

Artikel "We hebben een firewall, dus onze beveiliging is geregeld!"

Door G.J. van Manen op donderdag 08 november 2007 11:36

Hoewel security experts weten dat er meer is dan een goed ingerichte firewall, IDS/IPS omgeving en ACL lijsten, schijnen veel managers toch nog de illusie te hebben dat hun ICT netwerk hiermee 'veilig' is. Natuurlijk helpt een firewall, maar 100% beveiligen is onmogelijk of in ieder geval een erg kostbare zaak en heeft toch echt meer voeten in de aarde. Door beveiliging op een integrale wijze aan te pakken kunnen de onderkende risico's met minder kosten worden afgedekt.

Willen we informatiebeveiliging goed regelen dan moeten we de taal spreken die managers spreken. De belangrijkste doelstelling voor iedere organisatie is overleven (*ook vaak continuïteit genoemd*). Voor iedere manager of directeur is dat wel duidelijk. Toch zie je deze doelstelling maar zelden expliciet terug in de jaarverslagen, missies en beleidsplannen van de organisaties. Om deze continuïteit te waarborgen moet de organisatie waarde toevoegen aan de producten en diensten die ze verkoopt. Michael Porter introduceerde hiervoor halverwege de jaren tachtig de zogenaamde "waardeketen" waarbij onderscheid gemaakt werd tussen de primaire en secundaire processen.



Figuur 1: Waardeketen van Porter

In de huidige wereld waar informatie overal en altijd beschikbaar moet zijn, wordt het ondersteunen van deze primaire en secundaire processen door ICT steeds belangrijker. Daarmee wordt beveiliging een 'hot item'. Maar we moeten doel (primaire en secundaire processen) en middel (ICT) niet door elkaar halen.

Om een voorbeeld te geven: Microsoft heeft onlangs een dienst gepresenteerd waarmee gebruikers medische dossiers digitaal beschikbaar kunnen stellen. Volgens Google's vice president of engineering hebben steeds meer instanties (medische) informatie nodig die beschikbaar is over patiënten, georganiseerd en toegankelijk voor iedereen. Persoonlijk maken wij ons hier zorgen over omdat beschikbaarheid één item is, maar daarnaast zijn ook de, exclusiviteit en integriteit belangrijke en bekende begrippen geworden. Of die nu echt geholpen zijn met het online beschikbaar stellen vragen wij ons af.

Informatiebeveiliging moet zich dan ook richten op de combinatie van beschikbaarheid, integriteit en exclusiviteit om zo de continuïteit van de organisatie, de bedrijfsprocessen en de informatie te waarborgen. Maar daarnaast moeten we wel rekening houden met wetgeving zoals een Wet Bescherming Persoonsgegevens.

Veel managers denken bij het horen van 'informatiebeveiliging' aan de knipperende lampjes op de firewalls. (*vooral als deze blauw zijn doen ze het erg goed! Wie op infosecurity is geweest heeft zelf kunnen zien dat de stands met de meeste lampjes de meeste bezoekers trokken*). Vergeten wordt vaak dat deze firewall (*een technische maatregel*) alleen zijn werk goed doet als ook de organisatorische, procedurele, bouwkundige en elektronische maatregelen geregeld zijn. Om nog maar niet te spreken over informatie die op een andere

manier de organisatie verlaat, we kennen allemaal de incidenten met USB-sticks en verloren laptops, daar helpt een firewall echt niet tegen.

Een simpel voorbeeld maakt duidelijk wat we bedoelen: als de verantwoordelijkheden niet zijn toegewezen zal de firewall snel een doos met mooie knipperende (liefst blauwe) lampjes zijn waar niemand naar om kijkt, hij staat er, de lichtjes branden dus hij doet het. Als het patch beleid niet is beschreven in procedures voert vervolgens niemand op tijd de juiste updates door waardoor er al snel een gatenkaas ontstaat, maar gelukkig de lichtjes blijven branden, dus we zijn veilig. Ook moeten we er natuurlijk voor zorgen dat onze firewall in een stevig gebouwde serverruimte staat en moeten we zorgen dat er een alarm afgaat als iemand die serverruimte openbreekt om de firewall te stelen. Kortom een combinatie van technische, procedurele, organisatorische, bouwkundige en elektronische maatregelen is noodzakelijk om de firewall goed en vooral veilig zijn werk te laten doen en de firewall is slechts één maatregel.

