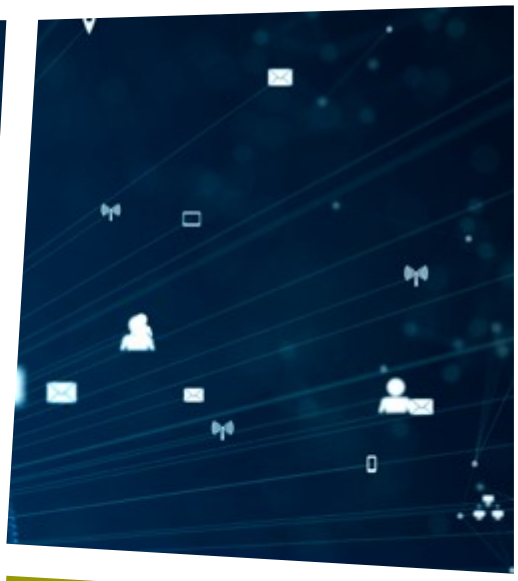
Cybersecurity in het mkb

Nulmeting



Raoul Notté

Lisanne Slot

Susanne van 't Hoff-de Goede

Rutger Leukfeldt

Centre of Expertise Cybersecurity

let's change
YOU. US. THE WORLD.

DE HAAGSE
HOGESCHOOL

INHOUDSOPGAVE

1. Aanleiding en doel

Het Nederlandse bedrijfsleven is in hoge mate gedigitaliseerd. In 2016 had 91 procent van de Nederlandse bedrijven toegang tot internet, een percentage dat sindsdien alleen maar is toegenomen.[1] Minstens de helft van de bedrijven doet betalingen online en beheert digitaal vertrouwelijke gegeven.

Door deze digitalisering zijn Nederlandse bedrijven ook vatbaar geworden voor cyberaanvallen, zoals het middels ransomware versleutelen van bestanden of het platleggen van een website via een DdoS aanval. Dergelijke aanvallen kunnen grote consequenties hebben voor bedrijven: van het verliezen van belangrijke data tot het platleggen van het bedrijfsproces. De schade van online criminaliteit voor de Nederlandse economie in 2014 besloeg ongeveer 1,5% van het BNP is, dus € 8,8 miljard.[2] Uit een analyse van Deloitte blijkt dat cybercriminaliteit Nederlandse bedrijven en de overheid jaarlijks ongeveer 10 miljard euro kost.[3]

Het bovenstaande probleem van cybersecurity is mogelijk nog problematischer voor het midden- en kleinbedrijf (mkb). Het mkb vormt de ruggengraat van de Nederlandse economie. Er zijn meer dan 1 miljoen mkb-bedrijven in Nederland, die gezamenlijk zorgen voor meer dan drie miljoen banen en een totale omzet van 858 miljard euro.[4] Deze grote groep mkb'ers, met een belangrijke rol in de Nederlandse economie, blijkt echter relatief vaak slachtoffer van cyberaanvallen te worden.[5] Dit probleem wordt versterkt doordat het mkb onvoldoende middelen, kennis en toegang tot kennis heeft om cyberdreigingen te onderkennen en zich vervolgens weerbaar te maken. Basale beveiligingsmaatregelen, zoals het updaten van software, het gebruik van sterke wachtwoorden of het maken van back-ups van belangrijke bestanden, worden vaak niet genomen.[6] Tenslotte liggen ondernemers met name wakker van sociaaleconomische ontwikkelingen. Mkb-ondernemers achten zichzelf veelal niet interessant genoeg voor cybercriminelen en zien online criminaliteit niet als een van de belangrijkste risico's voor de organisatie. Door het hierboven beschreven risico van onvoldoende kennis, middelen, genomen maatregelen en risicobewustzijn lijkt cybersecurity een aanzienlijk probleem voor het mkb en daarmee de Nederlandse samenleving in zijn geheel.

Exact om deze reden is in 2017 het lectoraat cybersecurity in het mkb van start gegaan. Het doel van dit lectoraat is om de kennispositie van het mkb op het gebied van online criminaliteit en cybersecurity te vergroten en zo het slachtofferschap en de impact van cyberaanvallen onder mkb'ers te verlagen.[7] Omdat er nagenoeg geen eerdere studies zijn gedaan naar cybersecurity in het mkb , zullen eerst basale vragen beantwoord moeten worden. Dit rapport bevat de uitkomsten van een van deze verkennende studies, die zicht richt op de beantwoording van basale vragen als: welk percentage van de mkb-bedrijven is al slachtoffer geworden en wat voor maatregelen nemen mkb'ers om zich te beschermen tegen cyberaanvallen?

