Risicomanagement en Business Continuity Management dienen hetzelfde doel

RM EN BCM: WAT IS HET VERSCHIL?

Risk Management (RM) of Risicobeheer c.q. de ingeburgerde vertaling Risicomanagement, wordt op vele manieren gedefinieerd, maar is in dit verband het best te omschrijven als 'Activiteiten en methoden die worden gebruikt om risico's te beheersen die het vermogen om doelstellingen te bereiken kunnen beïnvloeden'. Een risico is vervolgens in dit kader 'Het effect van onzekerheid op het behalen van doelstellingen'. Business Continuity Management (BCM) – in goed Nederlands Bedrijfscontinuïteitsbeheer – gaat over het beschermen van uw organisatie tegen de gevolgen van omvangrijke verstoringen en (on)bekende risico's op uw vermogen om producten en diensten te kunnen leveren aan uw afnemers. Op dit 'Platform voor organisatieontwikkeling' is hier al meerdere malen uitgebreid aandacht aan besteed. Wat is het verschil tussen beiden en wat is de samenhang?

Door Gert Kogenhop, bcm+

Wanneer men dit heel plat slaat en er zo simplistisch mogelijk naar kijkt houdt RM zich bezig met de risico's, dus in deze context welke risico's kunnen leiden tot een ernstige verstoring van de bedrijfsactiviteiten die benodigd zijn voor het leveren van uw producten en diensten aan uw afnemers. Het analyseren van bedreigingen als brand, stroomstoring, IT-uitval of een pandemie, waardoor u onvoldoende handjes beschikbaar hebt bijvoorbeeld. Door de kans en de mogelijke impact te beoordelen komt men tot risico's. Vervolgens wilt u beperkende maatregelen nemen en op deze wijze optimaal sleutelen aan de kans op en de impact van – met een mooi woord – mitigeren en als gevolg daarvan deze risico's beheren en beheersen (auteur: mijn vertaling van managen).

Het mag duidelijk zijn dat veel bedreigingen algemeen zijn. Een heel simpele is het niet beschikbaar zijn van water, maar dat voornamelijk in het bepalen van de impact hiervan dit bedrijfsspecifiek wordt. Een bierbrouwer of groenteverwerker is enorm afhankelijk voor het leveren van zijn producten van de continue beschikbaarheid van voldoende schoon water voor het produceren van bier respectievelijk verpakte gesneden groenten die elke dag vers in de schappen van de supermarkt dienen te liggen. Bij een IT-dienstverlener of advocatenkantoor is de impact op de mogelijkheid tot dienstverlening nagenoeg nihil. Vervolgens zijn er heel specifieke bedreigingen; denk aan de voedingsindustrie en de kans en impact van een bacteriële besmetting zoals Listeria, E.coli of Salmonella. Het draait om uw risico's.

EEN PLAN B

Indien u op dezelfde wijze naar bedrijfscontinuiteit kijkt, omschrijven we dit 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. Vanzelfsprekend is het uitstekend dat u aan RM doet, maar bepaalde risico's zijn van dien aard dat u daarop voorbereid wilt zijn. U moet, om uw doelstellingen te halen of in het slechtste geval om te overleven in geval van een echte crisissituatie, een plan B hebben. Dat hoeft niet in te houden dat u op 100% 'Business as Usual'-niveau moet functioneren, maar wel op een dusdanig niveau dat u kunt voldoen aan wat u zelf hebt vastgesteld als zijnde het minimaal acceptabele niveau. BCM dientengevolge is het complete managementproces dat mogelijke gevaren met betrekking tot de continuiteit 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 waardecreërende activiteiten, waar u uw bestaansrecht aan dankt, gewaarborgd.

In de omschrijving van bedrijfscontinuiteit staat *'plannen voor'* en dat is nou precies de link tussen RM en BCM. Verder houdt BCM zich bezig met het tweede stukje van dit deel van de omschrijving *'en te reageren op'*. Het is uitstekend dat we naar alle bedreigingen kijken die kunnen leiden tot verstoring van uw leveringsproces, deze vertalen naar risico's voor uw organisatie specifiek en deze vervolgens trachten te managen; daar vinden RM en BCM elkaar. Maar dan gaat BCM verder en stelt: 'Ja, maar wat gaan we doen als het nou tóch gebeurt, ondanks al onze mitigerende inspanningen?' Indien u dit laatste namelijk verzuimt te regelen en

de continuiteit van de product- en dienstverlening van de organisatie in gevaar komt als direct gevolg van een ernstig incident, komen clichés als: 'Hadden we nou tóch maar ...' naar voren. Helaas dan té laat. Hadden is wanneer hebben is geweest!

