruikt.

- De beveiliging van de toegang tot de AS/400-netwerkservices, gerealiseerd door middel van de parameterinstellingen:
  - de Remote Sign-on Control-systeemparameter (QRMTSIGN) voor DSPT;
  - het Job Action-netwerkattribuut (JOBACN) voor SNADS;
  - het DDM Access-netwerkattribuut (DDMACC) voor DDM;
  - het PC Support Access-netwerkattribuut (PCSACC) voor PC Support.

- De beveiliging van de remote subsystemen gebruikt door de AS/400-netwerkservices:
  - de default user-parameter (DFTUSR) in de communications entries van de remote subsystemen;
  - de bevoegdheden van remote gebruikersprofielen.

- De beveiliging van het besturingssysteem van de lokale AS/400:
  - het AS/400-beveiligingsniveau, ofwel de AS/400-security parameter (QSECURITY);
  - de bevoegdheden van lokale gebruikersprofielen;
  - de objectbeveiliging van lokale en remote applicaties en bestanden;
  - de beveiliging van het Submit Remote Command (SBMRMTCMD)-commando.

Audit van de AS/400-netwerkservices

De audit van de AS/400-netwerkservices moet rekening houden met de specifieke risico's per service.

Een basis-checklist over de specifieke technische risico's van de AS/400-netwerkservices kan worden afgeleid van de opsomming van de beveiligingsrisico's per netwerkservice, zoals die in deel 2 is uitgewerkt (zie de kaders 2 t/m 6).

CONCLUSIE

In dit artikel is gepoogd om inzicht te geven in AS/400-networking. Eerst zijn de basis AS/400-netwerkbegrippen toegelicht tegen de achtergrond van de SNA-netwerkarchitectuur en de implementatie daarvan voor de AS/400. Vervolgens zijn de AS/400-netwerkservices besproken in termen van functionaliteit, beveiligingsrisico's en -maatregelen. Ten slotte is voor het afgebakende kennisgebied een kader geschetst waarbinnen de technische AS/400-netwerkaudit moet plaatsvinden.

De nadruk is bewust gelegd op de technische auditaspecten, met als belangrijkste speerpunt een geïntegreerde benadering van de AS/400-security-audit, namelijk een audit uitgaand van de beveiligingsrisico's, zowel op netwerk- als op besturingssysteemniveau. De beschreven beveiligingsrisico's kunnen als kader fungeren bij het bepalen van de *ist-positie* (in de informatie-analyse aangeduid met de term 'huidige situatie') van de operationele AS/400-netwerk(-services).

De te treffen beveiligingsmaatregelen kunnen worden beschouwd als de *soll-positie*, de 'gewenste situatie', ofwel het ideaalbeeld, waarnaar de gebruikersorganisatie in de toekomst streeft. Of dit ideaalbeeld enkel toekomstmuziek blijft, hangt af van de beslissingen van het management van de gebruikersorganisatie.

De auditor moet streven naar een genuanceerde afweging van de verschillende risicofactoren, zowel technisch als organisatorisch, en moet letten op de samenhang tussen deze factoren, om tot een betrouwbaar oordeel te kunnen komen over de onderzochte technische infrastructuur.

Het management moet een keuze maken uit het brede palet beschikbare (beveiligings)maatregelen, binnen de grenzen van zijn organisatorische en financiële beperkingen.

Het beste resultaat, als het ware de soll-positie van de audit, wordt bereikt wanneer de auditor een pro-actieve, beslissingsondersteunende rol kan vervullen ten opzichte van het management, in plaats van de traditionele 'ex-post', controlerende rol. Dit moet het doel zijn van de moderne audit en van de nieuwe generatie auditors.

LITERATUUR

[Ande93a] R.E. Anderson, *Mission Control to PC-1: We Have Administration*, NEWS 3X/400, January 1993.

[Ande93b] R.E. Anderson, *Those Low-Down, Sign-On-Twice Blues*, NEWS 3X/400, February 1993.

[Ande94] R.E. Anderson, *Shared Folders Essentials*, NEWS 3X/400, July 1994.

[Cape92] C. Capesius, *Communications on a Budget*, NEWS 3X/400, January 1992.

[Galv93] P. Galvin, R. Kerr, E. Rupp, *Making the AS/400-Token-Ring Connection*, NEWS 3X/400, August 1993.

[Enck93] J. Enck, *SNA: At Your Service*, NEWS 3X/400, June 1993.

[Enck94] J. Enck, *Configuring the AS/400 and PC for Multiple LAN Protocols*, Part 1 and Part 2, NEWS 3X/400, March 1994.

[IBM92] *Managing Multiple AS/400s in a Peer Network*, IBM International Technical Support Centers, May 1992, GG24-3614-01.

[IBM94a] An Implementation Guide for AS/400 Security and Auditing: Including C2, Cryptography, Communications, and PC Connectivity, IBM International Technical Support Centers, June 1994, GG24-4200-00.

[IBM94b] *AS/400 APPN Problem Management*, IBM International Technical Support Centers, April 1994, GG24-4222-00.

[IBM94c] *AS/400 Security Reference*, IBM April 1994, SC41-8083-01.

[Koni95] F. de Koning, J. Matto en P. Roos, *Beveiliging en controle in een AS/400-omgeving*, Paardekooper en Hoffman, Rotterdam 1995.

[Madd92a] W. Madden, *Puzzling Out DDM Security*, NEWS 3X/400, May 1992.

[Madd92b] W. Madden, *Remote Database Access: Now You Have a Choice*, NEWS 3X/400, May 1992.

