Business Continuity Management (BCM)

NIET VERRAST WORDEN DOOR HET ONVERWACHTE

Business Continuity Management (BCM) gaat over het beschermen van uw onderneming tegen de gevolgen van omvangrijke verstoringen en (on)bekende risico's. Dit is anno 2015 geen overbodige luxe. Vele ondernemers denken niet voldoende na over hoe ze een calamiteit gestructureerd dienen aan te pakken en te overleven, terwijl de risico's zich voor menige sector ontwikkelen in een ongunstige richting. ISO 9001 (kwaliteit) en ISO 14001 (milieuzorg) zijn inmiddels bekende normen binnen ondernemingen. De 2015 versies van beide normen leiden voor iedereen tot een herijking van de bestaande en implementering van de nieuwe eisen in dat kader. Dit tweetal is echter, met in het vizier tevens het `Risk Based Thinking´ thema van de vernieuwde ISO 9001:2015-standaard, te verrijken door direct aan het bestaande managementsysteem Business Continuity Management toe te voegen, wel of niet gecertificeerd conform ISO 22301. Een op z'n minst gezegd 'interessante gedachte'. Maar het gaat niet sec om de certificaten, het gaat om de meerwaarde hiervan.

Door Gert Kogenhop, bcm+

Verkoop, productie, logistiek: eigenlijk alle functies binnen de onderneming zijn voornamelijk bezig met de dagelijkse uitvoering activiteiten, de plannen opgesteld door het management, de huidige en wellicht toekomstige orders... De aandacht is minder gericht op bekende en onbekende risico's die het voortbestaan van de onderneming ernstig kunnen bedreigen. Het halen van de (financiële) doelstellingen staat bovenaan elke agenda en dat is vanzelfsprekend begrijpelijk. Business Continuity – oftewel in goed Nederlands *bedrijfscontinuïteit* – en dan natuurlijk iets specifieker het managen hiervan, verdient zeker een meer prominente plek op diezelfde agenda dan momenteel het geval is. Indien de continuïteit van de onderneming in gevaar komt als direct gevolg van een ernstig incident, komen clichés als: 'Hadden we maar ....' naar voren, helaas dan té laat.

> 'ONDER DE HUIDIGE ECONOMISCHE OMSTANDIGHEDEN ZIJN VEEL BEDREIGINGEN ACTUELER DAN OOIT'

Bedrijfscontinuïteit kan worden omschreven als het vermogen van een organisatie om *te plannen voor* en *te reageren op* incidenten met als direct gevolg een ernstige verstoring van de organisatie, om zodoende te waarborgen dat men operationeel op minimaal een van tevoren vastgelegd niveau kan functioneren. BCM dientengevolge is het complete management *proces* dat mogelijke gevaren met betrekking tot de continuïteit van de bedrijfsvoering vaststelt en een kader schept voor het opbouwen van weerstandsvermogen en veerkracht. Door effectief reageren worden de organisatiebelangen, de reputatie alsmede het merk bewaakt. Tevens wordt de uitvoering van de waarde creërende activiteiten gewaarborgd.

GENOEG VOORBEELDEN

Binnen de ICT is het managen van continuïteit dé nummer één prioriteit. Sterker nog, wij eisen van de ICT-functie binnen onze organisatie minimaal 99,99% betrouwbaarheid en 'up-time' en zeker ook wanneer deze is uitbesteed aan een derde partij. Er mag niets gebeuren en als er iets gebeurt, moeten we zo snel mogelijk verder kunnen zonder al te veel vertraging en dataverlies. Het antwoord van de ICT-functie op deze (terechte) eisen is dat er onder andere back-up procedures zijn ontwikkeld en dezelfde 'realtime data' op verschillende plaatsen (in de wereld) beschikbaar is gemaakt.

De afgelopen jaren is men zich gaan realiseren dat dit eigenlijk zou moeten gelden voor alle belangrijke functies binnen de organisatie. Engeland loopt daarin duidelijk voorop. Het land heeft rond de eeuwwisseling in korte tijd een groot aantal rampen en bijna-rampen te verwerken gekregen. Denk hierbij bijvoorbeeld aan de enorme brand bij Hemel Hempstead in december 2005 (Hertfordshire Oil Storage Terminal), de diverse overstromingen waarmee men te kampen heeft gehad, de terroristische aanslagen en de gevallen van gekke koeienziekte, vogelgriep en mond- en klauwzeer. In het geval van de enorme brand in Hemel Hempstead is uiteindelijk driekwart van de bedrijven op het aangrenzende bedrijventerrein failliet gegaan als direct aanwijsbaar gevolg hiervan. Ook vliegveld Heathrow ondervond direct nadelige gevolgen van deze brand, daar een zeer groot deel van de benodigde kerosine door dit getroffen bedrijf werd geleverd.
Wat we hiervan kunnen leren is

Jaarlijks € 700 miljoen schade grote branden

Steeds meer stroomstoringen. Gemiddelde duur 26 minuten

In 2014: 7.600 bedrijven failliet. Uw klanten of leveranciers?

