BUSINESS CONTINUITY MANAGEMENT IS MEER DAN ALLEEN HOOFDSTUK 14 - ISO 27001

Gert Kogenhop (1958) is directeur van bcm+, een bedrijf dat is gespecialiseerd in training, consultancy en implementatie van Business Continuity Management Systemen conform de norm ISO 22301. Gert heeft een financieel economische achtergrond en is onder andere werkzaam geweest als Regional Finance Director Northern Europe bij DELL inc. en is tevens een gecertificeerd trainer op het gebied van leidinggeven. Voor meer informatie kunt U terecht op www.bcmplus.nl of per e-mail: gk@bcmplus.nl

We leven in een maatschappij waarvan de complexiteit continu toeneemt. We moeten met steeds meer partijen rekening houden en hebben langere en intensievere afhankelijkheidsketens met een grotere kans op verstoringen op meerdere plaatsen met een steeds grotere hoeveelheid aan verschillende mogelijkheden. Het Nieuwe Werken als oplossing voor flexibiliteit en efficiency lijkt aan belangstelling te verliezen. Het leidt tot flexibilisering van werkplek en woon-werk verkeer. Maar de balans werk-privé en de binding met organisatie, collega en uiteindelijk de klant lijdt hieronder en daardoor het resultaat. Tevens zorgt het voor een groot aantal nieuwe bedreigingen en risico's, zeker op het vlak van Informatiebeveiliging.

In de nabije toekomst komt er duidelijk meer focus op een toename van de verantwoordelijkheid en autonomie van werknemers, inclusief grote aandacht voor de kwaliteit van de samenwerking en daarmee de coördinatie binnen de organisatie - tot en met de klant. ICT is hier de drijvende kracht, de facilitator. Informatiekwaliteit, accuraatheid, veiligheid, betrouwbaarheid, beschikbaarheid en noem alle vereisten maar op, worden in toenemende mate van belang. Uit een recent onderzoek van de Carnegie Mellon University blijkt dat het weerstandsvermogen en de veerkracht van organisaties onder toenemende druk staat door onder andere een toename van het gebruik van technologie (ICT), de globalisering met z'n open grenzen, de versnelde toename van de complexiteit van (operationele) processen en dit alles versterkt door de huidige economische situatie en helaas de van toepassing zijnde wet- en regelgeving. Uit een inventarisatie door onder andere het Business Continuity Institute (BCI) blijkt dat de top drie bedreigingen in Europa op dit moment zijn:

- Unplanned IT and telecom outage
- Data Breach
- Cyber crime

In een artikel in Het Financiële Dagblad eind augustus zegt Dick Schoof (Nationaal Coördinator Terrorisme en Veiligheid - NCTV) over Cybercrime het volgende: 'De risico's die organisaties dagelijks op internet lopen, hebben het kabinet ertoe aangezet de aanpak van digitale kwetsbaarheid tot prioriteit van het veiligheidsbeleid te maken'. Er bestaat inmiddels een Cyber Security raad in samenwerking met het bedrijfsleven en de overheid heeft het National Cyber Security Centrum (NCSC) opgericht. Volgens Schoof nemen de illegale activiteiten in de cyberwereld in rap tempo toe. De weerbaarheid en het herstelvermogen van organisaties groeit gelukkig ook, maar minder snel. De balans is negatief. Wie het nieuws een beetje volgt, wordt hier niet door verrast. Regelmatig zijn er (ver) storingen, zoals in de telecomsector bijna normaal is geworden evenals bij de banken, als het gaat om telebankieren, al dan niet mobiel of met betrekking tot PIN transacties, maar laatst ook in een reserveringssysteem van een grote luchtvaartmaatschappij. Overigens wordt er door de telecomproviders inmiddels gesproken over het overnemen van elkaars sms- en telecomverkeer in geval van een ernstige calamiteit. Een nobel streven, maar het is nog niet zo ver. Ernstiger wellicht zijn de activiteiten van hackers, zoals diverse overheidsinstanties (bijvoorbeeld de belastingdienst) en gemeenten hebben ondervonden. Hoe veilig is onze (klanten)data bij bedrijven en instanties? Of het nu gaat om adres- en eventueel bankgegevens, het hacken van de ontwikkelaars website van Apple, of een ordinair beveiligingslek, iemand is de dupe en niemand wil dat zijn. In