[Meye94] B. Meyers, *AS/400 Network Management on $5 a Day*, NEWS 3X/400, February 1994.

[Neel93] K. Neely, *The Display Station Pass-Through Connection*, Midrange Computing, July 1993.

[Neel94] K. Neely, *Communications Options for Remote AS/400s*, Midrange Computing, February 1994.

[Otte90] M. Ottey, *AS/400 APPN: An Evolution in Networking*, NEWS 3X/400, June 1990.

[Otte92] M. Ottey, *Making PCS, NetWare and Windows Work Together*, NEWS 3X/400, December 1992.

[Otte93a] M. Ottey, *The ABCs of PC Workstations*, NEWS 3X/400, January 1993.

[Otte93b] M. Ottey, *The Definitive Guide to PC-to-AS/400 Connectivity*, NEWS 3X/400, September 1993.

[Pelk94a] C. Pelkie, *Getting Started with SNADS*, Midrange Computing, May 1994.

[Pelk94b] C. Pelkie, *Sending Files with SNADS*, Midrange Computing, July 1994.

[Rieh91] D. Riehl, *The Solution to Mixed-System Development*, NEWS 3X/400, October 1991.

[Russ92] M. Russell, *Distributing Data with DDM++*, NEWS 3X/400, May 1992.

[Smol93] P. Smolens, *Remote ASCII Communications Using PC Support*, NEWS 3X/400, September 1993.

[Stan94] D. Stansburry, *Configuring your AS/400 for SDLC or X.25*, NEWS 3X/400, June 1994.

[Stoc92] Th. Stockwell, *Networking in the Corporate Climate*, Midrange Computing, June 1992.

[Stoc93] Th. Stockwell, *An Overview of IBM's PC Support*, Midrange Computing, July 1993.

Mw. drs. A. L. Hristova RE Is sinds 1993 werkzaam bij de Achmea Interne Accountantsdienst. Zij heeft de studie Bedrijfskunde (Bestuurlijke Informatiekunde) en de post-doctorale opleiding EDP-auditing (Rotterdam) voltooid. In haar werk heeft zij zich onder meer gericht op AS/400-audits; zij heeft een afstudeerreferaat over dit onderwerp geschreven.

EDP AUDITORIUM

OVER NORMALISATIE EN RECHT

BOEKBESPREKING

C. Stuurman, Technische normen en het recht; Beschouwingen over de interactie tussen het recht en technische normalisatie op het terrein van informatietechnologie en telecommunicatie

Deel 17 van de reeks 'Informatica en Recht', Deventer 1995

Prof. mr. dr. J.M. Smits
Hoogleraar Recht en Techniek TU Eindhoven, Adviseur KPMG

Inleiding

De artikelen in Compact 96/1 over normering behandelden vrijwel uitsluitend, kort samengevat, kwaliteitsnormen. Kwaliteitsnormen die vooral het werk van (EDP-)auditors mee kunnen helpen faciliteren. Eén artikel maakt op de hierboven aangegeven reeks een uitzondering en wel het eerste. Dat artikel heet Normbesef, en handelt over de visie van de auteurs op het begrip norm, de mogelijke bronnen van normen, de classificatiemogelijkheden en de toepasselijke metanormen ([Anno96]). Hoewel dit een zeer verhelderend artikel is ziet het minstens één aspect van (kwaliteits)normen geheel over het hoofd, namelijk dat door allerlei juridische regels de normen in het recht worden 'opgenomen'. Zo bepalen bijvoorbeeld de Wet computercriminaliteit en de Wet persoonsregistraties dat beveiliging van 'bestanden' dient te geschieden naar de stand van de techniek. En hoe wordt nu vaak de stand van de techniek bepaald? Door gebruik te maken van in (norm)documenten opgenomen/vastgelegde technieken. Ziehier de reden voor een nadere uitleg van de doorwerking van normen in onze samenleving door wettelijke regels die verwijzen naar technische normen. Over deze en andere (juridische) problematieken handelt een zeer recent proefschrift van de hand van C. Stuurman, medewerker aan de Juridische Faculteit van de Vrije Universiteit en advocaat te Amsterdam.

De (onder)titel van het proefschrift van C. Stuurman laat niets aan duidelijkheid te wensen over, hier wordt precies aangegeven wat er door de promovendus zal worden behandeld: *Technische normen en het recht; Beschouwingen over de interactie tussen het recht en technische normalisatie op het terrein van informatietechnologie en telecommunicatie.* Op 23 november 1995 verdedigde hij zijn dissertatie.

Het is geen gemakkelijk boek. En dat niet vanwege de, in het huidige tijdsgewricht van AIO's, ongebruikelijke dikte van 565 pagina's. Het is vooral niet gemakkelijk omdat de meeste juristen, en dat is gelukkig niet alleen de doelgroep die Stuurman voor ogen heeft, zeer weinig weten van het onderwerp dat Stuurman zo overtuigend en veelomvattend behandelt. Daarbij heeft de schrijver het aangedurfd niet alleen oog te hebben voor het normalisatieproces in de Nederlandse context, maar hij heeft het toch al lastige onderwerp ook nog eens bestudeerd vanuit zowel de Duitse als de Amerikaanse normalisatie- en juridische praktijk.

Deze bespreking is opgebouwd rond de volgende onderwerpen:
- wat is eigenlijk een technische norm en waarvoor dient zo'n norm?
- de formele kant van het normalisatietraject: hoe komen technische normen tot stand?
- de 'opname' van technische normen in het recht;
- aansprakelijkheid bij het niet-naleven van normen;
- normalisatie en mededingingsrechtelijke aspecten, normen als technische handelsbelemmering, en normen en intellectuele eigendom.

