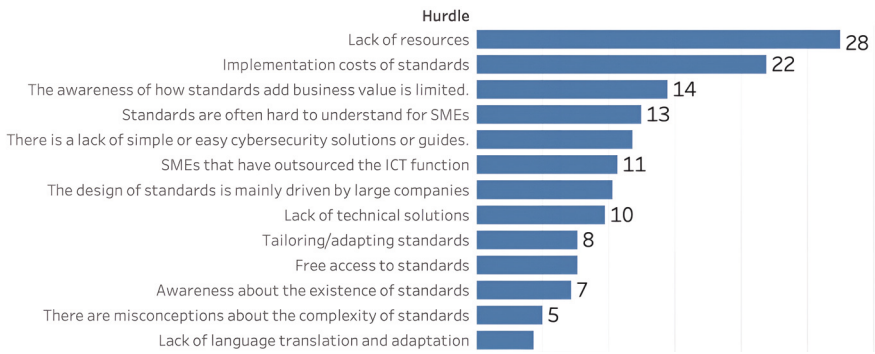
Auteur: Vincent van Dijk is eigenaar van Security Scientist en is bereikbaar via vincent@securityscientist.net. Dit artikel is geschreven op persoonlijke titel.

Cybersecurityinzichten voor het mkb

Midden- en kleinbedrijven (mkb) zijn de drijfveer van de meeste economieën op de wereld (1): ongeveer 99% van de economische activiteiten binnen Europa zijn te herleiden naar het mkb (2). Het doorgaans lage eigen vermogen van het mkb maakt hen gevoelig voor risico's (3); 60% van de cyberaanvallen zorgt voor een faillissement bij het mkb (4).

Het beveiligen van het mkb is dus belangrijk. Toch is er weinig aandacht voor cybersecurity bij het mkb. Cybersecurityframeworks, en standaarden zijn niet gericht op kleinere bedrijven, en wetenschappelijk onderzoek heeft tot nu toe ook (te) weinig aandacht gegeven aan dit thema (5). Het afgelopen jaar heb ik samen met de Antwerp Management School onderzoek gedaan naar cybersecurity bij het MKB. In dit artikel deel ik drie inzichten van dat onderzoek.



Figuur 1 - Puntenverdeling door onderzoekdeelnemers over 13 hindernissen.

Inzicht 1 - Factoren die de implementatie van een standaard verhinderen

Om de impact van cyberrisico's te verminderen, moeten organisaties hun niveau van cybersecurityvolwassenheid afstemmen op het risico dat ze bereid zijn te nemen. Echter, heeft het mkb niet de middelen om volwassenheid te kunnen bereiken (5). En dat heeft grote gevolgen voor het mkb, maar eveneens bij grotere organisaties omdat bij 99% van de economische activiteiten het mkb actief is.

Omdat het mkb dus zo economisch actief, is het van belang dat het mkb digitaal veiliger wordt. Alleen kan het mkb dat niet enkel op eigen kracht. Hulp zou kunnen komen in de vorm van subsidies, niet ter beschikking gestelde tools van grote organisaties of door ondersteuning van banken en hun netwerken. Om richting te geven zouden er ook duidelijkere standaarden gemaakt kunnen worden voor het mkb. Zo is het European Digital SME Alliance onder andere bezig met het ontwikkelen van standaarden (6).

Accountancy, een branche die al volwassen is in het stellen van internationale standaarden, heeft ook aanpassingen aan de standaarden gemaakt voor het mkb. Toen de Financial Reporting Standard (ISRS) gepubliceerd werd, bleek dat het implementeren van deze standaard niet ten goede kwam aan het mkb, vooral omdat kleinere bedrijven niet over passende middelen beschikken. Uiteindelijk publiceerde de International Accounting Standards Board (IASB) een aangepaste standaard voor het mkb. In een publicatie van de European Digital SME Alliance worden 13 hindernissen opgesomd die het voor de midden- en kleinbedrijven moeilijk maken om een standaard te implementeren (7). Tijdens een onderzoeksessie gaven de deelnemers met behulp van een puntensysteem aan welke van deze hindernissen het meest verstorend waren.

Twee hindernissen staken uit boven de rest:

1. Gebrek aan middelen;
2. De kosten voor het implementeren van de standaard.

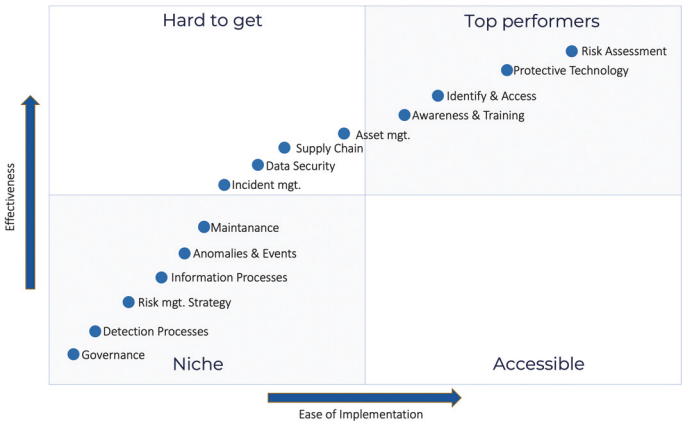
Het gebrek aan middelen en de kosten van implementatie blijken veruit de grootste hindernissen te zijn voor het invoeren van een cybersecuritystandaard bij het mkb. Om het probleem om te lossen zou het mkb beter geïnformeerd moeten worden om de juiste prioriteiten te stellen. Daarnaast zouden grotere organisaties het mkb kunnen steunen door informatie en middelen te delen met het mkb.