> Het weerstandsvermogen en de veerkracht van organisaties staat onder toenemende druk

de Boardroom Cyber Watch Survey 2013 van IT Governance Ltd staat het volgende te lezen: 'Although businesses tend to focus mainly on the external cyber-threats facing organisations, more than half of respondents say that the greatest threat to their company's data and computer systems in fact comes from their own employees.' En voorts: 'A significant minority – over 40% - of respondents say their company is either making the wrong level of investment in information security or are unsure if their investment is appropriate.' Eén op de vier organisaties heeft het afgelopen jaar te maken gehad met een aanval van buitenaf.

De schade voor de getroffen bedrijven valt zeker niet te onderschatten, of dit nu rechtstreeks toewijsbaar is of dat we spreken over reputatie- en/of merkschade, schade is er vaak direct en is veelal omvangrijk. Bedrijven schade toebrengen door het platleggen van websites of systemen middels bijvoorbeeld een DDoS-aanval leidt al niet meer tot headlines. Het is bijna "business as usual". Gespecialiseerde bedrijven als datacenters doen er vanzelfsprekend van alles aan om de continuïteit van dienstverlening, in dit geval simpelweg toegang tot data, te garanderen (zo optimaal mogelijk waarborgen wellicht). Maar zijn de SLA's die bedrijven afsluiten wel "continuïteits-proof"? Niet zo lang geleden ging een datacenter failliet. Is dan alles wel goed geregeld? Kan iedereen bij zijn of haar data? Van wie is de data - juridisch? Hoe is de transitie geregeld naar een nieuwe oplossing, als de ketting al op het hek zit, het personeel naar huis is en de curator het voor het zeggen heeft? De prestatieverplichting in de SLA helpt dan vaak niet meer, dat mag duidelijk zijn. Voor datacenters in z'n algemeenheid gaat het om vier uitermate kritieke elementen:

- Stroomvoorziening, liefst triple redundant;
- Internettoegang, ook het liefst meerdere opties en uitwijkstrategieën;
- Beveiliging, zowel fysiek als tegen bijvoorbeeld hackers;
- Koeling.

Zij doen hun uiterste best om voor iedereen, de stakeholders, de dienstverlening optimaal te garanderen. Het hoeft geen betoog dat bij menig bedrijf deze processen en elementen niet dezelfde aandacht (en investeringen) krijgen, met alle risico's van dien.

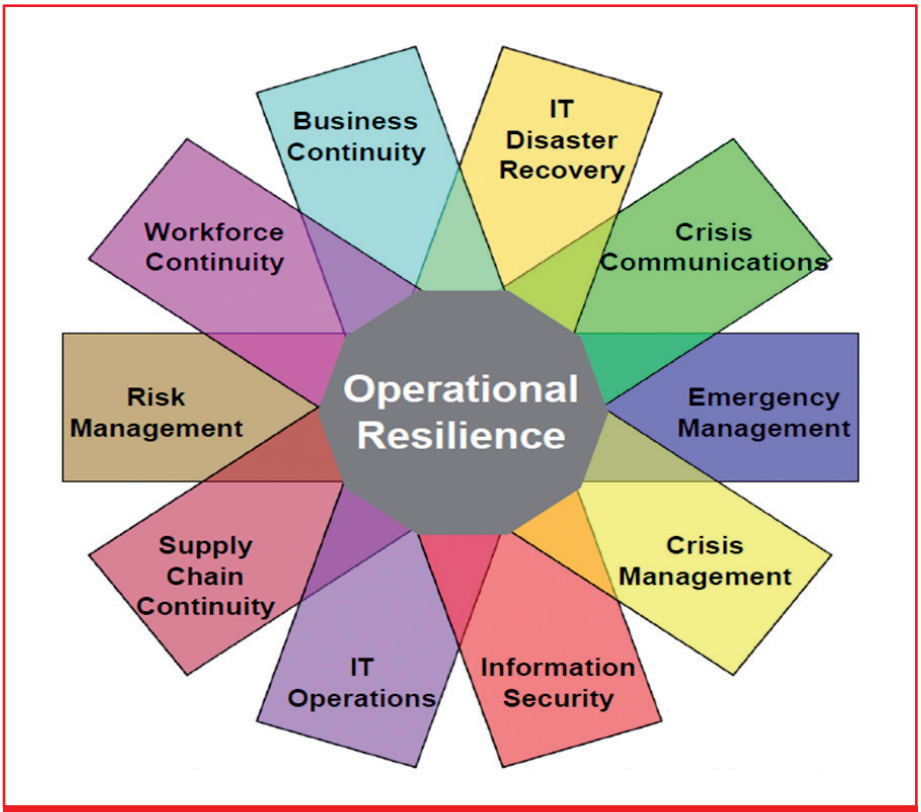
Laten we voor alle duidelijkheid even teruggaan naar de basis. Het begint eigenlijk allemaal met de Missie, Visie en Doelstellingen van de organisaties, leidend tot de uit te voeren activiteiten als gevolg van de gemaakte keuzes en vastgestelde uitgangspunten. Laten we het voorbeeld van het datacenter maar nemen. Wat de Missie en Visie ook zullen zijn, de Doelstellingen zullen liggen in de richting van groei van de activiteiten, gekoppeld aan redelijke doelstellingen met betrekking tot de winstgevendheid (Return On Sales - ROS) en het rendement op het geïnvesteerde vermogen (Return On Investment - ROI). De activiteiten benodigd om deze doelstellingen te bereiken zijn vrij duidelijk in beeld te brengen. Het gevolg hiervan leidt tot de eerste vaststelling. Het datacenter is als het gaat om de eerder genoemde vier kritieke elementen in mindere of meerdere mate kwetsbaar.