Wat is eigenlijk een technische norm?

Er bestaat geen consensus over de definitie van een technische norm dan wel een standaard en het verschil daartussen. Ook het tot stand brengen van normen/standaarden in diverse fora geschiedt niet volgens dezelfde procedures. Stuurman geeft in zijn inleidende hoofdstuk een kort en vooral helder overzicht van de verschillende definities die in de normalisatiewereld worden gehanteerd.

'In dit werk zal dan ook worden volstaan met het hanteren van de term normalisatie. Daaronder zal hier worden verstaan de ontwikkeling van technische normen voor beoogd gebruik in brede kring. Indien de normalisatie geschiedt door normalisatie-organisaties en/of -instituten, met als kenmerk dat er sprake is van consensus in een door formele procedurevoorschriften beheerst open proces waaraan alle belanghebbenden kunnen deelnemen, dan zal worden gesproken van formele normen en formele normalisatie. Indien buiten dergelijke gremia normen worden opgesteld, dan is sprake van de facto normen en de facto normalisatie.' (p. 17)

Dit is de *eerste* belangrijke afbakening die Stuurman kiest. Het merendeel van de normalisatieorganen die hij bespreekt bevindt zich in het formele normalisatietraject, hoewel met name bij de bespreking van het tot stand komen van IT-normen hij ook niet om de facto normalisatie heen kan. En dat brengt de *tweede* afbakening naar voren die de auteur gebruikt, namelijk de keuze voor de informatie- en telecommunicatietechnologie (IT&T) als de te behandelen technologie.

De formele kant van het normalisatietraject

De formele kant handelt over de manier waarop technische normen tot stand komen. Het gaat hierbij om de procedures. Bezwaren zijn er vooral te maken tegen de manier waarop de formele (procedurele) kant van de normalisatie is beschreven. In het tweede hoofdstuk staan veel overbodige stukken terwijl tegelijkertijd belangrijk feitenmateriaal ontbreekt. Bij een onderwerp dat juristen veel meer zou moeten bezighouden dan dat het doet, is het jammer dat het lezen van een dergelijk monumentaal werk wordt bemoeilijkt door zo uitvoerig stil te staan bij de formele normalisatietrajecten. Terwijl Stuurman hier juist had kunnen helpen de wat ondoorzichtige normalisatiebrij te verhelderen zoals hij dat wel doet met de begrippen en definities in hoofdstuk 1.

In de ondertitel is te lezen dat ook de normalisatie van de telecommunicatie zal worden behandeld. Die belofte wordt niet volledig gestand gedaan. Belangrijke wijzigingen die in de Internationale Telecommunicatie Unie (ITU) in de laatste paar jaren hebben plaatsgevonden, laat Stuurman vrijwel onbesproken en dat terwijl het juist deze veranderingen zijn die een stevige bijdrage aan zijn eigen argumentatie in het staatsrechtelijk hoofdstuk hadden kunnen leveren. Doorgaans wordt er in een normalisatieproces naar gestreefd een norm af te leveren waartegen (binnen de verschillende lagen van het desbetreffende normalisatie-orgaan) geen onoverkomelijke bezwaren van individuele deelnemers meer bestaan. Daarom komt in de literatuur over normalisatie nogal eens naar voren dat het een op consensus gericht proces zou zijn. Of dat in de werkelijkheid inderdaad het geval is, kan vooralsnog beter in het midden worden gelaten. Stuurman zegt hierover onder andere op pagina 103, waar hij refereert aan de nationale en Europese formele normalisatie-organen:

'Besluitvorming vindt daarbij in principe zoveel mogelijk plaats op basis van consensus, hoewel een duidelijke trend waarneembaar is in de richting van meerderheidsbesluitvorming.'

De normalisatieprocedures binnen de ITU zijn in de afgelopen jaren van deze 'consensusbenadering' afgestapt. Binnen ITU-normalisatiewerkgroepen kan nu met meerderheid van stemmen een technische norm worden aangenomen. Het is zelfs zo dat het niet langer noodzakelijk is fysiek aanwezig te zijn bij een stemming, ook schriftelijke stemmingen zijn voortaan mogelijk. In de verdragsteksten (bestaande uit een Constitutie, Conventie en Administratieve Regels) van de ITU is dit als volgt geformuleerd:

'Telecommunication standardization study groups shall study questions and prepare draft recommendations on the matters referred to them in accordance with the provisions of Article 6 of this Convention. Those drafts shall be submitted for approval to a world telecommunication standardization conference or, between two such conferences, by correspondance to administrations in accordance with procedures adopted by the conference. Recommendations approved in either matter shall have equal status' [ITUP92a].

Een ander element dat Stuurman niet goed taxeert in het kader van de ITU-normalisatie is dat hij op pagina 68 van zijn boek binnen de ITU geaccepteerde normen vrijwillige normen noemt.[1] Dit is onjuist; op grond van artikel 13C Constitutiegedeelte en de artikelen 6A en 7E Conventiegedeelte van het ITU-verdrag worden normen zoals die formeel door de ITU Standardization Sector zijn afgehandeld, deel van het ITU-verdrag. Daardoor ontstaat er formele juridische binding voor de Lid-Staten de normen te implementeren. Het enige juridische instrument dat een Lid-Staat ter beschikking staat, is een formele reservering in het Verdrag te maken op de dag van de ondertekening van het Verdrag. Dit is wat bijvoorbeeld de Verenigde Staten al sinds jaar en dag doen met betrekking tot de meeste van de binnen de ITU geaccepteerde normen ([ITUP92b]).

