Bescherming met minimale middelen en maximaal resultaat

Drs. M.R. Verhoef RE en ir. A.T. Wijsman

Het management van organisaties staat in het huidige economische klimaat onder druk om kosten te beperken en concrete financiële resultaten te behalen. Investeringen in voorzieningen voor de bedrijfscontinuïteit worden in dat licht gesteld, of zelfs afgesteld. Wat vaak onderbelicht blijft is het feit dat continuïteitsvoorzieningen ook veel financiële en non-financiële voordelen kunnen opleveren. In dit artikel wordt ingegaan op het benutten van deze voordelen, en op het minimaliseren van de kosten bij investeren in bedrijfscontinuïteit.

Inleiding

Als het economisch wat minder gaat, moeten ook organisaties de tering naar de nering zetten, een activiteit die het management voor moeilijke dilemma's plaatst. Bij veel organisaties is het ontstaan van zo'n situatie een reden om te snijden in de uitgaven die zich niet direct vertalen in een stijgende kasstroom. En tot die categorie van uitgaven behoort het gehele spectrum van beveiligingsinvesteringen, waaronder de investeringen in bedrijfscontinuïteit. Op de voordelen van en de tips voor 'slim' investeren in bedrijfscontinuïteit zal in dit artikel worden ingegaan, geïllustreerd door recente praktijkvoorbeelden uit het Nederlandse bedrijfsleven.

De issues

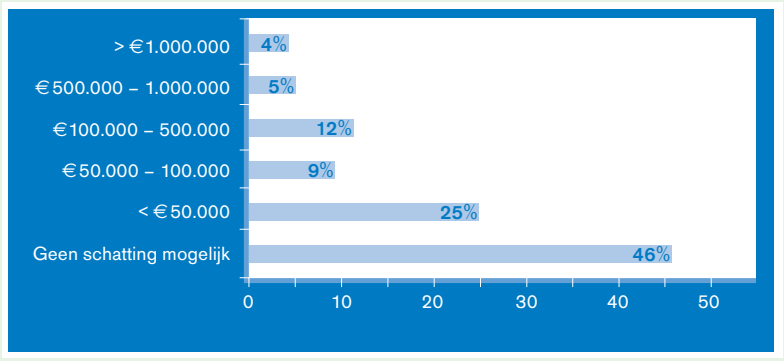
Vaak wordt door ondernemers, evenals in de politiek, kortetermijnresultaat geprefereerd boven continuïteit op lange termijn. Onderzoek wijst uit dat veertig procent van de organisaties die een grote calamiteit meemaken, na twee jaar niet meer bestaat ([Whea01]). Maar, 'De kans dat die calamiteit zich voordoet terwijl ik het hier voor het zeggen heb is zo klein ... ondernemen betekent nu eenmaal risico's nemen.' Zeker als de budgetten en persoonlijke posities onder zware conjuncturele druk staan, is de verleiding groot om te zwichten voor deze gedachten. Maar deze omstandigheden mogen geen excuses zijn om geen aandacht aan continuïteitsvoorzieningen te besteden. Niet voor organisaties die van belang zijn voor het functioneren van maatschappelijk vitale processen en te maken hebben met een overvloed aan regelgeving, zoals banken, telecommunicatiebedrijven, politie, justitie en socialezekerheidsinstanties, maar ook niet voor andere organisaties. Elke organisatie heeft te maken met partijen die in mindere of meerdere mate belang hebben bij of zelfs afhankelijk zijn van een zo ongestoord mogelijke voortzetting van haar bedrijfsvoering. Te denken valt in dit verband natuurlijk aan klanten, maar ook aan leveranciers, werknemers en hun families, verzekeraars, aandeelhouders en andere kredietverstrekkers. Deze afhankelijkheid is de afgelopen decennia toegenomen, en neemt nog steeds toe, onder andere door de invloed van schaalvergroting en de ketenintegratie die in veel sectoren heeft plaatsgevonden. Door deze schaalvergroting en ketenintegratie stijgen ook de kosten van uitval van bedrijfsprocessen. Deze kosten bestaan onder andere uit (indeling naar Gartner) ([Dot02]):

