CYBERSECURITY EN ICT AFHANKELIJKHEID

Als je een 'verkeerde' trend zou moeten benoemen op dit moment is dat toch wel de toename van allerlei vormen van cybercrime zoals Hacking, Data breach, Ransomeware en DDoS-aanvallen. De diversiteit en creativiteit op dit gebied is enorm en de ontwikkeling zorgwekkend te noemen. Cybercriminelen houden zich aan geen enkele regel, terwijl 'zij die hen bestrijden' dat wel moeten doen. Denk in dit geval aan wat de 'sleepwet' wordt genoemd en andere zaken rond privacy, gegevensbescherming en beperkte opsporingsmogelijkheden, laat staan de huidige strafmaat op dit vrij nieuwe gebied. Hoe ver mag de overheid gaan om onze veiligheid te waarborgen?

Door Gert Kogenhop, directeur bcm+

Een andere zorgwekkende trend is toch wel de toenemende afhankelijkheid van alles wat met ICT te maken heeft, zowel de techniek als gegevens. Veel activiteiten en processen komen compleet tot stilstand zonder ICT, met in het slechtste geval geen enkel of slechts een voorlopig alternatief. Tel hierbij op het gevoel van 'Bij ons gebeurt nooit nie wat', dus we hoeven ons niet voor te bereiden. Gecombineerd met het idee dat de ICT-ers het wel geregeld hebben en voor ons gebruikers oplossen en de cocktail wordt redelijk giftig.

RISICO'S WORDEN TÉ GROOT

Dat er iets moet gebeuren is wel duidelijk, de risico's worden té groot. Nederland dient in het kader van het maatschappelijk belang te zorgen voor betrouwbaar, betaalbaar en veilig netbeheer, conform een EU richtlijn op dit gebied uit 2016. Afhankelijk van wanneer je dit leest wordt 9 mei 2018 de nieuwe *Cybersecuritywet* (Csw) van kracht of is dan van kracht geworden. Een gezamenlijke Europese aanpak wordt toegejuicht, zolang dit maar geen lokale doublures en verwarring tot gevolg heeft. In dat kader bijvoorbeeld zal de huidige *Wet gegevensverwerking en meldplicht cybersecurity* (Wgmc) weer worden ingetrokken. Spannend blijft wel de link met de nieuwe *Algemene Verordening Gegevensbescherming* (AVG of GDPR) die gepland staat voor 25 mei 2018 of die inmiddels al van toepassing is.

De Csw is specifiek van toepassing op 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 benoemde gerelateerde 'digitale dienstverleners'. In Nederland kennen we reeds in dit kader de 'vitale infrastructuur' en die is iets uitgebreider dan deze AED's. Een van de belangrijkste elementen van de Csw is de meldplicht van cyberrisico's en incidenten bij het Cyber Security Incident Response Team en het benodigde toezicht bij de daarvoor bevoegde autoriteit. Veel stof om over na te denken, Wie betreft dit? Wat betekent dit inhoudelijk voor mij? En wellicht ook: wat gebeurt er wanneer ik het niet doe en hoe worden sancties opgelegd?

In de Csw wordt op diverse plaatsen melding gemaakt van 'continuïteit' en dat, kun je gerust stellen, is dan ook één van de belangrijkste doelstellingen, naast vanzelfsprekend het voorkomen van mogelijk misbruik van buitgemaakte gegevens. Continuïteit van de benoemde essentiële dienstverlening. Je kunt daar begrip voor opbrengen als je je bedenkt wat er zou gebeuren wanneer bijvoorbeeld water, energie of gezondheidszorg niet beschikbaar is. De technische invulling laten we hierbij even voor wat het is, maar de gevolgen wanneer informatiebeveiliging faalt, voor de bedrijfscontinuïteit niet. Er wordt gesproken over het nemen van preventieve maatregelen, alsook wat te doen wanneer 'hét' gebeurt. In dit geval benoem ik dat als aantasting van de netwerk- informatiesystemen en onze gegevens door ongeoorloofd handelen. Dit is volledig gericht op bedreigingen/risico's gerelateerd aan netwerk- en informatiesystemen, waardoor bijvoorbeeld kritische ICT-diensten niet beschikbaar zijn voor kritische activiteiten. Wanneer werknemers of andere gebruikers geen toegang hebben tot ICT-systemen en dus bijvoorbeeld techniek, applicaties of gegevens als gevolg van een beveiligingsincident komt de vraag 'En wat nu?' naar boven. Hoe afhankelijk zijn we hiervan? 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 (nu even niet) doen?

EEN VOORAF VASTGESTELDE STRATEGIE

Allemaal legitieme vragen die binnen Business Continuity Management dienen te worden beantwoord, conform de vooraf vastgestelde strategie. Het gaat hierbij 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, techniek of gegevens. We moeten voorbereid zijn en zorgen dat we weten wat we moeten doen om bedrijfsvoering, de levering van onze producten en diensten aan onze afnemers zo optimaal mogelijk te waarborgen en indien nodig over bijvoorbeeld de (on) mogelijkheden en prioritering van te voren afspraken maken met álle belanghebbenden. Dus, 'fijn' dat er een wet komt die al dit soort zaken regelt voor de 'aanbieders van essentiële diensten', maar dit gaat niet alleen om hen, dit betreft elke organisatie die vindt dat zij bestaansrecht heeft en een doel dient, toch?

Voor wie te maken krijgt met impact door problemen rond informatiebeveiliging, en wie krijgt dat niet anno 2018, het advies om verder te kijken dan de ICT-afdeling en eventueel hun disaster recovery of continuiteitsplan, maar aansluiting te zoeken met de algehele bedrijfsvoering. Het gaat erom dat we morgen ook nog bestaan, met of zonder cybercrime. Daar heeft iedereen belang bij.

BCM+
Postbus 410
1620 AK HOORN
Tel: (0229) 26 47 97
E-mail: info@bcmplus.nl
Website: www.bcmplus.nl