Het is de interactie tussen de probleemvelden waarin de grote waarde ligt van dit onderzoek.

De 'opname' van technische normen in het recht

De hoofdstukken 4 tot en met 6 vormen het (wetenschappelijk interessante) hart van dit proefschrift, en in het vierde hoofdstuk komt de belangrijke vraag aan de orde of technische normen eigenlijk wel rechtsnormen zijn. Stuurman geeft zelf een tweedeling van de behandeling van het onderwerp:

- de invloed van technische normalisatie op de rechtsvorming en rechtstoepassing;
- de invloed van het recht op technische normalisatie.

Het is met name de interactie tussen deze twee onderscheiden probleemvelden en de bespreking die Stuurman eraan wijdt waarin de grote waarde ligt van dit onderzoek. Noch in de Nederlandse rechtswetenschap noch daarbuiten komt bovenstaande benadering vaak voor.

De neerslag van een onderzoek in een boek als dit is belangrijk voor een versterking van het onderlinge begrip tussen twee volstrekt verschillende disciplines: aan de ene kant de juridische en aan de andere kant de (IT- en telecom-)technische. Beide disciplines zijn door Stuurman bij elkaar gebracht op een zodanige wijze dat zij van elkaars disciplinaire vertrekpunten (en de eigen axioma's) kunnen kennisnemen. Hiermee wordt overtuigend aangetoond dat zijn onderzoek een bijdrage levert aan deze zo noodzakelijke interactie. Het almaar 'technischer' worden van onze samenleving zorgt er immers voor dat juristen steeds meer worden geconfronteerd met ingewikkelde technologieën waarvan ze de 'ins and outs' nauwelijks begrijpen, terwijl dat een noodzakelijke voorwaarde is voor het adequaat kunnen vormgeven van contracten, rechterlijke uitspraken en regelgeving. Anderzijds is het goed dat Stuurman duidelijk maakt aan technici dat juristen (wellicht lastige) vragen hebben en

1. Als Stuurman hier met 'binnen' impliceert dat zij slechts gelding hebben binnen de ITU als (volkenrechtelijke) organisatie dan heeft hij natuurlijk gelijk. Maar waarschijnlijk bedoelt hij dat zij wel degelijk ook buiten de ITU zullen gelden, namelijk voor de Lid-Staten van de ITU. Als tevens wordt bedoeld dat zij dan 'vrijwillige' normen zijn dan heeft hij ongelijk (zie verdere tekst).

stellen over zaken waar technici zich over het algemeen te weinig mee bezighouden.
Dat geldt met name voor het vierde hoofdstuk: Technische normen en regulering. Hier stelt hij de nog steeds (in deze technische en juridische context) veel te weinig gestelde vraag naar de doorwerking in het recht van technische normen aan de orde. Dit hoofdstuk is beslist bestemd voor juristen en beleidsmakers, maar is ook voor de geïnteresseerde technicus zeer de moeite waard. Stuurman concludeert dat (formele) technische normen wat betreft hun karakter (in strikt positivistische zin) als zodanig niet als rechtsnormen zijn te beschouwen. Niettemin zullen per saldo de technische normen in brede kring worden gevolgd en ze zullen dan ook vaak feitelijke gelding bezitten. Stuurman suggereert in het kader van de vraag of normalisatie als een vorm van zelfregulering moet worden gezien dat verder onderzoek nodig is omdat onderzoek naar de maatschappelijke betekenis van technische normen achterblijft bij de vraag.

De technische normen zullen in brede kring worden gevolgd en feitelijke gelding bezitten.

Het deel van dit hoofdstuk dat handelt over de rechtsstatelijkheid (in hoeverre normen onderdeel uitmaken van ons rechtssysteem) is heel interessant en welhaast spannend om te lezen. Het is een belangrijk onderwerp dat in het boek van Stuurman gelukkig de aandacht krijgt die het verdient. Iemand met het inzicht in de materie dat hij hier tentoonspreidt, had echter mijns inziens wel krachtiger stelling mogen nemen. Nu schrijft hij op pagina 200:

'Hoewel principieel bezien mijn voorkeur uit zou gaan naar een sterke inhoudelijke overheidsbemoeienis met normalisatie – om op die wijze naleving van de beginselen van de democratische rechtsstaat te waarborgen – dwingt mijns inziens de (huidige) realiteit tot het beperken van verdere juridische interventies in het technische normalisatieproces.'

Hij komt met voorstellen tot verbetering van die huidige praktijk en hij pleit voor het maken van een wettelijke basis in de vorm van een 'Normalisatiewet'. Daarin wordt een systeem opgezet waarbij de overheid een actievere (normalisatie)rol op zich neemt, nadrukkelijker dan tot nu toe actieve deelname van belanghebbenden stimuleert en waarbij adequate onafhankelijke toetsing mogelijk wordt gemaakt en waarbij (ontwerp)normen die in wettelijke regels zullen worden opgenomen integraal worden gepubliceerd. Maar de (democratische c.q. rechtsstatelijke) bezwaren die hij eerder uitte tegen de huidige systematiek verhinderen wat hem betreft de implementatie van een sterkere overheidsrol.

Het materiaal dat Stuurman bijeengebracht heeft in de eerste vier hoofdstukken is vooral interessant voor wetenschappers die in de materie zijn geïnteresseerd. Het materiaal dat aan de orde komt vanaf hoofdstuk 5 is vooral voor de (juridische en normalisatie-) praktijk interessant. Een ieder die in zijn werk te maken heeft met normen – denk bijvoorbeeld aan de ISO 9000-serie, radio-ontstoringsnormen of toegestane toevoegingen in voeding – zal veel relevant materiaal kunnen vinden in dit boek. Ook vertegenwoordigers van bepaalde (van veel technische normen gebruik makende) sectoren zullen vooral in hoofdstuk 6 een uitgebreide bron vinden. Normalisatie kan immers, vanuit een bepaalde optiek, worden gezien als (pre-competitieve) samenwerking en komt daarmee op het terrein van het (Europese) mededingingsrecht terecht.