- *omzet*: direct omzetverlies, toekomstig omzetverlies, schadevergoedingen, contractuele verplichtingen, factuuratieverliezen;
- *productiviteit*: het aantal medewerkers maal het aantal uren waarin niet kan worden gewerkt;
- *reputatieschade*: bij klanten, leveranciers, aandeelhouders, banken en andere zakenpartners;
- *financiële schade*: inboedel, gemiste kortingen, betalingsgaranties, kredietwaardigheid en beurswaarde;
- *overige kosten*: juridische bijstand, tijdelijke medewerkers, huur van noodvoorzieningen, overuren, transportkosten, reiskosten.

> 'Companies have two choices: They can do little to prepare for disruptions and use the money they would have spent on a business continuity plan for other projects, or they can see business continuity as an investment.'
> *Todd Gordon, general manager of IBM Global Services' business continuity and recovery services ([Info01])*

Uit onderzoek blijkt dat verstoringen van de bedrijfsvoering in bijna zestig procent van de gevallen te wijten zijn aan verstoringen in de IT-voorzieningen ([Sain]). Dit percentage is een gemiddelde van verschillende soorten bedrijven, zowel hoog- als laaggeautomatiseerd, maar het is duidelijk dat veel organisaties voor hun bedrijfsvoering afhankelijk zijn van goed functionerende IT-voorzieningen. Deze stelling wordt bevestigd door een onderzoek dat in 2002 door KPMG Information Risk Management onder relaties is uitgevoerd ([Scho03]). De inschatting van de kosten van uitval door deelnemers aan dit onderzoek voor hun eigen organisaties is weergegeven in figuur 1.

Genoeg over de noodzaak van continuïteitsvoorzieningen vanuit het oogpunt van de gevolgen van uitval, deze zal het risicobewuste management genoegzaam bekend zijn. Interessanter is het om nader te beschouwen hoe aan de ene kant een organisatie ervoor kan zorgen dat continuïteitsmanagement zoveel mogelijk financiële voordelen oplevert, en aan de andere kant, op welke manier de kosten kunnen worden beperkt.



Figuur 1. Schatting van kosten per uur van uitval van bedrijfsprocessen (bron: KPMG Information Risk Management, 2002).