Leeswijzer

In hoofdstuk 2 zijn de onderzoeksvragen van dit onderzoek uiteen gezet, eveneens als de dataverzameling in analysemethoden.
In hoofdstuk 3 zijn de resultaten van dit onderzoek beschreven.
Hoofdstuk 4 bevat de conclusie van deze studie.

1 CSR (2016). *De economische en maatschappelijke noodzaak van meer security. Nederland digitaal droge voeten.* CRS.
2 McAfee (2014). *Net Losses: Estimating the Global Cost of Cybercrime. Economic impact of cybercrime II.* Center for Strategic and International Studies.
3 Deloitte (2016). *Cyber value at Risk in the Netherlands.* Deloitte.
4 Zie voor de meest actuele cijfers van het CBS: https://www.staatvanhetmkb.nl/factsfigures.
5 Veenstra, S., Zuurveen, R., & Stol, W. (2015). *Online criminaliteit onder bedrijven: Een onderzoek naar slachtofferschap van online criminaliteit onder het Midden- en Kleinbedrijf en Zelfstandigen Zonder Personeel in Nederland.* NHL Hogeschool/Politieacademie/ Open Universiteit.
6 Munnichs , G., Kouw, M., & Kool, L. (2017). *Een nooit gelopen race: Over cyberdreigingen en versterking van weerbaarheid.* Rathenau instituut, Den Haag.
7 Leukfeldt, E.R. (2018). *De 'Human' Factor in Cybersecurity. Intreerede Lectoraat Cybersecurity in het MKB.* Den Haag: De Haagse Hogeschool.

2. Data en methode

In dit hoofdstuk wordt verantwoord hoe dit onderzoek naar online criminaliteit en cybersecurity in het mkb tot stand is gekomen en is uitgevoerd.

2.1. Onderzoeksvragen

Dit rapport heeft als doel het uitvoeren van een "nulmeting". Deze nulmeting moet inzicht geven in de stand van zaken met betrekking tot cybersecurity en slachtofferschap van online criminaliteit in het mkb. Om deze doelstelling te behalen staan de volgende onderzoeksvragen centraal in dit onderzoek:

1. *Welke technische en organisatorische cybersecurity-maatregelen worden genomen door mkb-bedrijven om slachtofferschap te voorkomen?*
2. *Wat is de prevalentie van slachtofferschap van online criminaliteit in het mkb?*
3. *Welke organisatiekenmerken of risicovol gedrag zijn van invloed op het slachtofferschap van het mkb?*

2.2. Onderzoeksinstrument

Het onderzoeksinstrument van de huidige studie is een vragenlijst die mede tot stand is gekomen door literatuuronderzoek en deels is gebaseerd op vragenlijsten uit eerdere studies.[8] [9] Daarnaast is de vragenlijst verder ontwikkeld via bijdragen van verschillende experts, die mee hebben gewerkt aan het opstellen van vragen over onderwerpen waar niet eerder meetinstrumenten voor zijn ontwikkeld. Er zijn gesprekken gevoerd met 12 experts uit het werkveld. Op basis van deze gesprekken is een nieuw meetinstrument ontwikkeld en voorgelegd aan de experts. Tenslotte is de uiteindelijke vragenlijst in samenwerking met studenten Information Security Management aan de Haagse Hogeschool getest. De volledige vragenlijst is in de bijlage opgenomen. De volgende onderdelen zijn opgenomen in de vragenlijst:

Kenmerken organisatie

Het eerste onderdeel van de vragenlijst richt zich op de kenmerken van de organisatie, zodat op basis van deze kenmerken mogelijk een duiding of verklaring van de resultaten gegeven kan worden. Respondenten is bijvoorbeeld gevraagd aan te geven hoe groot het bedrijf en de omzet is, of uit welke sector het bedrijf afkomstig is.