De beoordeling van risico's dient ook regelmatig uitgevoerd te worden. Ontwikkelingen rond de afhankelijkheid van IT, cybercrime en terrorisme zijn voorbeelden van risico's die vandaag in vergelijking met nog niet zo lang geleden een compleet ander risicoprofiel hebben, zowel qua kans als qua impact. Als gevolg daarvan dient dus ook eventueel uw plan B aangepast te worden.

AFHANKELIJKHEID VAN IT

In de IT is het managen van continuiteit dé nummer één prioriteit. Sterker nog, wij eisen van de IT-functie binnen onze organisatie minimaal 99,9% betrouwbaarheid en 'uptime' en zeker ook wanneer deze functie is uitbesteed aan een derde partij, wat steeds vaker het geval is. Zeker nu u steeds afhankelijker wordt van IT, dient vanuit RM hier ruim aandacht aan besteed te worden. Heeft u zich ooit gerealiseerd dat een geaccepteerde downtime van 0,1% toch nog bijna negen uren per jaar zijn? En wat is die garantie waard? Dat zal maar net bijvoorbeeld op de drukste dag zijn, of drie keer drie uren tijdens piektijden of vlak voor een deadline.

Wilt u daar niet op voorbereid zijn of bent u van mening dat dit soort incidenten altijd bij anderen gebeuren en niet in uw organisatie, omdat u het uitstekend voor elkaar heeft?

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 IT-functie op deze (terechte) eisen is dat er onder andere backup-procedures zijn ontwikkeld en dezelfde 'realtime data' op verschillende plaatsen (in de wereld) beschikbaar is gemaakt – naast andere slimme oplossingen. De hersteltijden van applicaties en apparatuur plus mogelijk dataverlies door uitval is speerpunt nummer één. Redundancy is momenteel het magische woord in dit kader. Als organisatie 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. Wat te alle tijden een uitdaging blijft is het afstemmen van de hersteltijden die door de IT-afdeling kunnen worden gerealiseerd op de vereisten vanuit de bedrijfsvoering en omgekeerd. 'Dit is wat we zo snel weer nodig hebben om onze producten en diensten te kunnen blijven leveren en dus moeten jullie van de IT-afdeling daaraan voldoen.'

Was het maar zo eenvoudig. Dit betekent dat u dient na te denken over de vraag: 'Hoe ga ik mijn producten en diensten leveren zonder IT?' En het antwoord: 'Dat kan ik niet', om vervolgens de schouders op te halen, de armen over elkaar te gooien of vertwijfeld in de lucht te steken en met een vragende blik richting de IT-afdeling te kijken die met een oplossing moeten komen, is niet de juiste reactie. Wanneer een activiteit kritisch is voor het behalen van uw doelstellingen, dient u een plan B te hebben. Op een andere wijze, handmatig, door anderen, het maakt niet uit, maar denk er over na en bereid u voor!

CYBERCRIME

Organisaties zijn in toenemende mate afhankelijk van digitale platformen en gegevens. Inmiddels ontelbare netwerkapparaten zijn onderdeel van wat wordt genoemd de 'critical infrastructure facilities': ze leiden tot enorme efficiencyverbeteringen, maar tegelijkertijd een angstaanjagende toename van aan cybercrime gerelateerde risico's. Hoe groter het aantal aan elkaar geknoopte apparaten – denk in dit kader ook even aan IoT (the Internet of Things) – des te groter wordt het aantal mogelijkheden om toegang te verkrijgen tot deze netwerken middels steeds ingenieuzere aanvallen. Helaas heeft dit inderdaad geleid tot een zorgwekkende groei en ontwikkeling van de cybercrime-industrie, die beschikt over de modernste middelen en technieken, waar menige organisatie de vingers bij aflikt. Er wordt als gevolg van deze ontwikkelingen enorm veel onderzoek gedaan naar de kans en impact. Ontkennen heeft geen zin, we worden allemaal met dit fenomeen geconfronteerd, direct of indirect.