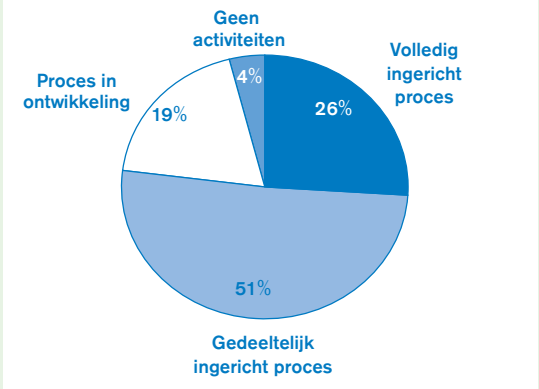
De aanpak

Bedrijfscontinuïteit als strategisch voordeel

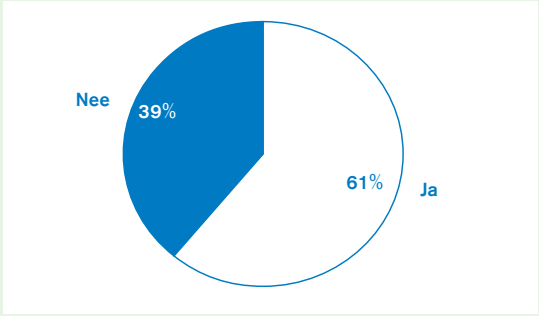
In een ideale organisatie zijn alle investeringen en bedrijfsactiviteiten direct of indirect gericht op het waarmaken van de missie en strategische doelstellingen. Investeringen die daar in mindere mate aan bijdragen zouden een lagere prioriteit toegekend moeten krijgen dan investeringen die daaraan in hoge mate bijdragen. In het kader van dit artikel is nu de vraag in hoeverre een hoge mate van continuïteit van dienstverlening – waaronder ook het begrip beschikbaarheid (*availability*) valt – onderdeel kan en moet uitmaken van de strategische doelstellingen, en dus investeringen waard is. Bij het hierboven aangehaalde Nederlandse KPMG-onderzoek uit 2002 gaf slechts 26 procent van de respondenten aan het proces van continuïteitsmanagement volledig te hebben ingericht (en 51 procent gaf aan het proces gedeeltelijk te hebben ingericht), terwijl 61 procent van de respondenten knelpunten bij de realisatie ervan signaleerde (zie figuur 2 en 3). Dertig procent gaf aan niet over een continuïteitsplan te beschikken. De *Global Information Security Survey 2003* van Ernst & Young ([Erns03]) bevestigt dit beeld: slechts tweederde van de deelnemers aan dit onderzoek meende in geval van een calamiteit de bedrijfsprocessen voort te kunnen zetten. Deze cijfers onderstrepen dat er voor organisaties voorlopig nog genoeg gelegenheid is om zich in positieve zin in de markt te onderscheiden door 'er gewoonweg te zijn voor hun klanten wanneer die hun diensten nodig hebben'. Continuïteit is blijkbaar een serviceaspect dat slechts een gedeelte van de organisaties tot op heden aan klanten kan bieden. Dit betekent dat continuïteit vooralsnog kan worden ingezet als strategisch wapen in de strijd om de gunst van de klant en/of burger. Hierbij moet wel worden opgemerkt dat de mate waarin continuïteit is ingericht per sector verschilt ([Mans03]). Continuïteit van dienstverlening heeft zich inmiddels in veel sectoren ontwikkeld tot een *conditio sine qua non*. Dit heeft niet op de laatste plaats te maken met de meer of minder imperatieve richtlijnen die in veel maatschappelijk vitale sectoren zoals de bancaire sector van kracht worden op het gebied van continuïteit. Continuïteit is dus voor veel organisaties geen strategische keuze, maar een *must*.

Bedrijfscontinuïteit in relatie tot economisch kapitaal

Dat continuïteit voor veel bancaire organisaties geen strategische keuze maar financiële noodzaak is, wordt evident in het Basel II Capital Accord voor banken. Het Basel II Capital Accord is de opvolger van het Basel I Capital Accord uit 1988 en is opgesteld door de Bank of International Settlements (BIS). Het Basel II Capital Accord bepaalt de hoogte van het economisch kapitaal dat een bank dient aan te houden in relatie tot de kredietrisico's, marktrisico's en operationele risico's die zij loopt. De doelstelling van economisch kapitaal is om de business te financieren en tevens als buffer te dienen tegen onverwachte verliezen. Zulke onverwachte verliezen kunnen voortkomen uit operationele gebeurtenissen



Figuur 2. Status van BCM-activiteiten in Nederlandse bedrijven (bron: KPMG Information Risk Management, 2002).



Figuur 3. Mate waarin zich knelpunten voordoen bij realisatie van BCM in Nederlandse bedrijven (bron: KPMG Information Risk Management, 2002).

zoals het uitvallen van informatiesystemen, brand, of andere vormen van calamiteiten. Het verband tussen continuïteitsmanagement en economisch kapitaal is duidelijk. Immers, effectief continuïteitsmanagement kan ervoor zorgen dat een operationele calamiteit wordt voorkomen of dat de ernst van een operationele gebeurtenis kan worden beperkt.

In het kader van dit artikel kan niet uitvoerig worden ingegaan op het Basel II Capital Accord. In het Basel II-raamwerk worden drie hoofdcategorieën van risico's beschreven:
1. kredietrisico;
2. operationeel risico;
3. marktrisico.

Als onderdeel van operationeel risico wordt in het Basel II Capital Accord nader ingegaan op continuïteitsmanagement. Operationeel risico wordt door BIS gedefinieerd als:

'Het risico van verliezen als gevolg van inadequate of falende interne bedrijfsprocessen, mensen en systemen of als gevolg van externe omstandigheden.'

Binnen het Basel II Capital Accord zijn er zogenaamde *loss events* gedefinieerd welke een direct effect hebben op het economisch kapitaal dat hiervoor opzij gelegd dient te worden. Deze typen *loss events* zijn in tabel 1 omschreven.