We worden toch nog regelmatig verrast door een bedreiging waar niemand rekening mee had gehouden

Het heeft mensen nodig, capaciteit in de vorm van ruimte en machines, energie, internettoegang, een beveiligingssysteem, koelsystemen die te allen tijde functioneren en noem maar op. Deze kunnen allemaal niet zelf worden gecreëerd, in de zin van "self supporting". Technisch gezien is in het kader van risicomanagement en continuïteitsmanagement deze kwetsbaarheid als volgt te omschrijven: *Omstandigheid die ervoor zorgt dat het doel van een object of activiteit mogelijk niet wordt gerealiseerd. Het is een onvervreemdbare eigenschap van een object of activiteit in die specifieke vorm, onafhankelijk van de omgeving. De kwetsbaarheid zelf is een inherente eigenschap, die alleen kan worden weggenomen door het object of de activiteit te veranderen. In het Engels aangeduid als "Vulnerability".* Het is van het grootste belang dat

organisaties een volledig beeld hebben van de kwetsbaarheden, daar dit de Achilleshiel van de organisatie kan bevatten.

Een volgende stap in het proces is vervolgens het kennen van de bedreigingen welke gelden voor de organisatie. In het geval van ons datacenter dus zaken als het uitvallen van de stroomvoorziening, internetverbinding of koeling of het ernstig falen van de beveiliging. De bedreiging wordt in dit kader als volgt omschreven: *Een kwetsbaarheid die daadwerkelijk uitgebuit kan worden in de eigen omgeving is een bedreiging. Het is een eigenschap die afhankelijk is van de omgeving waarin de onderliggende kwetsbaarheid optreedt. Een bedreiging kan worden weggenomen zonder dat de onderliggende kwetsbaarheid is weggenomen. Een kwetsbaarheid kan niet worden weggenomen zonder het object of de activiteit waarin deze optreedt te veranderen. In het Engels aangeduid als "Threat"*. Deze bedreigingen kunnen in kaart worden gebracht. Er bestaat in het algemeen wel voldoende kennis in de organisatie om het merendeel en de belangrijkste bedreigingen boven tafel te krijgen en in beeld te brengen. Bovendien zijn algemene bedreigingen toe te voegen aan de "interne" lijst. Dit gezegd hebbende worden we toch nog regelmatig verrast door een bedreiging waar niemand rekening mee had gehouden (z.g. Black Swans). Een bekend voorbeeld van niet al te lang geleden is de aswolk als gevolg van de vulkanische activiteiten op IJsland die ons land en vooral het vliegverkeer enige tijd danig dwars heeft gezeten. Het woord "aswolk" was sowieso een nieuw fenomeen en wordt bijvoorbeeld niet door MSWord herkend als bestaand woord en als zodanig rood onderstreept als zijnde wellicht niet correct, maar dat terzijde.



