WELKE BESCHERMING TEGEN DE CYBERDREIGING?

De heer Marcel Grisnigt, Thales Nederland

Voor het correct functioneren van onze samenleving is het van essentieel belang om de 'cyberspace' te beveiligen. Cybersecurity is geen modeverschijnsel en cyberdreiging is geen fataliteit, maar een belangrijke bedreiging van onze informatiesamenleving, waarvoor bewezen oplossingen bestaan.

De Thales Groep is al langere tijd actief in het 'cyberdomein' en beschikt al over referenties bijvoorbeeld in het Franse bankwezen. De binnen Thales aanwezige cybersecurity kennis, expertise en capabilities zijn uiteraard ook in Nederland beschikbaar. Thales Nederland heeft hiervoor recent een aparte unit opgericht, Thales SecurITy Nederland. De missie van deze unit is: "Your SecurITy is Our concern!"
Thales wil u in dit artikel deelgenoot maken van zowel een deel van haar Thales 'cybervisie' als van een van haar beschikbare en bewezen cybercapabilities: CYBELS (*CYBer Expertise for Leading Security*).

NAAR EEN ACTIEVE BEVEILIGING

De bescherming van gevoelige informatiesystemen is altijd een voorname zorg geweest van defensie en veiligheidsorganisaties. Toch is dit probleem de afgelopen jaren van karakter veranderd door de explosie van nieuwe informatie- en communicatietechnologieën. Het goed functioneren van samenlevingen (in de breedste zin van het woord) hangt steeds meer af van onderling verbonden informatiesystemen. Deze onderlinge verbinding vergroot de kwetsbaarheid voor en de verspreiding van aanvallen, die steeds vaker voorkomen.
Daarom staat cybersecurity momenteel wereldwijd steeds vaker en hoger op de agenda van de nationale overheden ,en op de agenda van supranationale organisaties zoals de EU, NAVO en VN.. De eerste stappen zijn nu ook duidelijk in Nederland gezet, getuige de dit jaar verschenen Nationale Cyber Security Strategie, de oprichting van de Cyber Security Raad, de gestarte research activiteiten, etc.

CYBERSECURITY

Cybersecurity kan gedefinieerd worden als het geheel van gecoördineerde acties voor preventie, analyse en reactie op cyberaanvallen, voor een permanente en zo vroeg mogelijke bescherming tegen de dreigingen gericht op een informatiesysteem. In deze context draagt cybersecurity bij aan de weerstand van organisaties door capaciteiten voor anticipatie en snelle reactie te bieden ten aanzien van opzettelijke of accidentele aanvallen.

Het is hierbij van essentieel belang de traditionele aanpak van 'passieve beveiliging', waarbij de gevoelige informatiesystemen werden beveiligd tegen aanvallen door fysieke (beveiligde ruimtes) en logische barrières (firewalls, filters, wachtwoorden), om te zetten naar een meer '(pro)actieve aanpak'. De 'passieve' aanpak heeft trouwens minder en minder zin aangezien informatie-infrastructuren steeds vaker worden uitbesteed (*cloud computing*).

Voor de beveiliging van open, onderling verbonden systemen is dus voortaan een meer actieve en verregaande beveiligingsaanpak nodig, die rust op een zo vroegtijdig mogelijke bescherming tegen cyberaanvallen. Effectieve en efficiënte cybersecurity vormt de overgang van een passieve beveiliging naar een actieve, die in *real time* permanent de blootstelling van informatiesystemen aan cyberaanvallen evalueert.

VEILIGHEIDSSUPERVISIE: FEEDBACK UIT DE INDUSTRIE

De industrie heeft al snel cybersecurityproducten ontwikkeld. Thales werkt bijvoorbeeld al tien jaar met een centrum voor permanente supervisie van de veiligheid van gevoelige informatiesystemen van vitale infrastructuren in het bankwezen, het vervoer en de energiesector.
Door de tijd heen heeft Thales deze ervaring in cybersecuritydienstverlening gecombineerd met de unieke expertise in het ontwerp en de ontwikkeling van *high tech security* producten om een volledig aanbod voor cyberdefensie te ontwikkelen: CYBELS (*CYBer Expertise for Leading Security*).
Het CYBELS product wordt gevormd door drie elkaar aanvullende modi:

- supervisie, 24/7, van gemonitorde informatiesystemen volgens genormeerde procedures,
- levering van capaciteiten voor cybersecurity, bijvoorbeeld de hypervisie van verschillende te bewaken systemen, de opleiding van experts die gaan werken in een centrum voor cybersecurity of het gebruik van machines voor 'event' correlatie,
- de levering van een operatiecentrum voor cybersecurity 'klaar voor gebruik' (zodat de klant zelf de cybersecurity van zijn informatiesysteem kan verzorgen).

MYTHE 'PASSIEVE BEVEILIGING'

De hardnekkige mythe van de 'passieve beveiliging'.
We horen nog veel te vaak: "Ik ben beschermd omdat mijn netwerk geen andere verbinding heeft". Zoals regelmatig, en ook recent met het DigiNotar incident, aangetoond in diverse (cruciale) netwerken, komt deze bedrieglijke, strikt plaatselijke beveiliging niet overeen met de realiteit van verborgen onderlinge of slecht beheerste verbindingen (USB-stick, laptop, smartphone enz.) en de verfijndheid van de aanvallen.

Het operatiecentrum voor cybersecurity maakt het mogelijk om een geheel van capaciteiten voor cybersecurity te besturen en de coherentie ervan te verzorgen:

- detectie van aanvallen op basis van geplaatste sondes binnen het informatiesysteem,
- verzamelen van informatie uit 'event' logs vanuit de diverse systeemcomponenten,
- correlatie en in perspectief brengen van alle verzamelde informatie om 'incidenttickets' op te stellen die een veiligheidsalarm kunnen genereren,
- analyse van de informatie en besturing van de operationele bestrijding, in samenspraak met de klant.

Deze belangrijke etappes in cybersecurity kunnen niet worden ontworpen zonder technische procedures en organisatorische maatregelen binnen het operatiecentrum voor cybersecurity, zoals het aflossen van de operators, het beheer van de incidenttickets, de traceerbaarheid van de actie, het vooruitlopen op nieuwe bedreigingen, internationale samenwerking, de opslag van de verzamelde informatie, het respecteren van het juridische kader, de autorisatie van de teams, de interne controle enz. Deze complexiteit die elk operatiecentrum eigen is, geldt vooral in de cyberspace, door de dichtheid van het verkeer en de dagelijks te verwerken hoeveelheid informatie.

DE ESSENTIE VAN HET BEHOUD VAN EEN VEILIGE OMGEVING

Elke detectie, correlatie, analyse en bestrijding heeft pas zin als de status van de IT-infrastructuur continue bekend is (de versies van de software, de configuraties, de structuren) en men in staat is om een veiligheidscorrectie of corrigerende maatregel toe te passen, bijvoorbeeld het wijzigen van een parameter om een aanval te blokkeren.

Cybersecurity berust ook op de capaciteit om de integriteit van een veiligheidssysteem voor langere tijd te garanderen. De eis van het permanente behoud van een veilige status is des te meer nodig omdat de cyberaanvallen gebruik maken van de kwetsbaarheid in systemen die snelle verspreiding mogelijk maken. Op het moment dat dit artikel verschijnt, zijn op internet meer dan 2000 zwakke punten gepubliceerd sinds het begin van 2010!

Thales heeft capabilities voor het behoud van een 'cybersecure' status teneinde te garanderen dat door de tijd heen, de randvoorwaarden voor deze veilige status blijven gelden. Deze capability is de basis van cybersecurity, het vormt de hoeksteen ervan.

CONCLUSIE: ER BESTAAN BEWEZEN OPLOSSINGEN VOOR REËLE ACTUELE DREIGINGEN

Hoewel de dreigingen en de problemen van de cyberspace alle aandacht krijgen, is de operationele realiteit van de cybersecurity onbekender. De realisatie van cybersecurity en het gebruik van gerelateerde (geïntegreerde) oplossing vereisen namelijk specifieke expertise en kennis. Dat vormt de waarde van de integrale aanbiedingen voor cybersecurity zoals CYBELS.