Grootste bedreigingen 2015: ICT-uitval, hacking & Cyber Crime

Beperking van de schade

Na verstoring weer snel op gang

Tijdig anticiperen op gevaar

Alternatieven direct bereikbaar

dat niet alleen het bedrijf zelf de nadelige gevolgen van een incident ondervindt, maar tevens onder andere buren, klanten en wellicht leveranciers die (voorlopig) een afnemer kwijt zijn. Dichter bij huis zijn daar ook voorbeelden genoeg van. De helikoptercrash in de Bommelerwaard enkele jaren geleden (dagenlang geen elektriciteit); de dreiging van een pandemie (nu wél opeens aandacht voor een continuïteitsplan); het voor langere tijd uitvallen van mobiel telefoonverkeer (regelmatig), elektriciteit (kort geleden nog in Noord-Holland) en Internet (bijvoorbeeld Ziggo na meerdere DDoS aanvallen in augustus). Denk echter ook aan de mogelijke gevolgen van een staking (ook een toename de laatste tijd); de beschikbaarheid en de prijsfluctuaties van belangrijke grondstoffen; die grote, trouwe relatie die niet meer voor u kiest of de overheid, die door veranderende regelgeving een behoorlijke spaak in het wiel steekt.

Op dit moment gaan zo'n 150 bedrijven per week failliet, waaronder niet ondenkbaar ooit een grote klant of die leverancier waarvoor u niet zo maar een alternatief heeft. Onder de huidige economische omstandigheden zijn veel bedreigingen actueler dan ooit. Wanneer u dit zo leest slaat de angst u wellicht om het hart en dat is misschien wel goed, zeker indien u niet goed voorbereid bent. Halsstarrig de andere kant op blijven kijken, de kop in het zand steken of denken: 'Dat overkomt mij niet' is in ieder geval geen verstandige strategie. De hierna omschreven aanpak helpt u wel bij het nemen van passende maatregelen.

DE AANPAK

In twee stappen analyseert u de organisatie. U gaat bijvoorbeeld uit van de voor de onderneming belangrijkste producten en/of

diensten. Nadat deze zijn vastgesteld worden alle activiteiten tegen het licht gehouden en die activiteiten geselecteerd, die een directe bijdrage leveren aan het tot stand komen van de belangrijkste producten en/of diensten middels een Business Impact Analyse (BIA). Deze activiteiten worden geanalyseerd en beoordeeld op gevoeligheid voor een aantal van tevoren vastgestelde bedreigingen, waaronder de eerder genoemde voorbeelden. Op deze wijze prioriteren we alle activiteiten en komen de meest kritische activiteiten naar voren en tegelijkertijd welke activiteiten best wel even kunnen stilliggen in geval van een calamiteit. De Risico Analyse (RA) geeft inzicht in welke risico's voor de onderneming reëel zijn – algemene risico's, risico's behorend bij de aard van de activiteiten (advocatenkantoor of chemieconcern) en de vestigingsplaats (nabij water, het spoor, tankstation aan de overkant, wie zijn de buren ...). Het gaat hier om de kans en de mogelijke impact van het feit dat een bedreiging een ernstige verstoring veroorzaakt. Niet alle risico's kunnen vanzelfsprekend worden uitgesloten. Er zal altijd een 'restrisico' blijven.

Wanneer het productieproces of de dienstverlening onverwacht stil valt kan men de gevolgen daarvan in de tijd gemeten grofweg onderverdelen in vier fasen. Des te langer het duurt, des te groter de schade. Wat gebeurt er bijvoorbeeld bij een producent van kunststof onderdelen voor de automobielindustrie die na een succesvol LEAN-traject alleen nog maar op order produceert en weinig tot geen voorraad heeft, gevestigd is in Noord-Holland en getroffen wordt door een stroomstoring? Als eerste ontstaat productiegerelateerde schade. De aangemaakte hoeveelheden halffabricaat of recepten in het productieproces kunnen wellicht niet langer worden gebruikt en moeten worden weggegooid en machines moeten worden ontdaan van materialen welke in het proces (vast)zitten, terwijl ook medewerkers met de armen over elkaar staan en niet productief zijn. Men heeft slechts een korte periode om zich te herstellen, anders komt de tweede fase van impact om de hoek kijken: het niet kunnen leveren van de eindproducten of misschien slechts een deel. Omzetschade is dan het directe gevolg.

