De oprichting van een Cyber Security Operations Centre (CSOC) bij Defensie

Kapt IMM Geert ALBERGHS
geert.alberghs@mil.be

I. DE CYBER-CONTEXT

IT is geëvolueerd van een reëel competitief voordeel voor de 'early adopters' in de jaren '80 tot een standaard hulpbron, gemakkelijk toegankelijk voor iedereen. De IT infrastructuur is nog steeds essentieel om zich op de huidige markten te kunnen handhaven, maar levert nog weinig concurrentieel voordeel op. Vandaag is 'cyber-security' 'booming business': de IT veiligheidsrisico's zijn belangrijker geworden dan de technologische voordelen. De massale media-aandacht onderstreept dit belang. Denk maar aan de gebeurtenissen rond Julian Assange en Edward Snowden. Ook België werd niet gespaard. Mediaberichten bevestigen dat het Kabinet van de Eerste Minister, het Ministerie van Buitenlandse zaken, Belgacom en Defensie allemaal het slachtoffer van cyberaanvallen werden.

II. DE TAAK VAN EEN CSOC

Een CSOC waarborgt de operationaliteit van Defensie door de cyberrisico's onder een aanvaardbaar niveau te brengen. Het CSOC is verantwoordelijk voor: (1) de snelle detectie, de consistente afhandeling en de beperking van de impact van alle cyber-incidenten, (2) voor een correcte inschatting van de cyberdreigingen, (3) voor de analyse van de kwetsbaarheden, (4) voor het leveren van advies bij de implementatie van preventieve - en correctieve veiligheidsmaatregelen en (5) voor het aanleveren van bewijsmateriaal in geval van een gerechtelijk onderzoek.

III. DE SITUATIE BIJ DEFENSIE

Defensie heeft actueel een zeer beperkte CSOC-capaciteit binnen ACOS IS, zowel qua personeel als qua materieel. Het huidige personeel, dat van een hoog professioneel niveau is, wordt voornamelijk ingezet voor ad hoc incident handling. Het ontbreekt aan gestructureerde werkmethodes. Bovendien is er momenteel geen 'vulnerability monitoring', er gebeuren geen analyses van de cyberdreiging en er is slechts een zeer beperkte capaciteit aan sensoren beschikbaar, zowel in aantallen als in types.

IV. VOORSTELLEN TOT VERBETERING

Het CSOC moet actief zijn in 4 domeinen, namelijk: 'threat management', 'vulnerability management', 'incident management' en 'security device management'. Hieruit worden de 'service catalog', de organisatiestructuur en de 'jobdescriptions' afgeleid. De voorgestelde 'policies' en - werkmethodes zijn gebaseerd op het karrewiel van de 'incident-handling', rekening houdend met de specifieke behoeften van Defensie. Een integratie in het CCB proces werd hierbij voorzien. De technologieën, noodzakelijk voor de goede werking van het CSOC, worden eveneens besproken. Om tot een volledig operationele CSOC te kunnen komen, wordt een gefaseerde implementatie voorgesteld.