Cybersecurity en het MKB: de praktijk

Hoe kwetsbaar is de ruggengraat van de verbonden samenleving?

Highlights

- De ICT-afhankelijkheid van derden in het MKB is groot en urgent.
- De samenleving is in belangrijke mate afhankelijk van MKB'ers.
- Capgemini Consulting heeft in samenwerking met Interpolis, een CyberPreventieDienst voor het MKB ontwikkeld, langs de klassieke drie dimensies van organisatie, mensen & middelen en technologie.
- Met name de dimensie 'organisatie' is weinig ontwikkeld bij MKB'ers.
- De dimensie 'technologie' is beter geregeld, hiervoor worden meestal derden ingeschakeld.

De toenemende connectiviteit van Nederland zorgt voor veel economische voordelen. Nergens in Nederland is de digitalisering zo groot als in de MKB-sector. Maar bij digitale transformatie hoort ook digitale veiligheid. Dus hoe zit het met de cybersecurity van MKB-bedrijven? Over cybersecurity in het MKB bestaat weinig feitelijke kennis. Door enkele tientallen cybersecurityscans in de praktijk uit te voeren, hebben Capgemini en Interpolis deze kennis wel. Deze scans (CyberPreventieDiensten) tonen aan dat beleid over het algemeen voor verbetering vatbaar is, en dat het regelmatig uitvoeren van penetratietesten (pentesten) absoluut essentieel is om te weten in hoeverre men weerbaar is tegen digitale dreiging en of dienstverleners en leveranciers goed werk leveren.

De rol van het MKB in relatie tot cybersecurity is traditioneel onderbelicht. Er is nog maar weinig onderzoek gedaan naar de beveiliging van de systemen die gebruikt worden door bedrijven in het MKB, die 90% van de bedrijven in Nederland vormt en voor een flink deel de economische activiteit bepalen[1]. Daarom is het essentieel dat er meer aandacht komt voor de (digitale) veiligheid van deze organisaties.

Op landelijk niveau is al langer aandacht voor het belang van cybersecurity in het MKB. In het Cybersecuritybeeld Nederland 2016 wordt gesteld: “Het MKB neemt, ten opzichte van grotere bedrijven, relatief weinig maatregelen op het gebied van cybersecurity[2].” Daarmee is de ruggengraat van de Nederlandse economie kwetsbaar. Maar hoe kwetsbaar?

Sinds 2014 hebben de adviseurs van Capgemini Consulting in samenwerking met verzekeraar Interpolis de CyberPreventieDienst opgezet[3]. Hierbij worden MKB-bedrijven doorgelicht op acht verschillende kerngebieden. Deze acht gebieden zijn: beleid en aansturing, beveiliging informatie, bewustwording en training, wet- en regelgeving, processen, fysieke beveiliging, toegang bedrijfsnetwerk en internet/web. Ook wordt de technische staat van de netwerken door een technische scan (een zogenaamde ‘pentest’) beproefd.

De verbonden samenleving manifesteert zich het duidelijkst in burgers en bedrijven die hun activiteiten steeds meer online ontplooien en verwachten dat dit veilig kan. Keer op keer blijkt dat de cybersecurity van Nederlandse bedrijven (van multinational tot de bakker om de hoek) afhankelijk is van veilige verbindingen.

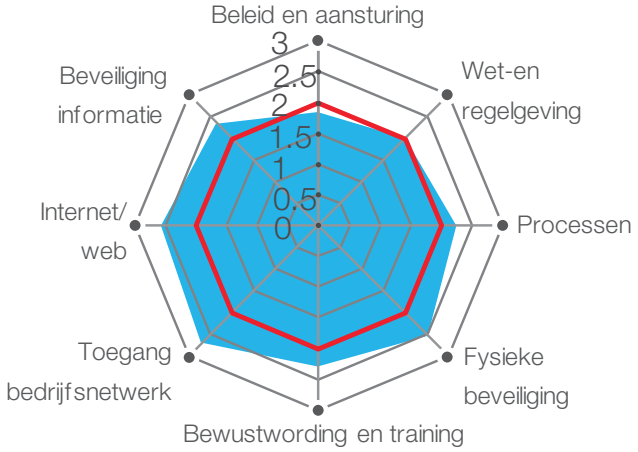
In 2015 hebben Interpolis en Capgemini Consulting het onderzoek ‘Cybersecurity in het MKB’[4] uitgevoerd, naar de stand van zaken omtrent cybersecurity binnen het midden- en kleinbedrijf. Uit dit onderzoek komt naar voren dat ongeveer de helft van de ondervraagde bedrijven gebruik maakt van digitale betalingsvormen, zoals creditcardbetalingen of online betalingsmogelijkheden. Ook maakt ongeveer de helft van deze bedrijven gebruik van intellectueel eigendom en/of vertrouwelijke gegevens. 32% van MKB-ondernemers verwacht dat het bedrijfsrisico dat zij lopen met betrekking tot cybersecurity in de komende vijf jaar zal stijgen. Met name de doelgroepen zakelijke dienstverlening, detailhandel en industrie komen naar voren als sectoren die grotere risico’s zien op digitaal vlak.

