Auteurs: Vincent van Dijk en Chris de Vries. Vincent van Dijk is eigenaar van Security Scientist en is bereikbaar via vincent@securityscientist.net. Chris de Vries is redacteur van het IB Magazine en daarnaast eigenaar van De Vries *Impuls* Management, hij is bereikbaar via impuls@euronet.nl

Hulpgids beveiliging voor het kleinbedrijf (deel 1)

Beveiliging van informatie (data), programmatuur (software), apparatuur (hardware) en ruimte (kantoren) tegen onbevoegden (‘hackers’) en tegen onbedoeld, abusievelijk, naïef handelen (personen/personeelsleden) is de kern van veilig digitaliseren. Elke ondernemer weet dat en ook dat er een oerwoud aan programma’s, apparatuur, handleidingen en adviseurs zijn om je daarmee te helpen.

Er zijn echter beperkingen, te weten: de (relatief) hoge prijzen voor programma’s en apparatuur. De hoge consultancy kosten en de tijd die je als ondernemer er zelf in moet stoppen, terwijl het je vak niet is en *zeker niet je liefde!* Voor instanties, overheden, groot- & middenbedrijven vaak geen probleem, maar voor de kleinbedrijven zeker wel. Vandaar het woordgebruik ‘relatief’.
De overheid, instanties en grootbedrijven spreken daarbij vaak over de ketenafhankelijkheden en de risico’s die daarvan uitgaan. En dus stellen ze eisen aan hun keten, voldoe je er niet aan (!?) … vergeet dan je kansen maar! Eisen zijn simpel, maar er aan bijdragen dat ook de kleinere partner mee kan doen, dat is andere koek. Die koek gaat uit van het kosten-denken, het denken aan sleutel-partners en aan kortstondige winstverlagingen. En wie zijn die kleinbedrijven eigenlijk, een ‘quantités negligeables’!?

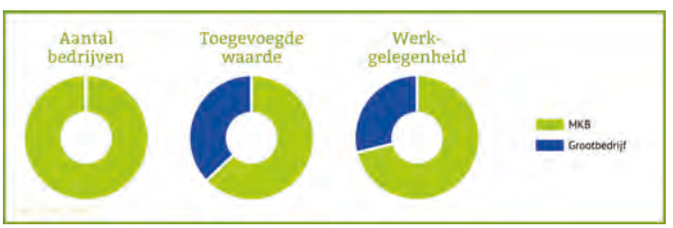
Het kleinbedrijf

De auteurs van dit artikel zien het kleinbedrijf zeker niet als een verwaarloosbare grootheid. Het is ons uitgangspunt dat juist de overheid, instanties en grootbedrijven medeverantwoordelijkheid moeten dragen om kleinbedrijven beter beschermd te laten zijn tegen de groot-hacker-machten. Dus eerst maar even ingaan op wat kleinbedrijf-getallen (uitgezonderd bedrijven met meer dan vijftig werkzame personen):

OK, wij weten dat er een groot aantal kleinbedrijven zijn, maar wat betekent dat nu in omzet? Wel in 2011 stond het MKB-bedrijf voor 888 miljard euro aan omzet en in 2020 voor 1.023 miljard euro aan omzet, dat betekent een groei van 135 miljard euro (15,2%) (2). De MKB-bedrijven zijn goed voor 71% van de Nederlandse werkgelegenheid in 2020 (3) en bijna 60% aan de Toegevoegde Waarde voor onze economie (4).

Werkzame personen	2007.Kw.1	2017.Kw.2	Toe-/afname
1	619.565	1.213.055	+593.490
2	158.445	176.905	+18.460
3 tot 5	81.295	89.490	+8.195
5 tot 10	60.100	62.940	+2.840
10 tot 20	32.635	31.280	-1.355
20 tot 50	20.280	18.865	-1.415
Totaal bedrijven	972.320	1.592.535	+620.215

Bron: Deels bewerkte cijfers, ontleend aan CBS, StatLine MBK, gewijzigd 13.01.2023 (1)



Figuur 1: Economisch belang aandeel mkb (5).

Er zijn in 2023 2,16 miljoen mkb-bedrijven in Nederland. In 2007 waren dat er 1,05 miljoen (6). De positieve/negatieve gang van zaken binnen het kleinbedrijf vertaalt zich in het aantal vacatures. In 2020, kwartaal 1, waren dat er in het kleinbedrijf 57.100. In 2022, kwartaal 3, circa 129.100: een groei dus van 126,1 procent (7). De vacatures bij het MKB, grootte 0-50 werkzame personen, in die jaren (2020 Kw.1 - 2022.Kw.3) waren respectievelijk 70.000 en 107.000 (een stijging van 52,9 procent) (7).