De rol die normalisatie speelt in innovatieprocessen, waarmee dus uiteindelijk iets wordt gezegd over de effecten die het al of niet meedoen aan normalisatie heeft op de concurrentiële slagkracht van een bedrijf, sector of zelfs land, wordt door Stuurman slechts kort aan de orde gesteld.

Normen en aansprakelijkheid

Leidt het niet naleven van normen tot aansprakelijkheid? Dit is in een sterk op techniek en haar toepassing gerichte samenleving een belangrijke vraag. Recentelijk kwam bijvoorbeeld de vraag naar voren wie verantwoordelijk was voor de hinder ondervonden door en schade aangebracht aan door GSM-telefoons gestoorde gehoorapparaten. Ook waren er GSM-telefoons die bepaalde ziekenhuisapparatuur zouden storen dan wel onklaar zouden maken. Wanneer er werkelijk schade ontstaat, zal de vraag naar voren komen wie die zal betalen. Zoals Stuurman het zelf zegt op pagina 209:

'Naarmate technische normen een belangrijker rol gaan spelen bij de onderlinge interactie tussen apparaten (dan wel het voorkomen van ongewenste interactie) en in de interactie tussen mens en machine, wint de vraag naar de mogelijke aansprakelijkheden rond het opstellen, het voorschrijven en het toepassen van technische normen aan betekenis'.

Hij behandelt deze vraag vanuit het civielrechtelijk aansprakelijkheidsperspectief en doet dat niet alleen voor Nederland, maar tevens voor Duitsland en de Verenigde Staten. In alle drie de rechtsstelsels geldt dat het sluiten van een contract waarin geen rekening wordt gehouden met de technische normalisatie, een (groot) aantal problemen kan veroorzaken. Tegelijkertijd dragen natuurlijk de huidige produktaansprakelijkheidsregimes ertoe bij dat een producent niet zomaar onder elke schadeclaim kan uitkomen. Een mooi voorbeeld van de interactie die er tussen normalisatie en recht (en omgekeerd) plaatsvindt, geeft Stuurman op pagina 296 bij zijn conclusies voor de Verenigde Staten en de (rol van) produktaansprakelijkheid:

'Niet alleen spelen normen een rol in het Amerikaanse produktenaansprakelijkheidsrecht maar omgekeerd heeft ook de ontwikkeling van de produktaansprakelijkheid invloed gehad op de invulling van de eisen die in de Verenigde Staten aan het normalisatieproces worden gesteld. Dit zowel wat betreft de aard van normen (ver-

schuiving van produktie- naar prestatiekenmerken), de presentatie van normen als voor wat betreft de aandacht die van het toepassen van normen kan uit gaan op de veiligheidsverwachtingen van de eindgebruikers.'

Mededinging

Eigenlijk vormt het normalisatieproces, het deelnemen door verschillende (vertegenwoordigers van) bedrijven, organisaties en overheidsentiteiten aan een normalisatiewerkgroep, een organisatievorm waarbij partijen met elkaar (gaan) afspreken hoe zij zich met betrekking tot een bepaald technisch aspect ten opzichte van elkaar zullen (gaan) gedragen. Voorwaar iets waar de mededingingsautoriteiten in geïnteresseerd zouden moeten zijn. Dat zijn ze ook. Hier doet zich een paradox voor. Wanneer dergelijke afspraken niet zouden zijn toegestaan, zou er veel verspilling in tijd en geld plaatsvinden doordat produkten pas na een strijd op de markt een positie als *de facto* norm zouden kunnen krijgen. Om nu ruïneuze concurrentie te voorkomen (en dit is slechts één van de voordelen van normalisatie) staan juist mededingingsautoriteiten dergelijke (pre-competitieve) samenwerking toe. Een door Stuurman aangehaald citaat van ex-staatssecretaris Yvonne van Rooij laat wat dit betreft niets aan duidelijkheid te wensen over: *'Wie de normen heeft, heeft de markt'.*

In het 'mededingingsgedeelte' van het proefschrift (de hoofdstukken 6 tot en met 8) stelt Stuurman een aantal zeer interessante vragen aan de orde, letterlijk geciteerd:

'Bij het bestuderen van de rol van normen in het economisch verkeer is als structuur gekozen voor het onderscheiden van de volgende thema's:

1. *De mededingingsrechtelijke aspecten van het ontwikkelen en toepassen van normen. De volgende kernvragen worden daarbij onderscheiden:*
   - *A. Welke beperkingen stelt het mededingingsrecht aan het (formele en de facto) normalisatieproces?*
     - *A.1 In welke mate is het (voor marktpartijen) toegestaan om samen te werken bij het opstellen van een norm?*
     - *A.2 In welke mate en op welk moment dienen derden te worden toegelaten tot het normalisatieproces?*
     - *A.3 In welke mate dienen derden te worden geïnformeerd over het normalisatieproces en de resultaten daarvan?*
   - *B. Welke grenzen stelt het mededingingsrecht aan het toepassen van normen?*
2. *Normen als technische handelsbelemmering;*
3. *Bescherming van normen en normdocumenten op grond van onrechtmatige daad en intellectuele eigendomsrechten.'* (p. 297)

De vragen worden in respectievelijk de hoofdstukken 6, 7 en 8 behandeld.

