Bedrijfscontinuïteitsmanagement wérkt niet geïsoleerd

Wanneer uw organisatie wordt getroffen door een ernstig incident dat de bedrijfsvoering verstoort, waardoor bepaalde activiteiten niet meer kunnen worden uitgevoerd, dan implementeert u het plan B, het bedrijfscontinuïteitsplan (Business Continuity Plan – BCP). Iedereen pakt zijn of haar taken op om de geprioriteerde, kritische activiteiten te herstellen om 'Wat wij hier doen' zo optimaal mogelijk voort te zetten. Een fantastisch streven, dat altijd samen met anderen uitgevoerd moet worden en niet in isolement.

Door Gert Kogenhop, bcm+

Neem een cyberincident. Wanneer bijvoorbeeld een virus via een e-mailtje is binnengekomen, dan kan dit ernstige gevolgen hebben voor de bedrijfsvoering. U kunt bijvoorbeeld geen gebruik maken van IT, er is geen toegang tot het netwerk en als gevolg daarvan kan niemand printen, is er geen internet en kan men geen applicaties gebruiken. Uw eerste reactie is waarschijnlijk 'Dan kan ik niks' en helaas komt dat redelijk in de buurt van de werkelijkheid.

De afhankelijkheid van IT is eerlijk gezegd in veel bedrijven onacceptabel hoog. Wanneer u geen plan B hebt gaat de factor geluk een té grote rol spelen. Dan gaan de armen over elkaar en volgt er een diepe zucht en zakt men achterover of vraagt men of men naar huis mag – met doorbetaling van salaris, want wij kunnen er toch zeker niets aan doen! Is er wel een BCP met het scenario 'IT niet beschikbaar' dan is er nagedacht over de aanpak en het herstel, hopelijk zelfs zo dat uw klanten dit niet merken voor wat betreft de levering van uw producten en diensten. In professionele organisaties komen er zeker drie teams in actie: Het *Crisis Management Team (CMT),* het *Computer Security Incident Response Team (CSIRT)* en het *Business Continuity Management Team (BCMT).*

Zonder verder teveel in detail te treden houdt in z'n algemeenheid alleen het CMT zich bezig met zaken rond merk en reputatie, plus de communicatie met stakeholders en de media. Het CSIRT is de enige die focust op de veiligheid van (persoons)gegevens en het verwijderen van het virus. Het BCMT stort zich op de verantwoordelijkheid voor zaken als gebouwen, werkomgeving en bijbehorende voorzieningen, faciliteiten, uitrusting en verbruiksmaterialen en transport met als doel: leveren.

Voor de overige uitermate belangrijke zaken als personeel, gegevens en informatie, ICT, partners en leveranciers, financiën en niet te onderschatten wet- en regelgeving (denk in dit geval ook aan de *Wet beveiliging netwerk- en Informatiesystemen* (Wbni) en de *Autoriteit Persoonsgegevens*) moeten alle drie teams zeer nauw samenwerken. De kernwoorden zijn Samenwerken, Informatie delen en Integratie. Naast het plan B met betrekking tot het leveren van producten en diensten, dient deze interactie en onderlinge afhankelijkheid vóóraf goed te worden geregeld. Duidelijkheid over de rollen en verantwoordelijkheden is van het allergrootste belang. Het zijn geen eilandjes of koninkrijkjes, er wordt – door het creëren van synergie en resilience – voor hetzelfde doel gestreden: de tevreden klant. Hoe is dat bij ú geregeld?

Drie tips die de bedrijfscontinuïteit ten goede komen

Business Continuity Management (BCM) wordt steeds meer volwassen. Dat is het logische gevolg van maatschappelijke, politieke en technologische ontwikkelingen die de wereld steeds sneller veranderen en de continuïteit van een organisatie in gevaar kunnen brengen. Denk aan cybercrime of de Brexit: twee voorbeelden die ontwrichtende gevolgen hebben en zelfs bedrijven kunnen platleggen. Daarnaast is er de opkomst van social media, waardoor elke misstap zich razendsnel verspreid over het internet.

Door Natascha Hannema, Corporate Business Continuity Manager equensWorldline

Hoewel we onbewust meerdere keren per week bezig zijn met het waarborgen van continuïteit in ons leven – denk aan het afsluiten van een autoverzekering – heeft nog niet elk bedrijf een draaiboek dat direct beschikbaar is wanneer een calamiteit zich voordoet. Vreemd eigenlijk, want via een draaiboek kan de toekomst van een organisatie voor een deel worden veiliggesteld. Hoe zo'n draaiboek eruitziet, hangt af van het type organisatie, maar de volgende drie tips kan ik elk bedrijf aanbevelen:

Tip 1: Breng je klantenbestand in kaart
Werken met één of twee grote klanten kan in de toekomst een continuïteitsrisico vormen: de kans bestaat immers dat je ooit afscheid van ze moet nemen. Ook politieke ontwikkelingen kunnen invloed hebben op je klantenbestand. Dat wordt nu duidelijk zichtbaar bij de Brexit-situatie: als een groot deel van je klanten uit Engeland afkomstig is of veelal zakendoet over het Kanaal, kan dat grote gevolgen hebben voor organisaties.

Tip 2: Train je medewerkers
Veel calamiteiten worden veroorzaakt door menselijke fouten. Denk aan datalekken door cybercrime, vaak veroorzaakt door phishing mails die door medewerkers zijn aangeklikt. Deze incidenten zijn te voorkomen door medewerkers te trainen en ze op de gevaren te wijzen. Blijf ook regelmatig oefenen en testen zodat het personeel op de hoogte is van nieuwe ontwikkelingen en zich bewust blijft van de gevaren.

Tip 3: Beschik over een gedegen communicatieplan
Wanneer een misstap op social media terechtkomt, is de kans groot dat deze zich razendsnel verspreidt en er zo een negatief beeld van de organisatie ontstaat. Veel organisaties houden zich vaak afzijdig in de hoop dat de online storm snel gaat liggen, maar niets van je laten horen wekt de indruk dat je de zaken niet onder controle hebt. Denk daarom vooraf goed na over crisiscommunicatie, zodat je adequaat kunt reageren wanneer je midden in het oog van een social media-storm terecht bent gekomen.

Kennismaken met Business Continuity Management en Resilience?

Voor veel organisaties zijn Business Continuity Management en Resilience nog vrij nieuwe begrippen. Het *Business Continuity Institute* is een organisatie waar vele professionals bij zijn aangesloten en er bestaan sinds enkele jaren afdelingen in Nederland en België. Jaarlijks wordt een eendaagse conference georganiseerd, waarbij de 'best practices' en diverse case-studies worden gedeeld, netwerkmogelijkheden worden geboden en waar alle informatie over deze onderwerpen is te vinden. Voor zowel de doorgewinterde professional als de nieuwkomer aangaande deze onderwerpen is er een interessant aanbod. Dit jaar vindt de conference plaats op 13 juni in DeFabrique in Utrecht. Er zijn speciale 'Early Bird' tarieven tot eind april, dus wees er snel bij.

Meer informatie is te vinden op: www.thebci.org/events/event-calendar.html (klik op het conference-logo in de maand juni).