Ons uitgangspunt

Wij menen dat het niet zo kan zijn dat een zo belangrijk deel van het Nederlands macro-economisch belang vanuit data- en ketenveiligheid alsook privacy zo veronachtzaamd wordt. Dit omdat diezelfde groep ondernemingen ICT-organisatie technisch nu eenmaal achterloopt in kennis, (praktijk)vaardigheden en inzichten.

Drie stappen

De auteurs willen in een artikelenreeks de navolgende weg vervolgen:

1. zij begeleiden de ondernemers op hun weg tot Informatie- & Ketenveiligheid;
2. zij doen dat door middel van een vraag- en antwoordaanpak en
3. zij vertrouwen erop dat het midden-, grootbedrijf, de instanties en de overheid meedoen.

1. Ondernemingsbegeleiding
   Wij zullen ondernemers, met name via de artikelen, vertrouwd maken met vrij beschikbare gereedschappen, vanaf de logboeken in hun computersystemen, over de `firewalls/routers/ switches' e.a. apparatuur tot en met Open Source dan wel betaalbare beveiligingssoftware.

2. Vraag & antwoord (in slecht Nederlands: `Q&A')
   Wij zullen vragen in onze artikelenreeks behandelen, welke wij of zelf ter illustratie stellen, dan wel vragen die via het LinkedIn-account van het Platform voor InformatieBeveiliging (PvIB) (8) binnenkomen. Op dat platform zullen wij thema's aankondigen, vragen stellen of vragen ontvangen van de lezer(s) van ons magazine dan wel van lezers van de LinkedIn pagina.

   Ook kun jij suggesties doen met betrekking tot thema's dan wel in rechtstreekse discussie met ons gaan of onze hulp inroepen. Ook zal op de artikelenreeks teruggegrepen worden om de inhoud daarvan te verduidelijken, tips van anderen te delen en verdere uitdieping van de onderwerpen te realiseren.

ACTIEVE INTERACTIE met jullie is gewenst en wordt nagestreefd

3. Wij streven ernaar dat op basis van deze artikelenreeks de grote, professionele organisaties (GO en NGO) hun kans waarnemen om op basis van bewustwording van de problematiek van het kleinbedrijf:
   - gratis kennis te delen,
   - programma's (software) te sponsoren of te schenken,
   - seminars en/of webinars te organiseren met ons (enkel gericht op het kleinbedrijf),
   - hun eigen ketens door te lichten en te zien hoe zij die in de praktijk kunnen steunen.
   En zo zullen er nog wel meer ideeën opduiken, zoals wij ook met universiteiten, hoge scholen en andere onderwijsinstellingen een samenwerking stimuleren.

Tot zover onze vooroverwegingen, nu dan het begin van de artikelenreeks.

De Start

Beste Vincent, als 'security scientist', kijkende naar het kleinbedrijf en uitgaande van zelfstandige computers, laptops, printers, smart-pad en -telefoon; wat zou de eerste stap zijn voor de ondernemer die zijn kennis over beveiliging van data, privacy en apparatuur wil verbeteren?

"Om te beginnen is het belangrijk te begrijpen wat cyberbeveiliging inhoudt. In de bedrijfsvoering heb je altijd een basisbegrip nodig van meerdere onderwerpen zoals onder andere: verkoop, marketing, netwerken. Hetzelfde geldt voor cybersecurity, eerst moet je een goed gevoel krijgen voor wat dát nu echt is.

In mijn eigen bedrijf hielp het mij om korte afspraken te maken met experts, die uit konden leggen over welke onderwerpen ik meer moest weten, dat kan ook voor cybersecurity. Je kan het ook zelf (willen) doen en het internet opgaan om een basisidee te krijgen over cybersecurity. Tegenwoordig kun je ook zelfs met online AI tools - zoals ChatGPT - het gesprek aan gaan. Maar wees je er dan wel van bewust dat deze gereedschappen nog aan het begin van hun ontwikkeling staan en naast zeer zinnige adviezen, opmerkingen en suggesties ook nog fouten kunnen maken. Vaar er dus niet blind op!

Wanneer je een begrip heb gekregen van cybersecurity, kun je overgaan naar de tweede vraag: waarom heb ik cybersecurity nodig? Door die vraag te beantwoorden kun je richting geven aan wat je precies wil beschermen. Ben je bang voor de veiligheid van jouw data, van jouw systemen, voor systemen en processen welke echt nooit zouden mogen omvallen? Van

daaruit rol je natuurlijk in de vraag en jouw antwoord: welke cyberrisico's zijn voor mij belangrijk?"
Vincent, het is duidelijk dat de eerste stappen je tot het besef (kunnen) leiden dat er cyberrisico's zijn, maar hoe kom je erachter welke risico's dat zijn en welke de belangrijkste zijn? Waar moet ik beginnen?
"Risico's kun je met behulp van allerlei handige gereedschappen inventariseren. Ik adviseer om het simpel te houden en eerst zelf te beginnen met het opschrijven van de risico's die je zelf denkt te lopen op het gebied van cybersecurity. Dit doe je vooral om zélf met het onderwerp te worstelen. Dit worstelen helpt je focus aan te brengen, om later de juiste taken uit te besteden dan wel zelf te doen.
Door alle vragen te beantwoorden maak je een begin met de cybersecuritystrategie. In de Cybersecurity Canvas (9), een tool waarmee je een cybersecuritystrategie in 1 slide kunt ontwerpen, zou je met voorgaande stap de linkerkant ingevuld hebben.