Uit tabel 1 blijkt dat sommige *loss events* ('Damage to physical assets', 'Business disruption and system failures') direct te koppelen zijn aan continuïteitsmanagement. Banken dienen gegevens over deze *loss events* te verzamelen, analyseren en modelleren. Het economisch kapitaal dat voor deze verliezen opzij dient te worden gezet door een bank kan echter worden verkleind. Door uit te gaan van effectieve modelleringstechnieken kan inzicht worden verkregen in de risico's waaraan een bank daadwerkelijk is blootgesteld, ten aanzien van de bovenstaande mogelijke *loss events*, en kan het continuïteitsprogramma effectiever en efficiënter worden ingericht.

Uit het bovenstaande kan worden afgeleid dat het hebben van inzicht in risico's en adequate back-up- en continuïteitsvoorzieningen een positieve impact kan hebben op het kapitaalbeslag van een bank. Er worden door BIS echter wel strikte eisen gesteld aan de continuïteitsvoorzieningen en het continuïteitsmanagement van een bank. Deze eisen zijn formeel gedefinieerd in de zogenaamde *Sound Practices for Operational Risk* behorende bij het Basel II Capital Accord.

Bedrijfscontinuïteit als onderhandelingsargument

Het treffen van de juiste continuïteitsmaatregelen zorgt ervoor dat belangrijke operationele risico's worden beperkt. En een reductie van risico's is iets waarbij niet alleen de eigen organisatie, maar ook andere belanghebbenden zijn gebaat. Het levert dus een versterkte onderhandelingspositie op. En deze moet worden benut! Een duidelijk voorbeeld van een organisatie die dit heeft omgezet in financieel voordeel, is beschreven in de casus behandeld in kader 1. Deze versterkte onderhandelingspositie kan ook op andere manieren worden verzilverd: denk bijvoorbeeld aan gunstige rente voor kredieten, de mogelijkheid om vooruit te factureren of meer leverancierskrediet te bedingen, het verdienen van de informele status van 'preferred supplier' in de afzetmarkt, en het vergroten van de aantrekkingskracht op de arbeidsmarkt.

Van maatregelen naar management: Business Continuity Management

Toegegeven, continuïteitsmaatregelen vormen een kostenpost. Deze kosten moeten worden beheerst en afgewogen, met andere woorden het efficiencyaspect mag niet uit het oog worden verloren. Dit is één van de redenen om verder te kijken dan technische, bouwkundige en organisatorische maatregelen op zich. Bedrijfscontinuïteit moet worden *gemanaged:* er moet een continuïteitsstrategie worden geformuleerd op basis van risico's en kosten-batenanalyse, maatregelen moeten op beheerste wijze worden ontworpen en geïmplementeerd, er moet onderhoud en evaluatie plaatsvinden. Met andere woorden, er moet een managementcyclus voor bedrijfscontinuïteit worden ingericht en op gang worden gehouden.

Loss event	Description
Internal fraud	Losses due to acts of a type intended to defraud, misappropriate property or circumvent regulations, the law or company policy (excluding diversity/discrimination events) which involve at least one internal party.
External fraud	Losses due to acts of a type intended to defraud, misappropriate property or circumvent the law, by a third party.
Employment practices and workplace safety	Losses arising from acts inconsistent with employment, health or safety laws or agreements, from payment of personal injury claims, or from diversity/discrimination events.
Clients, products and business practices	Losses arising from an unintentional or negligent failure to meet a professional obligation to specific clients (including fiduciary and suitability requirements), or from the nature or design of a product.
Damage to physical assets	Losses arising from loss or damage to physical assets caused by natural disaster or other events.
Business disruption and system failures	Losses arising from disruption of business or system failures.
Execution, delivery and process management	Losses from failed transactions processing or process management, from relations with trade counterparties and vendors.

Tabel 1. Typen loss events.

Kader 1. Continuïteitsplanning leidt tot kostenbesparing en is strategische randvoorwaarde.