Operational Resilience

Als laatste stap in het proces komen we bij het bepalen van de risico's. Hoe groot is de kans dat iets gebeurt, wat zijn dan de gevolgen en hoe lang hebben we last van die gevolgen. Voorts wellicht beoordelen en bepalen hoe wij de risico's kunnen beïnvloeden en wat onze huidige "control levels" zijn. In dit kader kijken we als volgt aan tegen risico's: *Risico is het gevaar op verlies of schade door het manifest worden van een bedreiging. De (geschatte) frequentie waarmee dat gebeurt wordt "kans" genoemd. De nadelige gevolgen in de vorm van verlies of schade worden samengevat onder de noemer "impact". Risico wordt vaak beschreven als - Risico = Kans x Impact. In het Engels aangeduid als "Risk"*. Nu zijn we automatisch aangekomen op de scheidingslijn en/of het raakvlak van risicomanagement en business continuity management.

Het uitvoeren van risicoanalyses gebeurt zowel vanuit een oogpunt van risicomanagement als vanuit bedrijfscontinuïteit

Het uitvoeren van risicoanalyses gebeurt zowel vanuit een oogpunt van risicomanagement als vanuit bedrijfscontinuïteit. Laten we het als volgt stellen. Risicobeoordelingen welke worden uitgevoerd vanuit een Business Continuity Management initiatief zijn over het algemeen gericht op het operationele niveau, daar zij gericht zijn op het voorkomen van en, indien van toepassing, optimaal reageren op een ernstige verstoring (disruption) van activiteiten. Dit is een uitermate waardevolle toevoeging of zelfs essentieel onderdeel van de risicobeoordeling welke wordt uitgevoerd als onderdeel van de risicomanagement inspanning van de organisatie, welke over het algemeen plaatsvindt op ondernemingsniveau, "enterprise", vandaar ook de benaming Enterpise Risk Management (ERM). De overlap tussen BCM en ERM levert de organisatie de ultieme mogelijkheid op om het weerstandsvermogen en de veerkracht (Resilience) te versterken, maar enkel wanneer het integraal wordt uitgevoerd, holistisch, het geheel én de onderlinge samenhang. Resilience wordt in dit kader dan ook gedefinieerd als: *het vermogen van een*

organisatie om een ernstige verstoring (disruption) te verwerken, er effectief op te reageren en hiervan te herstellen op de meest optimale wijze.

De continuïteit van bedrijfsvoering, de levensader van elke organisatie, moet zo optimaal mogelijk worden gewaarborgd. Het gaat aldus veel verder dan alleen ICT en in het geval van ICT bijvoorbeeld hoofdstuk 14, Bedrijfscontinuïteitsbeheer van de ISO 27001 norm. Het gaat om het zo optimaal mogelijk garanderen van de continuïteit van de bedrijfsvoering van elke organisatie, bedrijfsleven en overheid, profit en non-profit, oud en jong, groot en klein. Iedereen heeft belang bij een organisatie die morgen ook nog functioneert. Nu zijn continuïteitsplannen net als vele andere elementen als risicomanagement, communicatiestrategieën, Informatiebeveiliging en crisismanagement allemaal op hun eigen specifieke wijze van belang. Het gaat echter om het realiseren van weerstandsvermogen en veerkracht indien er écht iets gebeurt. 'Voorbereiding is 90% van het resultaat', wordt er wel gezegd en geschreven, maar in dit geval gaat dat zeker op. Het gaat om "Operational Resilience", de organisatie draaiende houden en overleven door een optimale voorbereiding.

