Zoek aansluiting met het Business Continuity Management System

NETWERK- EN INFORMATIE-BEVEILIGING... EN BCM!

Het Europees Parlement heeft in juli 2016 de nieuwe Europese cybersecurityrichtlijn aangaande Netwerk- en InformatieBeveiliging (de NIB-richtlijn) gepubliceerd, die gericht is op het creëren van een gemeenschappelijk niveau van netwerk- en informatiebeveiliging binnen Europa. Elke lidstaat dient in het kader van het maatschappelijk belang te zorgen voor betrouwbaar, betaalbaar en veilig netbeheer. Op dit moment wordt in Nederland gewerkt aan de Cybersecuritywet (Csw) met als doel invulling te geven aan de NIB-richtlijn. Op uiterlijk 9 mei 2018 moet de richtlijn zijn omgezet in wetgeving. We kunnen gerust stellen dat na de recente cybercrime incidenten met onder andere hacks en ransomeware dit geen overbodige luxe is.

Door Gert Kogenhop, bcm+

De NIB-richtlijn is van toepassing op door de lidstaten aan te wijzen 'aanbieders van essentiële diensten' (AED's) binnen de in de richtlijn specifiek genoemde sectoren (energie, vervoer, bankwezen, infrastructuur voor de financiële markt, gezondheidszorg, levering en distributie van drinkwater en digitale infrastructuur) en op 'digitale dienstverleners' (DSP's): aanbieders van onlinemarktplaatsen, onlinezoekmachines en cloudcomputerdiensten. Je kunt fronsen bij de keuzes, maar deze zijn specifiek benoemd. In de richtlijn wordt op diverse plaatsen melding gemaakt van het fenomeen 'Continuiteit' en dat is dan ook één van de doelstellingen – naast het voorkomen van misbruik van toegang en/of het buitmaken van gegevens.

> 'HET GAAT UITEINDELIJK OM HET MANAGEN VAN DE SITUATIE TIJDENS EN DIRECT NA EEN ERNSTIG INCIDENT'

Continuiteit van de benoemde 'essentiële' productlevering en dienstverlening. Je kunt daar begrip voor opbrengen wanneer je je bedenkt wat er zou gebeuren wanneer deze producten en diensten niet beschikbaar zijn. Op deze wijze is dan ook het onderwerp *informatiebeveiliging* onlosmakelijk verbonden met Business Continuity Management. Organisaties dienen zich te realiseren dat uitval van ICT als gevolg van een technische oorzaak (hardware uitval, software- of netwerkproblemen) al jarenlang in de spotlights staat en dat alle mogelijke opties en technische faciliteiten ter voorkoming daarvan een enorme ontwikkeling hebben doorgemaakt. Maar wat wanneer gebruikers geen toegang hebben tot ICT-systemen omdat er een beveiligingsincident is en men (nog) niet heeft kunnen vaststellen wat de omvang is? Men kan geen risico's op escalatie of verspreiding nemen en dat maakt de toegang tot gegevens, systemen en applicaties vooralsnog onmogelijk. Dan komt de vraag 'En wat nu?' naar boven. Hoe afhankelijk zijn we van ICT? Hebben we alternatieven? Wie gaat wat, hoe doen? Wat kunnen we nog wel? Hoe en wanneer informeren we derden die afhankelijk zijn van wat we hier doen? Allemaal legitieme vragen die binnen Business Continuity Management dienen te worden beantwoord, conform de daarbinnen vooraf vastgestelde strategie.

DE 'BUSINESS AS USUAL' SITUATIE

Bij Business Continuity Management gaat het uiteindelijk om het managen van de situatie tijdens en direct na een ernstig incident: een verstoring van de 'business as usual' situatie. In dit geval het niet beschikbaar zijn van (betrouwbare) ICT-systemen of gegevens. We moeten voorbereid zijn en zorgen dat we weten wat we moeten doen om de levering van onze producten en/of diensten aan onze afnemers zo optimaal mogelijk te waarborgen en indien nodig over bijvoorbeeld de (on)mogelijkheden en prioritering van te voren met álle belanghebbenden afspraken maken. Een niet te onderschatten beslissingstraject dat regelmatig wordt vergeten en tijdens een ernstig incident leidt tot chaos – en dus kans op verkeerde keuzes en beslissingen. Wellicht in dit geval nog versterkt door het feit dat het hier gaat om essentiële producten en diensten binnen de sectoren energie, vervoer, bankwezen, infrastructuur voor de financiële markt, gezondheidszorg, levering en distributie van drinkwater en digitale infrastructuur.

Voor wie te maken krijgt met de NIB-richtlijn en volgend jaar de Csw het advies om verder te kijken dan de informatiebeveiligingsimpact en het ICT-continuiteitsplan plus eventueel een separaat Disaster Recovery Plan. Zoek aansluiting met het Business Continuity Management System van de organisatie.