Een logistieke dienstverlener nam het initiatief om een continuïteitsplan op te laten stellen en te implementeren voor de belangrijkste logistieke processen. De organisatie wil in geval van een storing of calamiteit beter in staat zijn de dienstverlening weer binnen acceptabele tijd te herstellen en zodoende de continuïteit van de onderneming en de belangen van alle belanghebbenden te waarborgen. Deze doelstelling was direct afgeleid van de missie van de onderneming, waarvan de kern was dat klanten moesten kunnen rekenen op continue, tijdige en foutloze dienstverlening. Het invoeren van het continuïteitsplan was derhalve een activiteit van groot strategisch belang.
Maar naast het strategische voordeel heeft het project de organisatie forse kostenbesparingen opgeleverd. Dit was mogelijk doordat de organisatie het continuïteitsplan heeft ingezet als wapen in de onderhandelingen met haar verzekeringsmaatschappij. Dit heeft geresulteerd in een reductie van de premie voor de afgesloten bedrijfsschadeverzekering.

Hieraan wordt in veel organisaties invulling gegeven onder de naam Business Continuity Management (BCM).

KPMG Information Risk Management onderscheidt ten aanzien van BCM drie elementen, waarop tevens de indeling voor het laatste gedeelte van dit artikel is gebaseerd. Het betreft de volgende elementen ([Scho03]), die ook zijn weergegeven in figuur 4:

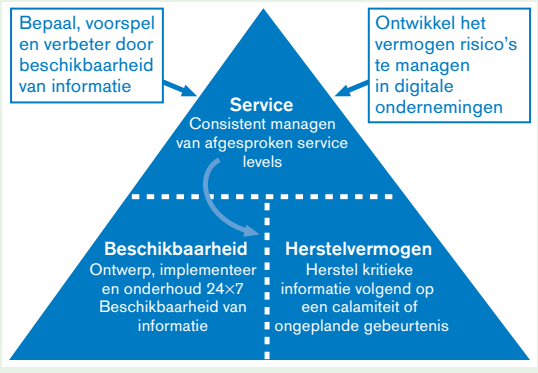
Herstelvermogen
Dit element omvat het ontwerp en de implementatie van voorzieningen om te zorgen voor snel herstel van de beschikbaarheid van de informatievoorziening na het optreden van een calamiteit. Activiteiten die hierbij horen zijn Disaster Recovery Planning (DRP) en Business Continuity Planning (BCP). De essentie van deze begrippen is dat een organisatie zich voorbereidt op herstel van respectievelijk de informatiesystemen – bij DRP – en de bedrijfsvoering – bij BCP – na het optreden van een calamiteit. Beide activiteiten zijn primair gericht op het minimaliseren van het gevolg van een calamiteit, en in mindere mate op het minimaliseren van de kans van optreden, en daarom vooral reactief van aard. Herstelvermogen zegt dus iets over de mate waarin een organisatie zich heeft voorbereid op 'buitengewone omstandigheden' zoals een aardbeving, overstroming, terroristische aanslag of grote brand.

Door het effectief inrichten van het herstelvermogen kan een organisatie de tijd die nodig is voor herstel van de informatiesystemen, de bedrijfsprocessen en de dienstverlening verkorten. Concreet betekent dit dat technische of contractuele voorzieningen worden getroffen – zoals het inrichten van een uitwijklocatie voor de apparatuur en het huren van redundante dataverbindingen – en dat een calamiteitenorganisatie wordt ingericht en voorzien van nood-, uitwijk- en herstelprocedures.