IT infrastructuur

Een omschrijving van de stand van zaken me betrekking tot cybersecurity is niet compleet zonder inzicht in de IT infrastructuur van deze bedrijven. Om een beeld te geven van de IT Infrastructuur van bedrijven zijn organisaties gevraagd naar de wijze waarop de bedrijfsserver wordt beheerd en is gevraagd naar de wijze van omgang met enkele IT aspecten die cyberrisico's kunnen opleveren: het aanbieden van Wi-Fi aan klanten, het koppelen van privé apparatuur aan het bedrijfsnetwerk (Bring Your Own Device) en het gebruik van Internet of Things apparatuur (hierna: IoT).

Naast de mogelijkheden die IoT mkb-ers biedt om de efficiëntie en effectiviteit te vergroten, biedt IoT ook kansen voor cybercriminelen. Onveilige IoT apparaten kunnen worden besmet, gebruikt om het bedrijfsnetwerk binnen te dringen of worden misbruikt voor cyberaanvallen op derden. Onveilige IoT zorgt in beperkte mate voor een dreiging richting de (mkb) eigenaren van de apparatuur. Groter is het probleem dat besmette apparaten als onderdeel van een botnet misbruikt worden om aanvallen uit te voeren op derden, zoals DDoS-aanvallen.[10] De afgelopen jaren waarschuwden verschillende securityexperts over de toenemende dreiging veroorzaakt door kwetsbaarheden van IoT apparatuur, die over het algemeen een matige tot slechte beveiliging blijken te hebben. [11] [12]

Deze gebrekkige veiligheid van IoT wordt mede veroorzaakt door het gebruik van standaardwachtwoorden en zwakke wachtwoorden, het ontbreken van encryptie, het ontbreken van software-updates om kwetsbaarheden te verhelpen en basale ontwerpfouten.

8 Domenie, M.M.L., E.R. Leukfeldt, J.A. van Wilsem, J. Jansen & W.P. Stol (2013) *Victims of offenses with a digital component among Dutch citizens. Hacking, Malware, personal and financial crimes mapped.* The Hague: Eleven International Publishers.

9 Veenstra, S., Zuurveen, R., & Stol, W. (2015). *Online criminaliteit onder bedrijven: Een onderzoek naar slachtofferschap van online criminaliteit onder het Midden- en Kleinbedrijf en Zelfstandigen Zonder Personeel in Nederland.* NHL Hogeschool/Politie Academie/ Open Universiteit.

10 Nationaal Coördinator Terrorismebestrijding en Veiligheid (2017). *Cybersecuritybeeld Nederland 2017*. Den Haag: Ministerie JenV/NCTV.

11 Nationaal Coördinator Terrorismebestrijding en Veiligheid (2017). *Cybersecuritybeeld Nederland 2017*. Den Haag: Ministerie JenV/NCTV.

12 Networkworld (2017). Hackers found 47 new vulnerabilities in 23 IoT devices at DEF CON. Geraadpleegd via: https://www.networkworld.com/article/3118759/hackers-found-47-new-vulnerabilities-in-23-iot-devices-at-def-con.html

De afgelopen jaren is er meerdere malen misbruik gemaakt van deze kwetsbaarheden en zijn IoT-apparaten als middel ingezet voor het uitvoeren van aanvallen. Daarnaast zijn in enkele gevallen apparaten misbruikt om gebruikers ervan af te luisteren of de omgeving van de gebruikers te manipuleren.[13] Om deze reden is gevraagd of respondenten de veiligheid van deze apparatuur standaard meenemen in overwegingen over aanschaf en implementatie.

Cyber security maatregelen

In de lijst met maatregelen die genomen kunnen worden om de digitale aspecten van de onderneming te beveiligen, wordt onderscheid gemaakt tussen puur technische maatregelen en maatregelen die gericht zijn op het gedrag van de organisatie en het personeel. Samenvattend staat in dit onderzoek het geheel van de volgende set technische en organisatorische cybersecurity maatregelen centraal:

