Business Continuity Management System moet niet beperkt blijven tot IT-functie

CONTINUÏTEITSMANAGEMENT **VERZILVERT** WAARDE IT

‘Business as usual’ wil elke organisatie. Maar zijn organisaties wel voorbereid op ernstige verstoringen? Continuïteitsmanagement of Business Continuity Management is een normale term in de IT-wereld, maar vindt nu zijn weg – met behulp van ervaren IT-professionals – in de rest van de organisatie. En dat wordt hoog tijd, zegt Gert Kogenhop.

door: GERT KOGENHOP **beeld:** SHUTTERSTOCK

In veel gevallen loopt IT voor op andere ontwikkelingen in de organisatie. De vooruitgang begint vaak bij een IT-oplossing. Men realiseert zich in toenemende mate dat de continue beschikbaarheid van IT steeds belangrijker wordt. In vele gevallen zelfs een levensvoorwaarde voor organisaties. Continuïteitsmanagement of Business Continuity Management (BCM) is een vanzelfsprekendheid, zeker bij organisaties die werken met of conform ISO 27001. IT-professionals die zich met dit onderwerp bezighouden, worden regelmatig betrokken bij organisatiebrede initiatieven op dit gebied. Een terechte en interessante ontwikkeling. Nu ISO 22301 BCMS steeds vaker wordt gebruikt als standaard of zelfs wordt geïmplementeerd en gecertificeerd als norm, kunnen de kennis, vaardigheid en vooral de ervaring van de IT-professional van doorslaggevend succes zijn bij de inrichting van zo’n systeem voor de gehele organisatie.
We leven in een tijd waarin de complexiteit van zakendoen continu toeneemt. We moeten met steeds meer partijen rekening houden. Zaken als open grenzen, langere en intensievere afhankelijkheidsketens (supply chain) met een grotere kans op verstoringen op meerdere plaatsen omdat het allemaal sneller en vooral goedkoper moet, maken het er niet eenvoudiger op. Leveren in dat kader besparingen en programma’s als Lean en Six Sigma geen ongewenste bijwerkingen op? Creëren we met sneller, strakker en eenvoudiger geen (continuïteits)risico’s? Dit is vaak het geval. De impact van een verstoring wordt steeds groter, zeker wanneer je te veel flexibiliteit en alternatieven om kostenbesparende of efficiencyredenen weghaalt. Daarnaast speelt IT een steeds dominantere rol binnen organisaties, inmiddels binnen élke functie en bij élk bedrijfsproces.

Sense of urgency

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. IT is hier de drijvende kracht, de facilitator. Informatiekwaliteit, accuraatheid, veiligheid, betrouwbaarheid, beschikbaarheid zijn in toenemende mate van groot belang. Uit een onderzoek van de Carnegie Mellon University (VS) blijkt dat het weerstandsvermogen en de veerkracht van organisaties onder toenemende druk staan door onder andere een toename van het gebruik van technologie, 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. Uit de laatste inventarisatie door onder andere het internationale Business Continuity Institute (bci) blijkt dat de top drie bedreigingen wereldwijd IT-gerelateerd zijn: cyberaanvallen, ongeplande IT- en telecomuitval en data-explosie.
Vanzelfsprekend is iedereen in de organisatie gefocust op de gestelde doelstellingen en ‘business as usual’, ook al is dat laatste momenteel niet eens voor iedereen weggelegd. Maar zijn organisaties voorbereid op een ernstige verstoring? Realiseert men zich wat de impact kan zijn? Hebben we ook een organisatie klaar staan die handelt als het niet business as usual is? Hoe garandeert de organisatie dat zij er morgen ook nog is, wat er ook gebeurt? Business Continuity Management, een normale term in de IT-wereld, vindt zijn weg in de rest van de organisatie, en dat wordt hoog tijd.
Hoe je het ook wendt of keert het gaat uiteindelijk bij dit soort initiatieven om de ‘sense of urgency’: waarom moet men hier tijd, geld en energie in steken? Op hoofdlijnen gaat het hier om drie mogelijkheden. Of het is een vereiste van het hoogste bestuur van de organisatie, wellicht de eigenaar of aandeelhouders. Verder kan het een verplichting zijn, zoals bijvoorbeeld in de bank- en verzekeringswereld, van De Nederlandsche Bank en door Europese of wereldwijde afspraken. Het meest waarschijnlijk is echter een dwingend opgelegde contractvoorwaarde door afnemers, als onderdeel van de leveringsovereenkomst. Business Continuity Management gaat over het zo optimaal mogelijk voorbereid zijn op het onverwachte. Het complete managementproces dat alle mogelijke bedreigingen met betrekking tot de continuïteit van de organisatie in kaart brengt en een kader schept voor het opbouwen van weerstandsvermogen en veerkracht. Door effectief reageren worden de organisatiebelangen en de reputatie tegen onnodige, vermijdbare schade beschermd. De organisatie wordt niet onaangenaam verrast en men houdt de volledige controle met betrekking tot het functioneren van de belangrijkste, kritische activiteiten van de organisatie, op een overeengekomen minimaal niveau.