In 1977 deed de Europese Commissie uitspraak in de zogenaamde X/Open Group zaak. Een groot aantal Europese ondernemingen sloot een samenwerkingsovereenkomst om te komen tot uniforme normen voor een gemeenschappelijke toepassingsomgeving voor computerprogrammatuur welke functioneerde onder Unix:

'De commissie constateerde dat, hoewel publikatie plaatsvond van de specificatie, voor de niet-deelnemers niettemin een concurrentienadeel ontstond omdat zij niet in het bezit kwamen van de technische kennis en know-how opgedaan bij de vaststelling van deze specificaties en pas later over de specificaties konden beschikken. Gezien het belang dat in de IT-industrie bestond bij een voorsprong stelde de Commissie vast dat de leden van de groep een aanzienlijk voordeel konden behalen. Dit leidde tot de vaststelling dat de toetredingsregels van bijzondere betekenis zijn. De Commissie stelde ten dien aanzien vast dat deze niet alleen concurrenten konden uitsluiten maar ook een discriminerende behandeling van lidmaatschapsaanvragen mogelijk maakten.' (p. 324-325)

'Bijzondere aandacht voor IT&T-normalisatie is gerechtvaardigd.'

Uiteindelijk heeft de Commissie deze samenwerking toch toegestaan. Er werd een ontheffing voor verleend omdat de voordelen (het tot stand komen van een open norm) groter waren dan de nadelen. De Commissie stelde wel een aantal strenge voorwaarden aan voortzetting van de samenwerking. Aan de hand van een groot aantal voorbeelden werkt Stuurman systematisch en zeer begrijpelijk de mededingingsrechtelijke kant uit. Zijn conclusie op pagina 374 laat niets te raden over:

'Uit de literatuur en de rechtspraak is niet af te leiden dat bij Europese en nationale mededingingsautoriteiten (althans in Nederland) een bijzondere aandacht voor normalisatieprocessen bestaat. Gezien de belangen die nu, in de geboortefase van de informatiemaatschappij, gemoeid zijn met IT&T-normalisatie acht ik een dergelijke bijzondere aandacht echter nadrukkelijk gerechtvaardigd.'

Hoofdstuk 7 stelt als vraag in hoeverre normen als technische handelsbelemmering kunnen (mogen) worden gehanteerd, binnen de Europese Unie (meer precies de Europese Economische Ruimte: EER) en tussen de EER en derde landen. Het Hof van Justitie heeft een grote rol gespeeld bij het tot stand brengen van een gemeenschappelijke markt binnen de Europese Unie. Stuurman concludeert (p. 430):

'Door een ruime interpretatie te geven aan artikel 30 [EU Verdrag, JS], *en voorts op basis daarvan het beginsel van wederzijdse erkenning te ontwikkelen, heeft het Hof van Justitie een cruciale rol gespeeld bij het slechten van intracommunautaire handelsbelemmeringen.'*

Hoofdstuk 8, waarin de juridische bescherming van normdocumenten en normen aan de orde komt, heeft meer dan de andere hoofdstukken in het boek een verkennend karakter. Stuurman stelt dit zelf overigens ook al in de eerste regels van het hoofdstuk. Niettemin is dit een onderwerp dat van

zeer groot belang is. Stuurman komt op pagina 472 tot de conclusie dat:

'Het lijkt er derhalve op dat normen niet zozeer juridisch worden achtergesteld, maar praktisch gezien de rechthebbenden daarop het wel zwaarder te verduren hebben. Daarbij is het van belang dat het ontwikkelen van een produkt of een deel daarvan dat tot norm kan worden veelal niet voldoende is; het tot norm 'maken' daarvan vereist veelal grote (marketing)inspanningen. Mag daar een per saldo verminderde bescherming tegenover staan?

Deze vraag, (..., lijkt) mij een meer dan voldoende rechtvaardiging voor nader (grondslagen)onderzoek naar de relatie tussen normalisatie en het intellectuele eigendomsrecht.'

Deze conclusie is tevens ook de allerlaatste zin van het inhoudelijke gedeelte van het proefschrift van Stuurman. In feite geeft de conclusie het sjabloon voor de meeste door hem aangeroerde onderwerpen. Op de meeste van deze onderwerpen zal nog (veel) nader onderzoek moeten worden gedaan. We kunnen Stuurman dankbaar zijn voor de systematische wijze waarop hij voor andere (toekomstige) onderzoekers de richting heeft aangegeven. Het is te hopen dat we in de nabije toekomst meer van dit type onderzoeken zullen zien, waarbij de door Stuurman aangegeven richting verder wordt uitgediept.

Afsluitend

Dit boek is een fraaie en belangwekkende bijdrage aan de discussie binnen het terrein van recht en techniek en het is te hopen dat meer publikaties van Stuurman op dit terrein het licht zullen zien. Juristen met een technische 'tic' zijn nog steeds te zeldzaam terwijl ze zo'n synergetisch effect op beide disciplines zouden kunnen hebben. Technici met een juridische tic zijn nog veel zeldzamer, dit belangrijke onderzoeksterrein zal het wel van in silicium gegoten juristen moeten hebben. Of toch niet?