Wanneer de stilstand langer voortduurt en er dagenlang niet kan worden geproduceerd, komt men in de derde fase terecht. Hier zien we de financiële impact escaleren met mogelijk contractuele boetes van klanten (de automobielbedrijven), daar zij ook met zeer kleine voorraden werken (Just-In-Time) en op uw leveringen rekenen, plus mogelijk cashflow-problemen omdat meerdere dagen niet is geproduceerd en geleverd en dus niet is gefactureerd. Indien men een bankkrediet heeft, zal de bank wellicht ook vragen hoe het er voor staat, om de spanningen nog maar even iets op te voeren. Voorts kan er nog sprake zijn van ernstige merk- en reputatieschade: de vierde fase. Het gaat dan om verloren vertrouwen bij allerlei betrokkenen, van banken tot aandeelhouders, van klanten en leveranciers tot personeelsleden. Wanneer men niet in staat is adequaat te reageren kan de continuïteit van de gehele onderneming serieus in gevaar komen. U kunt zelf ongetwijfeld een parallel trekken naar uw eigen organisatie.

Na bepaling van de 'gevaarlijke' combinatie van bedreigingen en de eerder vastgestelde activiteiten, die onze belangrijke producten en/of diensten ondersteunen, dienen de volgende mogelijkheden te worden overwogen:

1. Gaan we dit behandelen/afdekken in continuïteitsplannen (Treat)?
2. Accepteren we dit risico (Tolerate)?
3. Dragen we dit risico over aan derden middels uitbesteding of vorm van verzekering (Transfer)?
4. Beëindigen/opschorten/veranderen van deze activiteit (Terminate)?

Vervolgens wordt besloten 'Wat te doen' en nog belangrijker en uitermate krachtig: 'Hoe kunnen we het weerstandsvermogen en de veerkracht van de organisatie verhogen? Hoe kunnen we de kritische activiteiten minder kritisch maken en hoe kunnen we kans of impact van een bedreiging verlagen?' Het vinden van soms eenvoudige mogelijkheden gedurende en na de implementatie van BCM in de onderneming levert een enorme toegevoegde waarde. Het bijvoorbeeld tot de conclusie komen dat men enkele uitermate belangrijke medewerkers heeft rondlopen die specifieke kennis en vaardigheden bezitten (single point of knowledge), kan leiden tot de beslissing om de vastlegging van procedures en werkvoorschriften nóg strakker te organiseren en tevens de implementatie van bijvoorbeeld plannen met betrekking tot opvolging, kennisdeling en rouleren van medewerkers tot gevolg hebben. Ander voorbeeld: het vaststellen van het feit dat u voor enkele belangrijke grondstoffen of diensten slechts één leverancier heeft (single sourcing) en dat alternatieven nodig zijn lijkt een open deur, maar is dat voor veel ondernemers niet. Zeer regelmatig komt het voor dat er van een belangrijke machine slecht één exemplaar aanwezig is (single point of failure). Ook een niet te onderschatten situatie wanneer deze langere tijd niet kan functioneren. Al deze activiteiten dienen te worden opgenomen in een separaat actie/verbeterplan met stappen, eigenaren en deadlines, indien nodig voorzien van een budget. Het beheren van het hier geproduceerde 'Weerstandsvermogen en Veerkracht Plan' is een wezenlijk onderdeel van de succesvolle implementatie van BCM binnen de onderneming.

> 'ZORG ERVOOR DAT U NOOIT ONAANGENAAM VERRAST WORDT EN DE CONTROLE VERLIEST!'

HEEFT U ÉCHT GOED INZICHT IN DE RISICO'S ROND UW BELANGRIJKSTE LEVERANCIERS?

De invulling met betrekking tot 'Wat vervolgens te doen?' wordt in een belangrijke mate bepaald door een aantal factoren. Ten eerste welke activiteiten (met de juiste prioriteit) betreft het? En vervolgens welke (en hoeveel) mensen en middelen zijn nodig om deze uit te kunnen voeren?