Hier komt een begrip om de hoek waarin de beveiligingsmaatregelen aan elkaar, aan de waardeketen van Porter en aan informatie- en fysieke beveiliging wordt gekoppeld zodat managers snappen wat we nu echt bedoelen: integrale beveiliging (ook wel comprehensive of enterprise security genoemd).

We beginnen met een definitie voor dit begrip:

Integrale beveiliging is de beveiliging van informatie (geautomatiseerde en niet geautomatiseerde data) en de fysieke beveiliging (beveiliging van materieel en personeel) om de continuïteit van de organisatie te waarborgen door, op basis van risicomanagement en een kosten/batenanalyse, technische, procedurele, organisatorische, bouwkundige en elektronische maatregelen te selecteren en te implementeren.

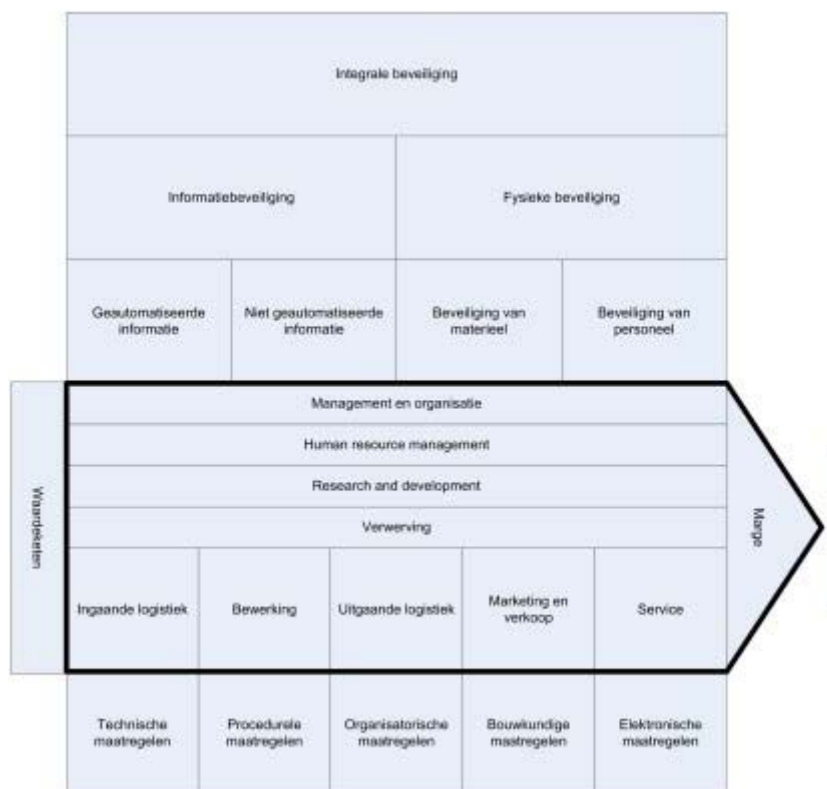
Dit klinkt natuurlijk goed, maar wat betekent het nu voor uw organisatie?

Door beveiliging op een integrale wijze aan te pakken ontstaat een pakket aan maatregelen dat afgestemd is op de specifieke situatie en processen van de organisatie. Uiteraard moeten deze maatregelen op basis van risicomanagement worden vastgesteld. Deze risico's moeten worden gewaardeerd, prioriteiten moeten worden gesteld en beslissingen moeten worden genomen over al dan niet te nemen beheersingsmaatregelen. We willen natuurlijk geen maatregelen nemen, maar risico's afdekken en het heeft weinig nut om een briefje van € 10,- te beveiligen met een kluis van € 1000,-.