Naast dat dit boek een grote bijdrage levert aan de discussie over normalisatie en recht bezit het vier zwakke punten:

1. de behandeling van de normalisatie binnen de ITU is relatief onderbelicht gebleven;
2. de structuur van met name hoofdstuk 2, en in mindere mate de hoofdstukken 7 en 8, zou wat sterker hebben gekund;
3. de omvang is aanzienlijk, hetgeen natuurlijk een rechtstreeks gevolg is van de gekozen opzet om het gehele IT&T-terrein en het daarop betrekking hebbende recht in de verschillende landen zo gedetailleerd mogelijk te beschrijven;
4. het is niet in het Engels geschreven, hetgeen jammer is omdat dit onderzoek nu zijn waarde vrijwel alleen zal kunnen hebben op een kleine thuismarkt terwijl de behandelde problematiek op zijn minst binnen de gehele Europese Unie speelt.

Het boek is beslist de moeite waard indien u:

- als technicus of jurist nu wel eens wilt weten hoe technische normen tot stand komen;
- wilt weten hoe het recht technische normen incorporeert en wilt weten welke nuances uw visie daarop zou moeten hebben;
- een naslagwerk wilt hebben waarmee u een inzicht krijgt hoe het recht reageert op bepaalde aspecten van normalisatie zoals mededinging, aansprakelijkheid en de positie van normen in relatie tot intellectuele eigendomsrechten.

Voor de in deze materie geïnteresseerde expert is dit boek een must; zelden is op een zo overtuigende wijze een poging gedaan twee op het eerste oog vrijwel onverzoenbare disciplines aan elkaar te relateren, waarbij tegelijkertijd ook zoveel verschillende literatuur toegankelijk is gemaakt en is geordend. Aan lezers, en dat zullen meestal technici zijn, die in hun praktische werkzaamheden met normalisatie te maken hebben en zich afvragen hoe het recht op het resultaat van hun werkzaamheden reageert, zal het boek het benodigde inzicht kunnen verschaffen. Voor juristen die zich afvragen op welke manier het mededingingsrecht en intellectuele eigendomsrechten kunnen en moeten worden uitgeoefend in relatie tot normalisatieprocessen en normen: zij zullen veel nuttige informatie aantreffen.

LITERATUUR

[Anno96] L. Annokkée en B. Sebregts, *Normbesef*, Compact 96/1.

[ITUP92a] ITU Plenipotentiary, *Final Acts Geneva*, artikel 14, lid 1, sub 1 (CV312), 1992.

[ITUP92b] ITU Plenipotentiary, *Final Acts Geneva*, artikel 43 (CV312), 1992.

EEN GEVOEL VAN VEILIGHEID

Dr. E. Roos Lindgreen, *A Sense of Secureness, approaches to information security*

Proefschrift, TU Delft

Edo Roos Lindgreen promoveerde op 29 maart 1996 aan de Technische Universiteit Delft op zijn proefschrift *A Sense of Secureness*. In de komende nummers van Compact treft u een aantal bewerkte en in het Nederlands vertaalde hoofdstukken uit dit proefschrift aan. In dit artikel geeft de auteur een blik vooruit.

Het aantal informatica-opleidingen dat structureel aandacht besteedt aan het onderwerp informatiebeveiliging is met een kaarsje te zoeken. Toch is informatiebeveiliging reeds sinds het einde van de jaren zestig onderwerp van academisch onderzoek. Zulk onderzoek werd en wordt veelal uitgevoerd in het kader van ontwikkelingsprojecten voor het Amerikaanse Ministerie van Defensie. De resultaten ervan kennen een wisselende verspreidingsgraad en levensduur. Sommige onderzoeksresultaten zijn in brede kring geaccepteerd en zullen waarschijnlijk tot in lengte van dagen bekend blijven; andere resultaten zijn slechts, al of niet terecht, in kleine kring bekend geworden en vervolgens in de vergetelheid geraakt. In beide gevallen kunnen we ons met recht afvragen wat een kwart eeuw onderzoek ons daadwerkelijk heeft opgeleverd. Zijn onze systemen zoveel veiliger geworden? Die vraag laat zich niet licht beantwoorden.

Een resultante van het verrichte onderzoek is wel dat we meer inzicht hebben in de kwetsbaarheden van onze systemen en de bedreigingen waaraan ze bloot staan. Er zal geen deskundige zijn die zal ontkennen dat veel van onze informatiesystemen lang niet zo veilig zijn als we eigenlijk zouden willen en dat we risico's lopen die eigenlijk niet verantwoord zijn. De qua beveiliging verre van optimale *state of the art* van de moderne informatietechnologie blijkt uit een groeiende stroom boeken en artikelen in vakbladen en wetenschappelijke tijdschriften en de steeds uitgebreidere aanvulling die het Internet daarop tegenwoordig biedt.

Voor het onderzoek, dat van 1991 tot 1996 plaatsvond aan de Technische Universiteit Delft, behoefde de onveiligheid van informatiesystemen dus niet nog eens onderzocht en aangetoond te worden; zij kon gevoeglijk als uitgangspunt worden gehanteerd. Ook werd het zoeken naar weer een nieuwe beveiligingsoplossing als onderzoeksonderwerp uitgesloten. In plaats daarvan werd gekozen voor een pas op de plaats: het inventariseren en analyseren van bestaande methoden en technieken voor het beveiligen van informatiesystemen, met bijzondere aandacht voor hun praktische toepasbaarheid. Bij het onderzoek werd in eerste instantie onderscheid gemaakt tussen de twee fundamentele fasen in de levenscyclus van een systeem – ontwikkeling en produktie – en werd in het bijzonder aandacht besteed aan recente ontwikkelingen.

