De essentie van het 'out of the box' security concept

Uit het KWINT document "Quick scan implementatie informatiebeveiligingsbeleid MKB" is gebleken dat het MKB behoefte heeft aan kennis en eenvoudige praktische methodes, om informatie beveiliging van de grond te krijgen. Beveiliging en Informatiebeveiliging beginnen vaak met een risico analyse. Gangbare risico analyse methodieken welke in informatie beveiliging worden gebruikt zijn onvoldoende toegesneden op het MKB. Om informatie beveiliging succesvol te kunnen inbedden in het MKB bedrijf is een eenvoudige risico analyse methodiek nodig die net als in BORG maatregelen in hoofdlijn en detail geeft.

BORG is een kwaliteitssysteem, zodat beveiligingsbedrijven garant kunnen staan voor het leveren van kwalitatief goede beveiligingsproducten en/of diensten. De risico analyse methodiek die BORG gebruikt is gebaseerd op een aantal tabellen waarmee eenvoudig het risico en de maatregelen in hoofdlijnen en detail kunnen worden bepaald. Wanneer een MKB bedrijf een inbraakdetectie systeem (beveiligingssysteem) wil aanschaffen dan komen zij in aanraking met BORG. Immers verzekeraars eisen van bedrijven een BORG certificaat. Dit certificaat krijgt men als het inbraakdetectie systeem is geleverd en geïnstalleerd door een BORG erkende beveiligingsbedrijf. De meeste BORG erkende beveiligingsbedrijf zijn vaak onvoldoende bekwaam om iets zinnigs over informatie beveiliging te kunnen adviseren en of te implementeren. Het verwijzen naar de Code voor Informatie beveiliging is iets wat met grote regelmaat gebeurt. Echter, kijkende naar de Code voor Informatie beveiliging en de daarin genoemde maatregelen zijn deze overvloedig en niet concreet genoeg.

'out of the box'

Met bewustwording en 'out of the box' maatregelen kunnen de risico's tot een voor het MKB aanvaardbaar niveau worden teruggebracht. In het document "Computer beveiliging voor ondernemers" uitgegeven door KWINT staat de volgende top 10 beveiligingsmaatregelen voor het MKB.

1. Opstellen en implementeren van beveiligingshuisregels internetten en een stappenplan voor de implementatie van maatregelen
2. Toewijzen van verantwoordelijkheid voor beveiliging
3. Lid worden van een waarschuwingsdienst
4. Tijdig installeren van softwarereparaties die zijn verkregen van een betrouwbare bron
5. Installeren, instellen en up-to-date houden van de virusscanners
6. Installeren en up-to-date houden van firewall(s), alsmede het regelmatig bekijken van het logboek van de firewall(s)
7. Fysieke beveiliging van de computer apparatuur
8. Frequent maken en testen van kopieën en deze op een veilige plek opbergen
9. (externe)Ontwikkelaars van bedrijfswebsite wijzen op belang van beveiliging in de ontwerpfase
10. Laat de beveiliging testen door een vertrouwd iemand die onafhankelijk is van degene die verantwoordelijk is beveiliging

Uitgaande van deze top 10 en de in het document genoemde voorbeelden moet het mogelijk zijn om een 'out of the box' security concept te maken. De meeste van de hierboven genoemde maatregelen kunnen, zelfs zonder een risico analyse, worden gezien als een noodzakelijk kwaad. De maatregelen zoals genoemd in het document 'Computer beveiliging voor ondernemers' zijn praktische zaken zoals een virusscanner, een firewall, een back-up mechanisme maar ook zaken zoals beveiligingshuisregels.

Critici

Nu zullen de critici opmerken dat virusscanners, firewalls en back-up mechanisme geconfigureerd en ge-update moeten worden. In principe is dat juiste, echter wat is er mis met de standaard instellingen (default) van dit soort middelen? Bovendien hebben virusscanner en firewalls automatische update faciliteiten. Was het een aantal jaren geleden nog zo dat default instellingen, security ellende veroorzaakt, dank zij de leercurve die de producenten en hun gebruikers doorgemaakt hebben, is dit niet meer zo. De default instelling geven een gemiddeld beveiligingsniveau, wat voor de gemiddelde MKBer voldoende is.

Conclusie

De BORG erkende beveiligingsbedrijven kunnen met een 'out of the box' security concept de eerste stap in de richting van Integraal BeveiligingsLeverancier zetten. Voor de technische beveiligingsbedrijven liggen de uitdagingen voor de toekomst in IP netwerken en hun beveiliging. Immers toegangsverleningssystemen, CCTV systemen en inbraakdetectie systemen worden meer en meer IP oriented. «

Bronnen: www.kwint.org