Met het oog op efficiëntie – en dus een beperking van de kosten van het inrichten en onderhouden van het herstelvermogen – zou een organisatie de volgende punten in overweging moeten nemen:

* Het is vanuit kostenoogpunt van belang dat investeringen volledig zijn gerechtvaardigd op basis van de bedrijfsdoelstellingen. Zo is het voor sommige systemen vaak niet nodig om een uitwijkfaciliteit te hebben, aangezien deze activiteiten handmatig kunnen worden verricht of op een later tijdstip. Ook dient het aantal beschikbare werkplekken bij de uitwijkfaciliteit optimaal te zijn afgestemd op de behoeften van de proceseigenaren. Het beschikbaar houden van te veel werkplekken en het inrichten van een te hoog herstelvermogen in relatie tot het belang van systemen voor de bedrijfsvoering (bijvoorbeeld het realiseren van *hot-stand-by* faciliteiten voor niet-kritieke systemen) leidt vaak tot onnodige kosten. Dit pleit voor het uitvoeren van een gedegen risicoanalyse, afhankelijkheidsanalyse en een business impactanalyse, en voor serieuze betrokkenheid van het verantwoordelijke management (systeem- en proceseigenaren) alvorens wordt overgegaan tot het gericht treffen van continuïteitsmaatregelen. Bij het inrichten van een uitwijkfaciliteit moet natuurlijk prioriteit worden toegekend aan kritieke informatiesystemen en bedrijfsprocessen, maar aandacht is vereist voor de afhankelijkheid van systemen of componenten die op het eerste gezicht onbelangrijk lijken. Zo zijn gevallen bekend waarin het verlies van één enkele pc met cruciale gegevens heeft geleid tot een faillissement.

* Het spreekt voor zich dat de getroffen technische en organisatorische voorzieningen moeten worden onderhouden en dat ermee moet worden geoefend, om te waarborgen dat deze effectief zijn op het moment dat zij nodig zijn. Daarnaast leidt structureel onderhoud van voorzieningen tot beperking en spreiding van de kosten. Deze stelling komt voort uit het feit dat met het periodiek toetsen en bijwerken van continuïteitsplannen en het inbedden van het onderhoud van voorzieningen en plannen in het reguliere change-managementproces kan



Figuur 4. Drie elementen van Business Continuity Management.

worden voorkomen dat de organisatie telkens na een aantal jaren van verandering in één keer 'groot onderhoud' moet uitvoeren dat leidt tot hoge uitgaven. De omgeving, de organisatie en de techniek veranderen zo snel dat in de praktijk in zo'n geval de bestaande plannen (hopelijk ongebruikt) de prullenbak in gaan en helemaal opnieuw moet worden begonnen. En daarvoor worden dan in het algemeen forse projecten geïnitieerd, die de organisatie veel tijd en inzet van externe medewerkers kosten. Structureel onderhoud kan deze hoge kosten voorkomen, en verhoogt bovendien de effectiviteit van de voorzieningen.

* Ook geldt dat goede planning van continuïteitsprojecten voor kostenbeheersing van belang is. In de praktijk blijkt dat een project onder grote tijdsdruk doorgaans kostbaarder is dan een project zonder grote tijdsdruk ([Hile01]). Dit is gemakkelijk te verklaren: een project onder tijdsdruk is niet of moeilijk door de organisatie zelf te dragen, zodat een grote inzet van externe medewerkers nodig is. Een kortere doorlooptijd en beperkte betrokkenheid van interne medewerkers impliceren ook dat meer kosten moeten worden gemaakt om de plannen 'tussen de oren' te krijgen. Ten slotte kan tijdsdruk de onderhandelingspositie tegenover leveranciers van continuïteitsdiensten en technische voorzieningen nadelig beïnvloeden, wat zich vertaalt in hogere prijzen.

* Veel organisaties hebben zelf beperkte kennis en ervaring in huis met betrekking tot het inrichten van herstelvermogen. Kostbare beginnersfouten en onnodig werk kunnen worden voorkomen door gebruik te maken van de ervaringen van andere organisaties. Dit kan worden gerealiseerd door kennis en voorbeeldmateriaal uit te wisselen met vergelijkbare bedrijven, of door ervaren specialisten op het gebied van continuïteitsmanagement in te zetten.