Restrisico

Binnen IT gaat het er vooral om wat de gebruiker merkt: bij voorkeur niets, bij incidenten dat zij zo kort mogelijk duren en dat er geen data verloren gaan. Het gaat hier in principe over in eerste instantie de interne klant, de collega’s. Voor de gehele organisatie ligt dat breder en dieper. Het gaat uiteindelijk ook om de klant, al is hij in het geval van de gehele organisatie een buitenstaander, maar toevallig wel degene die de rekeningen betaalt. Waar kunnen de kennis en ervaring van de IT-professional in dat geval een bijdrage leveren? Erg simpel. De IT’er kent het proces dat doorlopen dient te worden. Na het vaststellen van onder meer de omvang en de doelstellingen van het BCMS wordt vervolgens een Business Impact Analyse gemaakt. Wat is de impact op activiteiten binnen de organisatie wanneer zij door verschillende oorzaken stil komen te liggen? Van bijvoorbeeld de salarisadministratie tot werkzaamheden op de afdeling productieplanning, van het produceren van het product tot het laden van de vrachtwagen voor de klant. De definitie van impact mag dan iets anders luiden, bijvoorbeeld met betrekking tot persoonlijke veiligheid, productkwaliteit of leveringsbetrouwbaarheid, maar de methodiek is hetzelfde en dus zijn kennis en ervaring waardevolle bijdragen. Bij de risicobeoordeling is het wederom de ervaring met dit fenomeen waar de organisatie van kan profiteren. Het strategisch, tactisch en operationeel voorbereid zijn, met rol- en taakverdelingen, is eveneens gesneden koek voor IT’ers.
Elke organisatie moet voor zichzelf bepalen in welke mate zij voorbereid wil zijn. Belangrijk is dat die voorbereiding effectief is, anders is het verspilde energie. Om het voorbeeld van een goed geoutilleerd datacenter te nemen: in z’n algemeenheid gaat het uiteindelijk om vier uitermate kritieke elementen:
1. elektriciteitsvoorziening, liefst triple redundant;
2. internettoegang, ook het liefst meerdere opties en uitwijkstrategieën;
3. beveiliging, zowel fysiek als tegen bijvoorbeeld hackers;
4. koeling, ook hier zeker twee separate systemen.