We pleiten dan ook voor een benadering die begint bij de directie en waarbij managers zich af vragen:

- Wat moeten we beschermen?
- Waarom moeten we juist dat beschermen?
- Wat gebeurt er als we het niet goed beschermen?

Als deze vragen beantwoord zijn kunnen we met behulp van het integrale beveiligingsmodel de juiste maatregelen selecteren, implementeren en de status ervan monitoren. Wijzelf gebruiken hierbij graag het volgende model om duidelijk te maken waar we het over hebben.



Figuur 2: Integrale beveiliging

De verbetering van de integrale beveiliging gaat over alle producten, diensten, materialen, medewerkers en vestigingen van de organisatie. Het betreft alle bedrijfsprocessen van de organisatie (en de koppelvlakken met de klanten) om de continuïteit van de bedrijfsvoering te kunnen waarborgen. De kritieke processen, die per organisatie verschillen, verdienen hierbij natuurlijk de hoogste prioriteit. We kunnen allerlei mooie theorieën ontwikkelen en ideeën bedenken maar uiteindelijk gaat het erom op operationeel niveau maatregelen te implementeren waarmee we ook echt beter beveiligd zijn (dus toch die firewall, maar dan in combinatie met alle andere procedurele, organisatorische, bouwkundige en elektronische maatregelen). Het integraal beveiligingsbeleid, dat afgestemd is op het beleid, de missie en de doelstellingen van de organisatie, vormt het vertrekpunt voor alle beveiligingsmaatregelen.

Alle medewerkers moeten hun steentje bijdragen. Het heeft geen zin om duizenden euro's te besteden aan maatregelen, als de medewerkers ze niet snappen en ze niet uitvoeren (dan laten we de opzettelijke handelingen maar even buiten beschouwing, maar vergeet niet: de vijand zit ook intern daar helpt die firewall niet tegen). Het (top)management van de organisatie vervult een voorbeeldfunctie die nogal eens wordt onderschat. Als het management onvoldoende steun geeft aan de maatregelen (of ze zelfs probeert te ontlopen onder het mom van dat geldt niet voor mij als directeur) dan kan men niet van de medewerkers verwachten dat zij zich wel aan de regels houden. Beveiligingsbewustzijn moet zich niet alleen richten op de medewerkers, maar juist ook op de managers.

Kortom de integrale beveiliging is meer dan een stel knipperende blauwe lampjes op de firewall maar is een bedrijfskundige uitdaging die gebaseerd moet zijn op risicomangement. De coördinatie en eindverantwoordelijkheid voor beveiliging moet op een hoog niveau binnen de organisatie worden opgepakt. Het vereist een aanpak die zichtbare steun geniet van het management, daarbij steeds kijkend naar de kritieke bedrijfsprocessen voor de organisatie en die firewall kan één van de maatregelen zijn.

We moeten met zijn alle af van de 'whack a mole' cultuur, waarin we incidenten oplossen door er maar een dure appliance tegen aan te gooien. Laten we beginnen bij het kritisch beoordelen van onze kritieke processen en daar de technische, procedurele, organisatorische, bouwkundige en elektronische maatregelen op af stemmen.

Door ing. Godert Jan van Manen & drs. Thimo Keizer RSE, beide senior consultant bij [Northwave](#).

UBM Global: als hulpmiddelen voor organisaties en haar medewerkers ter voorkoming van dataverlies heeft DriveLock de volgende edities:

- *DriveLock Basic. Poort- en randapparaatcontrole en autorisatie plus netwerkprofielen.*
- *DriveLock Encryption. Versleutelen van informatie op verwijderbare drives.*
- *DriveLock Security Reporting Center. Verzamelen en rapporteren van DriveLock events.*
- *DriveLock Application Filter. Applicatiecontrole en -autorisatie.*
- *DriveLock Terminal Services. DriveLock functionaliteiten voor Terminal Server sessies.*