Het feit dat uit een van deze onderzoeken blijkt dat meer dan 50% van de bedrijven wel eens een hacker heeft betaald tijdens een aanval met 'Ransom Ware' helpt niet echt: men wordt beloond voor de inspanning.

In een ander recent onderzoek onder grote organisaties met betrekking tot DNS (Domain Name System) gebaseerde bedreigingen is vastgesteld dat 77% van organisaties in Europa is getroffen met een gemiddelde impact van bijna driekwart miljoen euro per aanval. DNS is de 'gateway' voor elk organisatienetwerk en is aldus hét doelwit voor 'boefjes'; dé deur om binnen te geraken. Die 'gateway' bewaken is van enorm groot belang. Het gaat hier bijvoorbeeld om diefstal van gegevens en/of knoeien met de website, waardoor deze offline moet worden gehaald en werkelijk direct verlies van omzet het gevolg is.

EEN ORGANISATIEBREED CONTINUÏTEITSPLAN

Dit risico wordt vanzelfsprekend door RM en BCM en de gehele IT-community onderkend en er wordt hard gewerkt aan het voorkomen van impact door dit soort activiteiten van buitenaf. Het vermogen van een organisatie om de IT-systemen te beschermen en om te herstellen van wat voor cybercrime-activiteit dan ook, wordt ook wel Cyber Resilience genoemd; ook hier dus weerstandvermogen én veerkracht. Dit is een uiterst belangrijk proces. Dit gaat dan ook niet alleen om de techniek, maar dient ook mensen en processen af te dekken en kan niet geïsoleerd aangepakt worden. Het moet geïntegreerd worden in een organisatiebreed continuiteitsplan, het werkgebied van BCM. Het gaat om achtereenvolgens het borgen op topmanagement-niveau van dit onderwerp, de samenwerking tussen IT en de bedrijfsvoering als het gaat om de strategie en de juiste balans tussen wat we acceptabel vinden als impact en de kosten van het creëren van het benodigde weerstandsvermogen en veerkracht. Alles 100% dichttimmeren is ook een illusie, laat dat duidelijk zijn. Voor het kunnen leveren van producten en diensten kijken we voornamelijk naar de impact van cybercrime op de activiteiten die hiertoe bijdragen – dus naar heel veel. Net als bij de afhankelijkheid van IT op zich, gaat het hierbij bijvoorbeeld om het niet beschikbaar hebben van gegevens (die gestolen of gecompromitteerd zijn), systemen (die besmet zijn) of applicaties (die niet meer werken of waartoe we voorlopig even geen toegang hebben). In grote lijnen kan vervolgens dezelfde aanpak worden gekozen. Wanneer een activiteit kritisch is voor het behalen van uw doelstellingen, dient u een plan B te hebben. Dus op een andere wijze, handmatig, door anderen, het maakt niet uit, maar denk er over na en bereid u voor!

DE IMPACT VAN TERRORISME

Dit betreft wel een andere dimensie, dat weet men inmiddels in plaatsen als Parijs, Londen en Brussel, om het maar een beetje in de buurt te houden. Komen wij in Nederland aan de beurt? Niemand hoopt het vanzelfsprekend, maar is het of, of is het wanneer? Binnen RM wordt hier uiteraard aandacht aan besteed en volgt men de ontwikkelingen op de voet, maar binnen BCM gaat het toch eigenlijk voornamelijk over de mogelijke impact. Kunt u uw locatie nog gebruiken, ook indien u niet direct geraakt bent? Waar spant de politie bijvoorbeeld het lint? Indien u uw locatie niet kunt gebruiken, hoe staat het dan vervolgens met de IT-toegankelijkheid en bruikbaarheid? Hoe staat het met uw personeelsleden, zijn zij hierbij betrokken als slachtoffer of zijn ze door de schrik niet in staat (hier) te werken? Willen zij begrijpelijkerwijs bij hun gezin zijn? Wat is de situatie rond machines, middelen en voorraden? Kunt u uw belangrijkste partners en leveranciers bereiken en gebruiken? Allemaal legitieme vragen *als hét gebeurt*, dus is het uitermate belangrijk ook hiervoor een plan B te hebben. Zeker wanneer u in, wellicht gevoelsmatig, een risicogebied zit. Denk hierbij bijvoorbeeld aan de omgeving van Schiphol, het Centraal Station van Amsterdam of Utrecht, nabij het Binnenhof, militaire installaties en kazernes, knooppunten van energievoorziening, de haven van Rotterdam en het Botlekgebied. Dit is een voorbeeld waar RM een uitdaging heeft als het gaat om mitigerende maatregelen. De impactkant is voor de organisatie naast het verschrikkelijke persoonlijke drama indien het direct geraakt wordt, toch voornamelijk het hebben van een uitwijkplan gebouwd rond de beschikbaarheid van locatie(s), mensen, ICT, gegevens en documenten, machines, middelen, voorraden en wat nog meer nodig is om producten en diensten op een van te voren bepaald niveau te kunnen blijven leveren aan de afnemers.