Inzicht 2 - Focus

In het onderzoek hebben experts de categorieën van het NIST Cybersecurity Framework beoordeeld. Elke categorie werd geëvalueerd op effectiviteit en het gemak van implementatie. Hieruit is het `SMB Cybersecurity Quadrant' ontstaan (figuur 2). Dit Quadrant onthult welke maatregelen effectief zijn en welke juist helemaal niet. Zo blijkt uit het onderzoek dat een riscoassessment de beste categorie is om te implementeren. In tegenstelling blijkt `governance' niet goed te scoren in een mkb-context. De maatregelen bij het mkb moeten vooral praktisch en simpel zijn en niet te veel middelen kosten.

Het Quadrant legt vier focuspunten bloot voor goede cybersecuritymaatregelen voor het mkb:

1. Risicoassessment;
2. Protective Technology;
3. Identity & Access;
4. Awareness & Training.



Figuur 2 - SMB Cybersecurity Quadrant (V. van Dijk, 2022).

Risicoassessment

Het merendeel van de lezers heeft wel eens een risicoassessment gedaan. Toch worden deze assessments vaak overgeslagen bij het mkb. Een risicoassessment werkt bij het mkb namelijk ook net wat anders dan gebruikelijk. Bij het mkb is het handig om risico niet alleen te zien als 'kans maal impact'. Gebruik in plaats daarvan de ISO-definitie: 'The effect of uncertainty on objectives' (het effect van onzekerheid op de doelstellingen).
Je kunt een risicoassessment bij het mkb in drie simpele stappen doen. Ga niet te veel de diepte in, want dan sla je de plank mis:

1. Bepaal de doelstellingen van het bedrijf;
2. Bepaal de doelstellingsonzekerheden;
3. Zoom daarna in op de (cyber)risico's.

Bedenk dat dit niet betekent dat je als ondernemer enkel oog moet hebben voor de (cyber)risico's, maar er juist op moet letten dat je het bedrijf als geheel (holistisch) blijft bekijken. Het mkb behandelt namelijk alle risico's onder de algemene bedrijfsvoering; zonder de bedrijfsrisico's kun je geen goede vergelijking maken. En zonder een goede vergelijkingsbasis wordt het nemen van goede beslissingen lastig. Het kan namelijk zo zijn dat een hoog risico buiten de cyberspace meer aandacht en budget nodig heeft dan een cyberrisico.

Protective Technology

Na het nagaan van je risico's is het tijd om aan de slag te gaan met protective technology. Met andere woorden: securityproducten die je gemakkelijk kunt implementeren en waarnaar je weinig omkijken hebt. Denk hierbij aan firewalls, endpoint protection, backups en managed cybersecurityservices.
Zorg ervoor dat de kosten die je maakt logisch zijn. Gemiddeld genomen heeft het mkb een winstmarge van 5 tot 10%. Als we uitgaan van 10% betekent dit, dat een midden- en kleinbedrijf met 10 miljoen euro omzet, 1 miljoen euro winst maakt. Een securityoplossing van 100.000 euro per jaar snoept dan dus meteen 10% van de winst weg en is wellicht niet rationeel qua omvang!

Identity & Access

Meestal heb je bij kleinere bedrijven geen extra producten nodig om Identity & Access goed te regelen. Identity & Access gaat namelijk vooral om het invoeren van een goed en sterk proces, waarbij de toegang wordt goedgekeurd en er een overzicht is van de uitgegeven rechten, gebruikers en applicaties. Met een eenvoudig maar degelijk proces kun je bij het mkb prima besparen op je maatregelen, omdat je niet per se nieuwe technologie hoeft aan te schaffen.

Awareness & Training

Awareness & Training is een categorie van maatregelen waarvoor je niet per se dure technologie hoeft aan te schaffen. Zo kun je 1 à 2 personen opleiden tot security champions. Deze champions kunnen de awareness en trainingen geven en daarnaast vragen beantwoorden. In plaats van trainingen zou je ook kunnen denken aan coaching. Het is een optie om security champions maandelijks te coachen bij het uitvoeren van hun training en awareness-activiteiten.