Op basis van dit onderzoek hebben Capgemini Consulting en Interpolis de CyberPreventieDiensten geïntensiveerd en uitgerold. De aanpak die is ontwikkeld, is op concrete aanbevelingen gericht langs de klassieke drie dimensies van organisatie, mensen & middelen en technologie (‘people, process & technology’). Deze dimensies zijn uitgewerkt in een achttal kerngebieden en vervolgens in een pilot bij een vijftal ondernemers uitgevoerd. De drie dimensies staan centraal bij de interviews en informatieverzameling. Het resultaat wordt hierna geanalyseerd en de aanbevelingen worden gekoppeld aan de zogenoemde ‘gaps’ die gevonden zijn tijdens de analyse.

In de afgelopen twee jaar is de CyberPreventieDienst enkele tientallen keren uitgevoerd. Daarmee is het mogelijk om een eerste verkenning te doen van de resultaten van de uitgevoerde CyberPreventieDiensten. Hiervoor is een speciale benchmark ontwikkeld die inzicht geeft in de weerbaarheid van de deelnemende ondernemers en een vergelijking op sectorniveau voor enkele sectoren mogelijk maakt. Zo kan een individuele ondernemer zien hoe zijn eigen onderneming scoort ten opzichte van het gemiddelde van de deelnemende ondernemers, en vaak dus zijn concurrenten.

De bedrijven die zijn opgenomen in de benchmark kunnen gecategoriseerd worden onder de volgende sectoren: retail, overheid, financial, industrie, dienstverlening en horeca/entertainment. Mogelijke antwoorden op de vragen waren: of men bepaalde maatregelen niet, ad hoc, deels of geheel heeft geïmplementeerd. Met bijbehorende scores van 0-3. Een score van 2 (deels) vormt naar ons idee de gewenste baseline voor cybersecurity.

Figuur 1: Cybersecurity Benchmark



(Rood is de baseline)

Bron: Uitkomsten CyberSecurity Benchmark, N=26.

[1]https://www.interpolis.nl/~/media/files/ebook_cybersecurity_in_het_mkb.pdf

[2]https://www.ncsc.nl/binaries/content/documents/ncsc-nl/actueel/cybersecuritybeeld-nederland/cybersecuritybeeld-nederland-2016/1/CSBN2016.pdf

[3]https://mijn.interpolis.nl/zakelijk/preventiediensten/paginas/cyberpreventiedienst.aspx

[4]https://www.interpolis.nl/~/media/files/ebook_cybersecurity_in_het_mkb.pdf

Als op hoofdlijnen gekeken wordt naar de resultaten, valt op dat de bedrijven over het algemeen boven de gestelde baseline scoren. Zeker op de gebieden fysieke beveiliging, toegang tot het bedrijfsnetwerk en de beveiliging van de website scoren de ondervraagde partijen een voldoende. Bedrijven zorgen ervoor dat ICT-faciliteiten en informatiebronnen goed fysiek zijn afgeschermd tegen ongeoorloofde toegang, zoals door een afgesloten deur. Toegang tot het bedrijfsnetwerk is afgeschermd door bijvoorbeeld het WiFi-netwerk te beveiligen met een wachtwoord en het gastennetwerk grondig af te schermen van het reguliere netwerk. De deelnemende bedrijven investeren vaak in hun digitale omgeving door een externe partij in dienst te nemen die hun netwerk, digitale dienstverlening en werkplekken inricht en bijhoudt, waarmee externe expertise wordt binnengehaald. Hiermee ontstaat ook het risico van 'wegmanagen': het cyberrisico zou, nu het technisch belegd is, van de agenda kunnen verdwijnen.