Beschikbaarheid

Beschikbaarheid staat voor het ontwerp en de implementatie van een veerkrachtige infrastructuur, onderbouwd door sterk ICT-beheer. Het begrip dat hierbij hoort is Enterprise High Availability (EHA). Het houdt in dat de organisatie zorgt voor beschikbaarheid van systemen en processen door zich voor te bereiden op (kleinere) verstoringen van de informatiesystemen en/of bedrijfsprocessen onder 'normale omstandigheden', dat wil zeggen situaties waarin (nog) geen sprake is van een calamiteit. Activiteiten zijn zowel gericht op het minimaliseren van de kans van optreden als op het minimaliseren van de gevolgen, en zijn daarom zowel reactief als preventief. Het inrichten van beschikbaarheid betreft technische en bouwkundige maatregelen – zoals het stand-by houden van redundante verwerkingscapaciteit, opslag van gegevens en dataverbindingen, een installatie die ervoor zorgt dat een beginnende brand vroegtijdig wordt gesignaleerd en geblust – en organisatorische maatregelen. Voorbeelden van organisatorische beschikbaarheidsmaatregelen zijn het inrichten en/of professionaliseren van beheerprocessen zoals problem management, incident management, change management en availability management, maar ook het invoeren van gedragsregels die zijn gericht op het voorkomen van uitval, zoals een rookverbod in technische ruimten.

Onder herstelvermogen is een aantal punten genoemd die van belang zijn voor het beperken van de kosten die gepaard gaan met de inrichting ervan: maatregelen moeten steeds zijn afgestemd op het belang van processen en systemen, de voorzieningen moeten worden onderhouden en periodiek worden getest, projecten moeten zorgvuldig worden gepland, en er moet zoveel mogelijk gebruik worden gemaakt van de kennis en ervaringen van andere organisaties. Alle genoemde punten zijn ook van toepassing op de inrichting van beschikbaarheid. Bij het inrichten van beschikbaarheid is in aanvulling daarop nog het nu volgende aspect van consolidatie en duplicatie van belang.

Consolidatie van gegevensopslag en mirroring

Het inrichten van beschikbaarheid van data wordt vaak gerealiseerd door middel van consolidatie en duplicatie (mirroring) van data, bijvoorbeeld in de vorm van een SAN (storage area network). Dit houdt in dat dezelfde gegevens worden opgeslagen op enkele grote, fysiek gescheiden machines, liefst op twee verschillende locaties. Via een glasvezelverbinding wordt continu de data van de ene naar de andere locatie gekopieerd. Mocht zich op locatie A een grote storing of kleine calamiteit voordoen, dan kan in het ideale geval direct worden overgeschakeld op de data op locatie B. Deze oplossing is populair, hoewel er ook nadelen aan kleven: zo is de maximale afstand tussen locatie A en B beperkt, zodat de kans bestaat dat een calamiteit beide locaties tegelijkertijd treft, en beschermt de oplossing bijvoorbeeld niet tegen corrupte databases, de gegevens zijn namelijk identiek op beide locaties. Een groot voordeel van het consolideren van gegevensopslag op twee locaties is dat naast een hoge beschikbaarheid ook forse kostenvoordelen kunnen worden gerealiseerd. Een voorbeeld hiervan laat de casus in kader 2 zien. De belangrijkste kostenvoordelen die doorgaans met een consolidatie van gegevensopslag kunnen worden gerealiseerd, komen voort uit:

* vermindering van de beheer- en onderhoudslast (FTE's) ten aanzien van de voorzieningen voor gegevensopslag;
* vermindering van de hoeveelheid ongebruikte opslagcapaciteit die moet worden aangehouden (in verband met schaalbaarheid van de opslagcapaciteit);
* vermindering van huisvestingskosten voor apparatuur.

Een productiemaatschappij heeft besloten om haar servers en overige apparatuur, verspreid over een aantal fysieke datacenters, te centraliseren in slechts twee fysieke datacenters, waarbij de beide datacenters tevens als elkaars back-up functioneren.
Hiertoe zijn beide datacenters verbonden met redundante datacommunicatieverbindingen. De organisatie is tot dit besluit gekomen vanwege overcapaciteit in de oorspronkelijke datacenters en om beter in staat te zijn in geval van een storing of calamiteit de dienstverlening binnen acceptabele tijd te herstellen. Er dienen nu immers slechts maatregelen voor twee datacenters te worden getroffen. Tevens zijn de eerste kostenbesparingen reeds gerealiseerd op de volgende gebieden:

* Er zijn contractvoorwaarden onderhandeld met businesspartners die gunstiger zijn dan voorheen.
* Er vindt hergebruik van reeds aanwezige stroomapparatuur en koelingsapparatuur plaats.
* Vanwege een modulaire stroomtoevoer zijn de onderhoudskosten lager.