Figuur 2: Cybersecurity Canvas opgesteld door de auteur, V. van Dijk.

Dan kun je beginnen met de rechterkant: hoe ga ik deze risico's verminderen? Online kun je tal van maatregelen vinden. Echter, het wordt vrij snel technisch en de mogelijkheden zijn eindeloos. Dit is het juiste moment een expert te betrekken.
Na beantwoording van voorgaande vragen heb je een goed beeld verkregen van wat je precies wilt. Je kunt de expert de juiste vragen stellen. Daarnaast verneemt die van jou de benodigde kaders voor het goed (kunnen) meedenken.

Kies je er toch voor om het zelf te doen dan raad ik je aan om te kijken naar de **C**enter for **I**nternet **S**ecurity Critical Security Controls (**CIS** Controls), een geprioriteerde lijst van 18 maatregelen verdeeld over basis, fundamentele en organisatorische groepen (10).

Op het moment dat je de benodigde maatregelen in kaart hebt, kun je een stappenplan opzetten. Je kunt het stappenplan zo uitgebreid maken, zoals je wilt, maar ik raad aan om het advies van schrijver Patrick Bet-David ter harte te nemen en een 5-stappenplan (ten aanzien van 'Clarity, Strategy, Growth Tactics, Skills & Insight') te definiëren (11)."
Je hebt de eerste fase beschreven van het realiseren van cyberveiligheid binnen het eigen mkb-bedrijf. Zou je een uitdaging aan de lezer willen/kunnen doen welke wij op de PvIB-LinkedIn pagina dan wel in het volgende artikel kunnen opvolgen?

"Ik zou de lezer willen uitdagen om terug te gaan naar de basis en te bedenken waarom je met cybersecurity bezig bent vanuit het perspectief van de organisatie. Is het omdat je je zorgen maakt over mogelijke risico's, vereisten van belangrijke stakeholders of omdat je een goede indruk wilt achterlaten bij de klant.

Ook als grote organisatie, die al druk met cybersecurity bezig is, is het goed te reflecteren waarom je met cybersecurity bezig bent – wat is belangrijk? Dit geeft het benodigde inzicht om een cybersecurity-programma te starten, prioriteiten aan te passen en om mensen mee te krijgen in jouw activiteiten.
Ik ben heel benieuwd waarom mensen nu echt met cybersecurity aan de slag gaan. Ik nodig je uit om me een bericht te sturen met daarin je redenen (voor zover je die mag delen)."

Referenties

(1) https://mkbstatline.cbs.nl/#/MKB/nl/dataset/48015NED/line?dl=30B3
(2) https://www.staatvanhetmkb.nl/livechart/economisch-belang-banner-omzet-mkb
(3) https://www.staatvanhetmkb.nl/livechart/economisch-belang-banner-werknemers-mkb
(4) https://studiozakelijk.nl/hoe-belangrijk-is-het-mkb-voor-de-nederlandse-economie/ , hun website 13.06.2018
(5) https://www.staatvanhetmkb.nl/livechart/economisch-belang-banner-aantal-mkb-bedrijven
(6) https://mkbstatline.cbs.nl/#/MKB/nl/dataset/48013NED/line?graphtype=-Line&ts=1498474760139
(7) https://mkbstatline.cbs.nl/#/MKB/nl/dataset/48013NED/line?graphtype=Line&ts=-1498474760139 en https://mkbstatline.cbs.nl/#/MKB/nl/dataset/48013NED/table?ts=-1677668553426
(8) https://www.linkedin.com/search/results/all/?fetchDeterministicClustersOnly=-false&heroEntityKey=urn%3Ali%3Agroup%3A133202&keywords=pvib%20-%20platform%20voor%20informatiebeveiliging&origin=RICH_QUERY_SUGGESTION&position=1&searchId=bb89db86-3e58-484c-86b7-cd71a0dc056a&sid=t~)
(9) https://www.securityscientist.net/content/files/2022/11/Cybersecurity-Canvas.pdf
(10) https://www.cisecurity.org/controls
(11) Your next five moves, master the art of Business Strategy;22.07.2021; auteurs Patrick Bet-David en Greg Dinkin – 320 pagina's, EAN code: 9781982154813 / ISBN: 1982154810; (Paperback € 11,09 bol.com d.d. 23.01.2023)