BCM is geen hobby van de kwaliteitsmanager

Wanneer jouw bedrijf wordt getroffen door een ernstig incident wat de bedrijfsvoering verstoort en waardoor (bepaalde) activiteiten niet meer kunnen worden uitgevoerd, dan implementeer je je 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, maar dan moet je wél zo'n Plan B hebben!

Door Gert Kogenhop, Operationeel Manager BCM Kader group

Iemand moet zorgen dat het Plan B er is en dat het volledig, accuraat en actueel is, liefst geborgd in een managementsysteem (BCMS). Vaak ligt dit op het bordje van de kwaliteitsmanager. In alle situaties dient hij of zij dit tezamen met collega's te implementeren en te onderhouden: het moet niet worden gezien als de nieuwe hobby van de kwaliteitsmanager.

Neem nu een cyberincident. Stel je wordt geraakt door ransomware; niet ondenkbaar, tóch? Dit kan ernstige gevolgen hebben vanuit het perspectief van de bedrijfsvoering. Waarschijnlijk kun je hierdoor geen gebruik maken van IT; geen toegang tot het netwerk en als gevolg daarvan niet printen, geen internet en dus geen contact met de buitenwereld en geen toegang tot de zo broodnodige applicaties. De 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 je geen Plan B hebt, gaat de factor geluk een té grote rol spelen en dat kun je je niet veroorloven. Is er wel een Plan B (BCP) met daarin opgenomen het scenario 'IT uitval', dan is er vooraf nagedacht over de aanpak en het herstel, hopelijk zelfs zonder dat klanten dit merken.

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). Maar de voorbereiding – wat moet ik beschermen tegen welke risico's – waarvan ransomware er anno nu eentje is, hoort daar ook bij. Iedereen is betrokken bij de inrichting en implementatie van een optimale actie/reactie middels het Plan B.
Zonder verder in te veel detail te treden houdt in z'n algemeenheid alleen het CMT zich bezig met zaken rond merk en reputatie plus de communicatie met alle betrokkenen, inclusief de media. Het CSIRT is de enige die focust op de veiligheid van (persoons)gegevens en het verwijderen van het 'probleem'. Het BCMT stort zich in zo'n situatie op het op een andere manier, eventueel op een andere plek en met wellicht andere mensen, voortzetten van de levering van de producten en diensten op een vooraf vastgesteld niveau (minimaal acceptabel niveau) binnen de afgesproken tijdsduur dat de boel stil mag liggen (hersteltijddoelstelling).

Duidelijkheid over de rollen en verantwoordelijkheden is van het allergrootste belang. Er wordt voor hetzelfde doel gestreden: de tevreden klant. Je moet wel als organisatie het een en ander van tevoren regelen en dit ook geregeld oefenen. Het gaat dan bijvoorbeeld om een bedrijfsimpactanalyse. Doel hiervan is vast te stellen welke activiteiten heel kritisch zijn en welke minder kritisch (dus wel even stil kunnen liggen) plus de risicoanalyse om te bepalen welke risico's voor jou actueel zijn en waar je je zeker op moet voorbereiden. Hoe is dat bij jou geregeld?