Kader 2. Integratie van datacenters leidt tot kostenbesparing.

Bij het realiseren van consolidatie en mirroring van gegevensopslag is het ten slotte vanuit kostenoogpunt van belang om zodanig te plannen dat de realisatie van de nieuwe infrastructuur plaatsvindt op een moment dat een groot gedeelte van de bestaande systemen toch al aan vervanging toe is (technisch en/of economisch is afgeschreven).

Service
Dit element houdt in het zodanig inrichten van de bedrijfsprocessen en de informatievoorziening dat de wensen van de klanten en de gerealiseerde *service levels* continu worden gemeten en met elkaar worden vergeleken, en de dienstverlening hierop proactief wordt aangepast. Hierbij hoort de activiteit Service Level Management (SLM). Het proces Service Level Management is ten aanzien van continuïteitsmanagement noodzakelijk om te waarborgen dat de niveaus van herstelvermogen en beschikbaarheid blijven aansluiten op de behoeften van de gebruikersorganisatie. Daarmee draagt het bij aan de efficiëntie van continuïteitsvoorzieningen. Het proces Service Level Management zal in dit artikel niet verder worden uitgewerkt. Voor de inrichting van het proces kan bijvoorbeeld worden aangesloten op het bekende ITIL-raamwerk van beheerprocessen.

Conclusie

Economische malaise dwingt het management van organisaties om extra kritisch te kijken naar de uitgaven en uitsluitend te investeren indien er besparingen of een verhoging van de opbrengsten tegenover staan. Ten aanzien van bedrijfscontinuïteit bestaan er veel mogelijkheden om hierbij te ondersteunen, hoewel de voordelen niet altijd op zeer korte termijn kunnen worden geïncasseerd. Enerzijds is het mogelijk kosten te besparen bij de inrichting en het onderhoud van continuïteitsvoorzieningen door met een aantal aspecten rekening te houden. Anderzijds kan een organisatie op veel gebieden voordeel halen uit de getroffen voorzieningen. Veel van deze voordelen kunnen leiden tot kostenbesparingen op allerlei gebieden en tevens de omzet verhogen, maar vaak blijven de mogelijkheden daartoe in de praktijk onbenut.

Literatuur

[Dot02]
Achieving 99.9998+% Storage Uptime and Availability, Dot Hill Systems Corp., januari 2002.

[Erns03]
Global Information Security Survey 2003, Ernst & Young, 2003.

[Hile01]
Andrew Hiles & Peter Barnes, *The Definitive Handbook of Business Continuity Management*, 2001.

[Info01]
Information Week, 2 March 2001.

[Mans03]
Ir. K. Manschot en drs. J.W.R. Schoemaker, *De stand van zaken in Nederland*, Controllers Journaal, 20 februari en 6 maart 2003.

[Sain]
Lord Sainsbury, parliamentary under-secretary of state for Science and Innovation, *'A government lead' Business Continuity, Helping Directors build a strategy for a secure future*, Institute of Directors – A Director's Guide series.

[Whea01]
Vic Wheatman, *'Aftermath: Disaster Recovery'*, GartnerGroup, September 21, 2001.

Ir. A.T. Wijsman
is als IT-adviseur en -auditor werkzaam bij KPMG Information Risk Management. Zijn primaire aandachtsgebieden zijn risico- en continuïteitsmanagement en organisatorische en beheeraspecten van informatiebeveiliging.

wijsman.antoine@kpmg.nl

Drs. M.R. Verhoef RE
is als manager werkzaam bij KPMG Information Risk Management en medeverantwoordelijk voor de dienstverlening van KPMG op het gebied van Business Continuity Management. Hij heeft uitgebreide ervaring met risico- en continuïteitsmanagement en het beoordelen van (IT-gerelateerde) systemen en processen.

verhoef.marcel@kpmg.nl