Tevens is het van het grootste belang te weten wat de maximaal toelaatbare periode van de ernstige verstoring mag zijn, oftewel na welk moment in de tijd gemeten heeft doorgaan geen zin meer en kunt u beter energie steken in andere zaken. De laatste factor is het minimale activiteitenniveau waarop u tijdelijk kunt functioneren. U hoeft niet altijd direct 100% te functioneren, maar voor welk percentage dan wel? Met welke machines en bezetting, welke producten of diensten voor welke klanten? Gaan bepaalde klanten voor, of wilt u uw producten in een bepaalde volgorde produceren of wilt u eerst bepaalde processen hebben draaien? Allemaal legitieme vragen die u toch liefst voor dat iets ernstig gebeurt duidelijk wilt hebben om de juiste herstelstrategie te kunnen uitvoeren.

Naast het genoemde Weerstandsvermogen en Veerkracht Plan worden diverse scenario's uitgewerkt met de kritische activiteiten (uit de Business Impact Analyse) als eerste prioriteit, op basis van de grootste bedreiging (uit de Risico Analyse). Eenvoudig gesteld zijn dit scenario's met als uitgangspunt: 'Hoe leveren wij onze klanten zo snel mogelijk in de volgende situaties':

- Uitval van ICT;
- Stroomuitval (of water/gas);
- De locatie is onbereikbaar (wegafsluiting, afgebrand, explosiegevaar bij de buren...);
- ...

En niet direct productiegericht: 'Hoe overleven wij als onderneming in geval van':

- Een grote terugroepactie van ons product;
- Het verlies van een grote klant, order of tender;
- Het verlies van een belangrijke (product)certificering;
- ....

Hoe goed bent u voorbereid op brandschade ...

Langdurige stroomstoring ...

Of uitval van ICT?

Uiteindelijk zijn we dan zo optimaal mogelijk voorbereid op een ernstige verstoring, ook al gebeurt er iets waar we nou nét níet een scenario voor hebben bedacht. De denk- en werkwijze zit nu in onze genen, dus u zult even verrast zijn, maar niet de controle verliezen.

ZORG ERVOOR DAT U NOOIT ONAANGENAAM VERRAST WORDT EN DE CONTROLE VERLIEST!

Uiteindelijk zult u wat is geproduceerd moeten oefenen en testen (samen met de bedrijfshulpverlening bijvoorbeeld), onderhouden en herzien (samen met andere normen indien van toepassing). Voorts is het verstandig dit regelmatig te laten auditeren en zeker de direct betrokkenen uit te dagen middels Key Performance Indicators (KPI's).

RELEVANT VOOR IEDEREEN

Het is duidelijk voor welke ondernemingen BCM relevant is, namelijk *alle*. Geen enkele onderneming, *lees directie*, mag zich onttrekken aan haar verantwoordelijkheid om al het mogelijke te doen aan de waarborging van de continuïteit van de onderneming. Tevens moet u het belang voor uw '*stakeholders*' niet vergeten of onderschatten. Vele bij de onderneming betrokken partijen zullen de inspanningen op dit gebied met vertrouwen en waardering ontvangen. Klanten, banken en verzekeraars, maar ook leveranciers en niet in de laatste plaats aandeelhouders en werknemers hebben baat bij een onderneming die er morgen ook nog is.

Als laatste – en zeker niet het minst belangrijke – moet erop gewezen worden dat in geval van ernstige bedrijfsschade of erger (faillissement of bedrijfsbeëindiging) de aandeelhouders en andere betrokkenen met een belang, mogelijk de correctheid van de handelswijze van bestuurders tijdens de calamiteit in twijfel kunnen trekken. 'Kennelijk onbehoorlijk bestuur' kan leiden tot individuele aansprakelijkheid van bestuurders op grond van bestuurdersaansprakelijkheid of zelfs onrechtmatige daad. Het mag duidelijk zijn dat wanneer de bestuurder kan aantonen dat BCM is geïmplementeerd en er een correcte en zorgvuldige uitvoering van de geproduceerde plannen heeft plaatsgevonden, men de kans (en impact) hierop uitsluitend positief beïnvloedt. Welke ondernemer kan het zich veroorloven dit onderwerp niet op de agenda te zetten? ■

OVER DE AUTEUR

Gert Kogenhop is directeur van bcm+, een bedrijf dat is gespecialiseerd in advies en implementatiebegeleiding van Business Continuity Management Systemen conform de norm ISO 22301 en leverancier van ClearView software. In samenwerking met de Security Academy worden diverse trainingsprogramma's verzorgd op dit gebied. Voor meer informatie kunt U terecht op www.bcmplus.nl of per e-mail: gk@bcmplus.nl.