Zo zijn maar weinig IT-afdelingen bij bedrijven ingericht. Wat de organisatie ook onderneemt, er blijft toch een bepaalde mate van kwetsbaarheid over, een restrisico. Men heeft naast deze elementen ook mensen nodig, capaciteit in de vorm van ruimte die ook nog eens moet voldoen aan allerlei voorwaarden, en machines. Zo is het ook met bedrijven. Je kunt onmogelijk alle continuïteitsrisico’s uitbannen. Voor elk productiemiddel (single point of failure) een back-up op de plank hebben liggen, is vaak onmogelijk, maar nadenken over hoe te handelen wanneer er onverhoopt toch iets misgaat, is uitermate verstandig. Voor elke kritieke leverancier (single sourcing) een alternatief zoeken, is sowieso een zinvolle exercitie en voor elke medewerker (single point of knowledge) iemand hebben die dezelfde activiteiten ook kan uitvoeren, is eigenlijk voor elke organisatie een ‘must have’.
Een gedegen BCMS levert enorm veel waarde op voor organisaties en moet zeker niet beperkt blijven tot de IT-functie (zie kader). De kernbegrippen zijn: een gestructureerde aanpak, beter voorbereid zijn, meer inzicht vooraf creëren, duidelijke processen, kortere hersteltijd en als gevolg hiervan minder schade. En de IT-professional kan hierbij van grote waarde zijn voor de organisatie. «

Gert Kogenhop is directeur van bcm+, een bedrijf dat is gespecialiseerd in consultancy en implementatie van Business Continuity Management Systemen conform de norm ISO 22301, en trainer bij de Security Academy. Tevens is hij voorzitter van de BCM-normcommissie bij NEN.

MASTERCLASS BEVEILIGING

Gert Kogenhop is een van de sprekers bij de Masterclass Security, Business Alignment 2.0. In een serie van zes masterclasses leert de (IT-)manager hoe hij het beveiligingsproces optimaal kan faciliteren. Hoe zorgt hij voor een doordacht securitybeleid dat verder reikt dan alleen de IT-afdeling? In de masterclasses laten AutomatiseringGids, Nyenrode Business Universiteit en Security Academy zien hoe security een goede plek krijgt in de organisatie. Sprekers zijn: Jan Veldsink, Johan Bakker, Gert Kogenhop, Michiel Kuethe, Peter van Schelven en Patrick de Brouwer. De masterclasses starten op 11 mei aanstaande. Meer informatie: http://bit.ly/1EUs51S.

Waarde creëren

Een gedegen BCMS levert enorm veel waarde op voor organisaties en moet zeker niet beperkt blijven tot de IT-functie. Er wordt waarde gecreëerd voordat er ook maar iets gebeurt. Vanzelfsprekend ook tijdens een ernstige verstoring en zeker ook erna. Die laatste twee kan men dan labelen als ‘waarde behouden’.

Vóór het incident ooit werkelijk plaatsheeft:
- Verdieping van de kennis van bedrijfsprocessen.
- Inzicht in zaken als Single Sourcing, Single Point of Failure en Single Point of Knowledge.
- Bekendheid met afhankelijkheden: tussen afdelingen en disciplines onderling en met derden.
- Identificering van kwetsbaarheden en bedreigingen: soorten incidenten en bronnen van incidenten.
- Vermindering van risico’s (kans en/of impact).
- Versteviging van betrouwbaarheid voor partners.
- Verbetering van onderhandelingspositie.

Tijdens het incident:
- De organisatie operationeel houden met minimale verstoring als gevolg van het incident.
- Verzekeren van veiligheid van mensen.
- Beschermen van ‘bezittingen’: reputatie en merk, aandeelhouderswaarde en financiën, voorraden en (bedrijfs)middelen, kennis en vaardigheden.
- Minimaliseren van verwarring en onzekerheid: leiderschap (rollen en taken), beslissingsbevoegdheid en communicatie.

Direct na het incident:
- Optimale herstelcapaciteit van de organisatie en zo snel mogelijk terug naar de normale gang van zaken.
- Wederopbouw van marktaandeel en winnen van vertrouwen van klanten door effectief reageren.
- Leren.

Voor reacties en nieuwe bijdragen van IT-experts: Henk Ester, 070 3046812 h.ester@automatiseringgids.nl