Inzicht 3: Flexibiliteit by design

Het mkb staat bekend om zijn flexibiliteit. In tegenstelling tot grote organisaties, kan het mkb zichzelf eenvoudiger en sneller veranderen. En dat moet ook wel: flexibiliteit is één van de meest gewaardeerde eigenschappen van het mkb. De huidige zakelijke omgeving is ingewikkeld en lastig te voorspellen, dus bedrijven moeten flexibel zijn om te blijven draaien. In de snelle en altijd veranderende wereld van vandaag is het vermogen van een organisatie om te veranderen een concurrentievoordeel. Mee veranderen met de omgeving is voor het voortbestaan van het mkb essentieel. De wetenschap ondersteunt het idee dat het mkb flexibel moet zijn. Uit onderzoek blijkt bijvoorbeeld dat er vanuit strategisch oogpunt een positieve connectie bestaat tussen

strategische flexibiliteit en de prestaties van het mkb. Cyberbeveiligingsstrategieën moeten ook flexibel zijn, zodat midden- en kleinbedrijven zich kunnen aanpassen aan het dynamische karakter van de bestaande en toekomstige risico's.
Uit onderzoek is gebleken dat een cybersecuritystrategie flexibel moet zijn by design, oftewel, de focus moet vanaf het begin op flexibiliteit liggen (5). Op basis van deze criteria is er een flexibele aanpak ontstaan: het Cybersecurity Canvas. Met dit Canvas kan je pragmatisch een cybersecuritystrategie opstellen.

Figuur 3 - Een voorbeeld van Cybersecurity Canvas dat is opgesteld tijdens een workshop met 20 Vlaamse gemeentes.

Het Cybersecurity Canvas bestaat uit twee componenten:

- Aan de linkerkant het bedrijf;
- Aan de rechterkant de maatregelen.

Aan de linkerkant, binnen de bedrijfscomponent, wordt de vraag gesteld: waarom? Waarom moet het bedrijf zich bezighouden met cybersecurity? Daarnaast worden de risico's genoemd. De rechterkant houdt zich bezig met de maatregelen. Deze worden gekozen op basis van de meest effectieve categorieën aan de hand van de specifieke risico's die de organisatie ervaart.

Conclusie

Ongeveer 99% van de economische activiteiten binnen Europa zijn te herleiden naar het mkb (2), maar het mkb kan zichzelf op het moment niet goed beveiligen (5). Meer organisaties moeten betrokken worden bij het beveiligen van het mkb. Zo zouden grotere organisaties maatregelen en informatie kunnen delen met de midden- en kleinbedrijven met wie ze zaken doen.

Hulp zou ook kunnen komen in de vorm van subsidies of gratis middelen vanuit grote organisaties.
Daarnaast moet cybersecurity anders aangepakt worden bij het mkb. Het beveiligen van het mkb werkt namelijk net wat anders. Het mkb heeft een pragmatische, simpele en flexibele aanpak nodig (8). Om richting te geven zouden er ook duidelijkere standaarden gemaakt kunnen worden voor het mkb die pragmatisch, eenvoudig en flexibel zijn.
De nieuwe aanpak moet focus aanbrengen op de vier meest effectieve NIST-categorieën (9). Zo zullen we het mkb en daarmee ook de (Nederlandse) economie een stukje veiliger maken.

Referenties

(1) Burgstaller, J., & Wagner, E. (2015). How do family ownership and founder management affect capital structure decisions and adjustment of SMEs? *Journal of Risk Finance

(2) Gama, A. P. M., & Geraldes, H. S. A. (2012). Credit risk assessment and the impact of the New Basel Capital Accord on small and medium-sized enterprises. Management Research Review, 35(8), 727–749.

(3) Altman, E. I., Sabato, G., & Wilson, N. (2008). The Value of Non-Financial Information in SME Risk Management. https://doi.org/10.2139/ssrn.1320612

(4) Munro, D. 2013. A Guide to Financing SMEs. New York: Palgrave Macmillan.

(5) van Dijk, V. (2022, July 4). Research - A cybersecurity standard for SME. Security Scientist. https://www.securityscientist.net/blog/research-a-cybersecurity-standard-for-sme/

(6) Zie https://www.digitalsme.eu/

(7) European Digital SME Alliance. (2020). *The EU Cybersecurity Act and the role of standards for SMEs*. https://www.digitalsme.eu/digital/uploads/The-EU-Cybersecurity-Act-and-the-Role-of-Standards-for-SMEs.pdf

(8) Het is goed om bewust ervan te zijn dat het MKB een speciale cybersecurity aanpak nodig heeft. Dat is de conclusie uit het onderzoek. De speciale aanpak bestaat uit een pragmatische, simpele en flexibele aanpak. Het resulteerde in twee prachtige gereedschappen: het "SMB Cybersecurity Quadrant" en het "Cybersecurity Canvas". https://www.securityscientist.net/blog/research-a-cybersecurity-standard-for-sme/

(9) Het Quadrant legt vier focuspunten bloot voor goede cybersecuritymaatregelen voor het MKB: 1. Risk Assessment 2. Protective Technology 3. Identity & Access 4. Awareness & Training