En dat laatste was hard nodig. Want al snel bleek gedurende het onderzoek dat informatiebeveiliging bepaald geen rustig vaarwater was en is. De afgelopen vijf jaar hebben veel nieuwe ontwikkelingen plaatsgevonden. Ontwikkelingen die, om de gewenste aansluiting met de praktijk niet te verliezen, bij het onderzoek betrokken moesten worden. De verdergaande deconcentratie van informatiesystemen, nieuwe toepassingen van encryptie, de opkomst van het Internet en de Code voor Informatiebeveiliging vonden zo hun plaats in het onderzoek. Daarbij kon worden gesteund op de praktijkervaringen in drie door het Ministerie van Economische Zaken gesubsidieerde ontwikkelprojecten.

Vooruitlopend op de komende artikelen kan gesteld worden dat het onderzoek twee belangrijke conclusies heeft opgeleverd.

De eerste conclusie luidt dat onveilige informatietechnologie kennelijk een beter commercieel perspectief heeft dan veilige informatietechnologie. Onveilige systemen zijn goedkoper, sneller gereed en doorgaans vriendelijker in het gebruik dan veilige systemen. Met name de kortere time-to-market zorgt ervoor dat onveilige systemen de markt veroverd hebben voordat veilige systemen het stadium van de tekentafel gepasseerd zijn. Een gevolgconclusie is dat onveilige informatietechnologie voorlopig niet uit de maatschappij weg te denken zal zijn. Leren omgaan met onveilige systemen lijkt dan ook een betere strategie te zijn dan streven naar systemen met vooraf ingebouwde veiligheid.

De tweede conclusie luidt dat het nog ontbreekt aan goede technieken om specifieke beveiligingsmaatregelen af te stemmen op de beleidsdoelstellingen van een organisatie. De Code voor Informatiebeveiliging vormt in dit traject niet meer en niet minder dan een belangrijke schakel, een schakel die op veel punten nog nadere invulling behoeft.

En de toekomst? Nieuwe ontwikkelingen creëren nieuwe risico's, nieuwe bedreigingen – en nieuwe uitdagingen voor diegenen die in het vakgebied informatiebeveiliging werkzaam zijn. Het Internet en aanverwante netwerkruimten vormen hierbij essentiële kennisbronnen, maar het raadplegen van deze bronnen wordt in veel gevallen gehinderd door tijdgebrek. Verval van kennis is daarmee misschien wel het grootste risico. Juist op het gebied van de informatiebeveiliging zijn permanente educatie en kennisoverdracht van vitaal belang. Hopelijk kan de komende serie artikelen hieraan een kleine bijdrage leveren.

CUMULATIEF

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

1 22e jaargang 95/1 lente 1995

Internetworking; beheerproblematiek en security-risico's
H. Roos RA en ir. M.T.H. Heesbeen

Geïntegreerd netwerkbeheer
Ing. W.A.A. Zoon

Client/server geconcretiseerd
J.C. van Praat RE RA

Radio-LAN's in de praktijk
Ir. B.J. Busropan, ir. G.J. de Groot, ir. W. Hollemans, ir. E.C. den Toom en ir. A. Verschoor

3DAS-kenmerk, een uniek middel voor identificatie en authenticatie
Ir. W.H.M. Sipman RI

2 22e jaargang 95/2 zomer 1995

Het beheer van PC-netwerken
Drs.ing. R.F. Koorn CISA

Multimedia nader bekeken
Drs. A.M. Buren
Introductie van een bancair systeem in een wide area netwerkomgeving
W.N.P. Zethof RE RA

GEBIT. Gestructureerd Evalueren van de Baten van IT-investeringen
Mw. M.S. Hablous

3 22e jaargang 95/3 herfst 1995

Informatietechnologie als beoordelingsobject in de hedendaagse controlebenadering
Mw. W.A. de Munck RA

Plaats en taken van de EDP-auditfunctie bij de KLM
J.G. de Vries RE RA

Wet op het consumentenkrediet: systeemgericht onderzoek vereist
R. van den Hoorn RA

Third party review en -mededeling bij uitbesteding van IT-services
Drs. P. Veltman RE RA

Maatwerk past informatiebeveiliging
Drs. E. Roos Lindgreen en mw.drs. C. Schönfeld RI

Stroomlijnen en herontwerpen in een onderhoudsbedrijf: gelijktijdig en/of volgtijdig?
Drs. O.C. van Leeuwen RA en drs. M.C. van Veen RC

Het ontwikkelen van methoden en technieken van EDP-auditing
Drs. R.G.A. Fijneman RE RA

4 22e jaargang 95/4 winter 1995

Informatieplanning en standaardpakketten
Drs. J. de Boer en ir. J.A.M. Donkers RE

Certificatie van een standaardpakket voor financiële administraties
Drs. H.G.Th. van Gils RE RA

AO en standaardpakketten: integratie verhoogt de kans op een succesvolle selectie en implementatie
Drs. J.J. van Beek RE RA, drs. W. Boogaard RA CPIM en drs. J.J.B. van den Oever

Waardebepaling van software
Ir. J.A.M. Donkers RE en drs. G.J.J. Timmer

Business Process Controlling
Drs. J.J. van Beek RE RA en W. Teeuwissen RA

2 23e jaargang 96/1

Normbesef
L. Annokkée RE en B. Sebregts RE

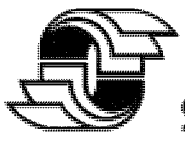
ISO 9000 en EDP-auditing
Mr. W.R. Nanninga RE en ltkol J.M.W. van de Garde RE

ITIL als inrichtings- en beoordelingsinstrument
Drs. F.J. Hut

De Code voor Informatiebeveiliging
Dr.ir. P.L. Overbeek

De Code voor Informatiebeveiliging als norm voor de EDP-auditor
W.S.C. Krol RE en drs. M.M. Smits

KPMG EDP Auditors



Samsom BedrijfsInformatie