Bij het organisatorisch inrichten van de bedrijfsprocessen schort het echter vaak aan een duidelijke visie vanuit de bedrijfsleiding en prioriteiten en de (interne) communicatie over deze visie (kerngebied 'beleid en aansturing'). Omdat de urgentie van het onderwerp ontbreekt, wordt ook 'bewustwording en training' van het eigen personeel een zwakke plek, die pas wordt onderkend als er een incident binnenshuis of een groot schandaal optreedt. Diverse bedrijven die deelnamen aan de CyberPreventieDienst bleken ook te weinig aandacht te geven aan het voldoen aan wet- en regelgeving omtrent cybersecurity en privacy. Sinds 2016 moeten bijvoorbeeld alle Nederlandse organisaties voldoen aan de Meldplicht Datalekken, en hiervoor een procedure hebben ingericht. Zo'n procedure is vrijwel nergens aanwezig. Op specifieke wettelijke of andere juridische vereisten waaraan verwerking van informatie in de organisatie moet voldoen, wordt over het algemeen ook laag gescoord.

Naast de gecontroleerde vragenlijst, is bij vrijwel iedere deelnemende organisatie een pentest uitgevoerd. De meeste organisaties kennen een aantal kritieke kwetsbaarheden, waaronder verouderde versies van besturingssystemen. Hoewel dit niet direct deel is van de gepresenteerde benchmark, onderstreept dit terugkerende fenomeen de noodzaak van een regelmatige scan van de digitale omgeving.

Conclusie

De praktijk van cybersecurity in het MKB in Nederland toont dat nog veel te winnen is. De eerder genoemde uitspraak van het NCSC, dat 'het MKB relatief weinig maatregelen op het gebied van cybersecurity (neemt)', kan als volgt geïnterpreteerd worden: op technisch vlak worden maatregelen vaak wel getroffen, maar deze worden niet getest en op organisatorisch vlak gebeurt er weinig.

MKB-bedrijven ontplooien steeds meer activiteiten online en vertrouwen hierbij vaak op externe dienstverleners om de technische aspecten af te dichten. Zaken als fysieke beveiliging, toegang tot het bedrijfsnetwerk en de beveiliging van de website zijn vaak uitbesteed en hiermee naar een aantal criteria op papier 'geregeld'. Het regelmatig testen van de staat van deze beveiligingsmaatregelen is echter vaak een blinde vlek.

Op vijf van de acht kerngebieden (beleid en aansturing, beveiliging informatie, bewustwording en training, wet- en regelgeving en processen) kunnen MKB-bedrijven nog een flinke slag maken om hun (digitale) veiligheid op een hoger volwassenheidsniveau te brengen.

Een aanpak gericht op de grootste risico's, voortkomend uit inzicht in waar de belangen van de organisatie liggen, is hierbij cruciaal om de juiste maatregelen te nemen. Weten waar de gaten zitten, is essentieel om deze te kunnen dichten. Organisaties hebben vaak een blinde vlek voor hun zwaktes, want ze denken hun risico's te hebben afgedicht door deze uit te besteden.

Over de auteurs

Dr. Dana Tiggelman en Drs. Melle van den Berg zijn security consultants bij Capgemini Consulting. Melle is gespecialiseerd in cybersecurity en crisisbeheersing en is hoofdauteur van het onderzoek MKB en Cybersecurity uit 2015. Dana is gespecialiseerd in cybersecurity en intelligence. Tim Wells MSc is security analist bij Schiphol Group. Hij houdt zich bezig met de operationele veiligheid van alle processen binnen de terminals en de innovatie van veiligheid. Ir. Margot Hol is business consultant bij Interpolis en doet ontwikkeling van preventiediensten.




Voor meer informatie kunt u contact opnemen met de auteurs via:
dana.tiggelman@capgemini.com,
www.linkedin.com/in/danatiggman en
melle.vanden.berg@capgemini.com,
www.linkedin.com/in/mellevdberg,
@mellevdberg, tim.wells@schiphol.nl
www.linkedin.com/in/timwells90 ,
margot.hol@achmea.nl
www.linkedin.com/in/margot-hol-977969115