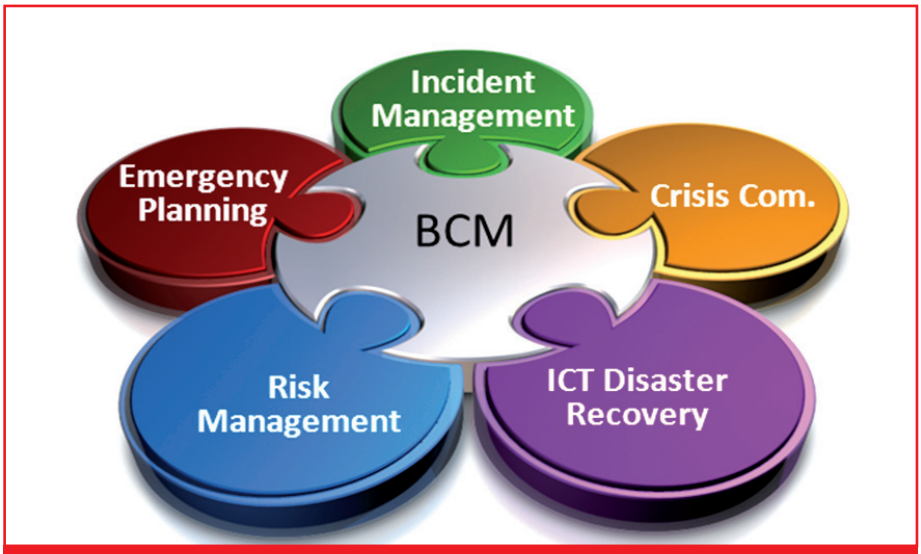
Zoals al eerder aangegeven is de toenemende afhankelijkheid van ICT een gegeven, terwijl tevens heden ten dage de grootste bedreigingen ook op dit gebied liggen. Vanuit een holistische gedachte, het geheel (de organisatie) en de onderlinge samenhang van alle activiteiten en de onderlinge afhankelijkheden van de verschillende activiteiten, zowel intern als extern, kan worden gesteld dat ICT het middel is waarop men bouwt, de bron, de voeding en de smeerolie van de organisatie.

Voorbereiding is 90% van het resultaat

Samen met andere activiteiten en met de continuïteitsgedachte als uitgangspunt dienen alle puzzelstukjes op de juiste plaats te worden gelegd om de organisatie te voorzien van bescherming op het juiste niveau. Business Continuity Management is onlosmakelijk verbonden met zaken als Incident Management, Crisis Communication, ICT Disaster Recovery, Risk Management en Emergency Planning.

Zoals gesteld in ISO 27001 dient Informatiebeveiliging opgenomen te worden in het continuïteitsbeheer, dient er te worden beoordeeld welke gevolgen ernstige incidenten kunnen hebben op Informatiebeveiliging en dient er naar gehandeld te worden, moet er aandacht besteed worden aan de beschikbaarheid en hoe lang verstoringen mogen duren (bijv. RPO) en zal dit alles getest en gecontroleerd moeten worden. Laat duidelijk zijn dat niemand deze wensen c.q. eisen betwist, echter ze dienen nooit en te nimmer op zich te staan, als een ICT-ding. Business Continuity Management is van ons allemaal. Iedereen in de organisatie en zelfs daarbuiten, de zogenoemde "Interested Parties", partijen met een belang, een interesse, moeten zich zorgen maken over en zich bezig houden met zowel vandaag als morgen. De fout maken om geen plan te hebben voor wanneer het onverwachte gebeurt, is eigenlijk plannen om een enorme fout te maken wanneer het onverwachte gebeurt. In elke organisatie dienen de bestuurders de afweging te maken of er tijd, geld en aandacht moet worden besteed aan Business Continuity Management. Elke bestuurder zal zijn of haar eigen afweging moeten maken en standpunt bepalen. Is het overbodig, doomdenken en gebeuren "dat soort dingen" bij ons toch niet, of is het een onderdeel van Maatschappelijk Verantwoord Ondernemen en Good Governance. Aan Darwin wordt de volgende quote toegeschreven: 'It is not the strongest of the species that survives, nor the most intelligent that survives. It is the one that is most adaptable to change.' Hieruit kan worden afgeleid dat zij die de (plotselinge, onverwachte) verandering (gebeurtenis) zo goed mogelijk kunnen opvangen, de grootste kans op overleven hebben. Continuïteitsmanagement, niet alleen binnen ICT en specifiek Informatiebeveiliging, maar voor de gehele organisatie. ●

Business Continuity Management is van ons allemaal



BCM in Context