RM, BCM EN DE STRATEGIE

Het komt er simpelweg op neer dat de gekozen strategie in al deze situaties van het grootste belang is. Om het niet te

Indien de gekozen strategie is dat alle activiteiten in een bepaalde volgorde worden hersteld, dan heeft dat direct invloed op welke producten en/of diensten vervolgens geleverd kunnen worden en daardoor welke afnemers wel en (nog) niet beleverd kunnen worden.

ingewikkeld te maken stel ik hier vast dat het overgrote deel van de bedrijven door middel van bepaalde activiteiten (processen) bepaalde producten en/of diensten leveren aan bepaalde afnemers (markten, klanten). Dit leidt er automatisch toe dat er drie ingangen zijn voor de continuiteitstrategie, namelijk de activiteiten, de producten en/of diensten en de afnemers.

Er zullen keuzes moeten worden gemaakt, wat het eerst hersteld moet zijn en wat wellicht helemaal (of nu nog even) niet. Indien de gekozen strategie is dat alle activiteiten in een bepaalde volgorde worden hersteld, dan heeft dat direct invloed op welke producten en/of diensten vervolgens geleverd kunnen worden en daardoor welke afnemers wel en niet beleverd kunnen worden. Indien de producten en/of diensten bepalend zijn voor de volgorde – dus eerst dit product en vervolgens dat product – dan heeft dat directe gevolgen voor de te herstellen activiteiten en die zijn bepalend voor welke afnemers wel en niet beleverd kunnen worden. Echter, indien de afnemers leidend zijn tijdens de continuiteitsinspanning, dus eerste deze klant en dan die en die (nog even) niet, dan is vervolgens bekend welke producten gemaakt moeten worden en/of diensten geleverd dienen te worden. Daaruit kan rechtstreeks afgeleid worden welke activiteiten in welke volgorde hersteld dienen te worden. Deze strategische keuzes zijn bepalend voor de tactische (management) handelingen en de inspanningen op de 'werkvloer': de operationele kant. Een niet te onderschatten beslissingstraject dat regelmatig wordt vergeten en tijdens een ernstig incident leidt tot chaos en kans op verkeerde keuzes en beslissingen. Uw plan B.

HETZELFDE DOEL: CONTINUÏTEIT

De samenhang en combinatie van de disciplines RM en BCM zorgt voor een optimale invulling met uiteindelijk hetzelfde doel: continuiteit. Er morgen óók nog zijn, wat er ook gebeurt. RM bepaalt via een analyse van alle mogelijke bedreigingen en de huidige staat van mitigerende maatregelen de risico's. BCM analyseert de activiteiten en bepaalt de meest kritische op basis van uw eisen. Denk hierbij aan impact op het gebied van veiligheid (mensen, product of omgeving), geld (schade, omzetverlies of boetes), klanttevredenheid of merk/reputatie. Deze twee uitkomsten – welke risico's loop ik en wat is de prioritering van herstel van mijn activiteiten in geval van een ernstige verstoring – leiden tot de bepaling van de herstelstrategie en uiteindelijk plan B. Hier ligt een één-op-één-relatie met oorlogvoering volgens Sun Tzu, de grootste en belangrijkste militair strateeg die China ooit heeft gekend. Wanneer u uw risico's kent en uw eigen organisatie, dan hoeft u niet te vrezen voor een ernstig incident. Indien u uw eigen organisatie en uw prioriteiten goed kent, maar niet weet welke risico's u mogelijk loopt, dan wordt de kans op een acceptabele uitkomst in geval van een ernstig incident tot zo'n 50% gereduceerd. Wanneer u geen enkel inzicht heeft zal het resultaat waarschijnlijk onbevredigend of zelfs desastreus zijn. In de woorden van Sun Tzu: 'If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.' Q