Organisatorische en beleidsmatige maatregelen
Er is een schriftelijke weergave aanwezig van de huidige IT infrastructuur
Er zijn scenario's ontwikkeld waarin is beschreven hoe het bedrijf slachtoffer kan worden van online criminaliteit.
Er is een protocol opgesteld waarin is beschreven hoe te handelen bij online criminaliteit.
Er is informatiebeveiligingsbeleid aanwezig.
Er worden regelmatig (veiligheids)audits uitgevoerd.
Werknemers worden bewust gemaakt van online risico's.
Werknemers hebben geleerd om geen e-mail van potentieel onbetrouwbare afzenders te openen
Werknemers hebben geleerd om goed op te letten bij het doen van online betalingen.
Werknemers hebben geleerd geen gevoelige informatie op internet te verstrekken.
Werknemers moeten verschillende, sterke wachtwoorden voor online accounts gebruiken.
Het is verplicht om wachtwoorden met regelmaat te wijzigen.
Er zijn (schriftelijke) regels opgesteld over het gebruik van IT voor privé doeleinden.
Er zijn (schriftelijke) regels opgesteld voor het doen van online betalingen.
Er zijn (schriftelijke) regels opgesteld over het omgaan met vertrouwelijke informatie, zoals persoonsgegevens van u, uw medewerkers en klanten.
Er zijn (schriftelijke) regels opgesteld over het openen van onbekende bestanden (zoals bijlagen in e-mails).
Er zijn (schriftelijke) regels opgesteld over het (op verzoek) afgeven van bedrijfsgegevens.

Technische maatregelen
De computers van het bedrijf zijn voorzien van een virusscanner
De virusscanner(s) is (/zijn) up-to-date
De computers / het netwerk van het bedrijf zijn/is voorzien van een firewall
De firewall(s) is(/zijn) up-to-date
Het (draadloze) netwerk is beveiligd
De software op het bedrijfsnetwerk wordt up-to-date gehouden
(Internet)activiteiten op het bedrijfsnetwerk worden geregistreerd (gelogd)
De logs worden (regelmatig) bekeken/geëvalueerd
Er worden regelmatig back-ups gemaakt van bestanden op computers en/of het bedrijfsnetwerk
Back-ups worden (ook) buiten het bedrijfspand opgeslagen
Bestanden met vertrouwelijke informatie worden versleuteld opgeslagen (bijvoorbeeld middels encryptie)
Bestanden met vertrouwelijke informatie worden versleuteld verzonden (bijvoorbeeld middels encryptie)
Er wordt gebruik gemaakt van biometrische beveiligingsmethoden, zoals vingerafdruklezers

Risicomanagement

Een goede cybersecurity vereist risicomanagement: het analyseren en inschatten van de risico's dat het bedrijf loopt, om maatregelen te implementeren die passend zijn op deze risico's. Passend betekent dat de voor de organisatie vitale informatie en systemen sterker worden beveiligd dan minder cruciale zaken. Onder beveiligen is immers niet wenselijk, evenals teveel uitgeven aan minder essentiële beveiliging.

De perceptie van risico's is voor risicomanagement essentieel. Om een inschatting te maken van deze risicoperceptie is bedrijven gevraagd naar de impact die online criminaliteit op de organisatie zou hebben, afgezet tegen de inschatting van de waarschijnlijkheid dat slachtofferschap van een cyber incident zich voordoet. Ten slotte is bedrijven gevraagd of zij vertrouwen hebben in de genomen maatregelen om deze risico's te mitigeren.

Slachtofferschap en schade

Om een inschatting te maken van het slachtofferschap is respondenten een lijst voorgelegd van incidenten en is gevraagd of deze zich hebben voorgedaan binnen het bedrijf. Wanneer een incident zich heeft voorgedaan, is gevraagd of het bedrijf schade heeft ondervonden aan dit incident. Een bedrijf is in dit onderzoek als slachtoffer van online criminaliteit aangemerkt indien er een incident met schade is gerapporteerd.

13 Nationaal Coördinator Terrorismebestrijding en Veiligheid (2017). *Cybersecuritybeeld Nederland 2017*. Den Haag: Ministerie JenV/NCTV.

2.3. Steekproef

De digitale vragenlijst is tussen medio 2016 en medio 2017 uitgezet door 19 verschillende brancheorganisaties, die gezamenlijk ruim 200.000 leden vertegenwoordigen. Het uitzetten van de vragenlijst is door de brancheorganisaties op verschillende wijze gedaan, naar gelang hun wensen en mogelijkheden. De vragenlijst is bijvoorbeeld door brancheorganisaties uitgezet via een directe e-mailuitnodiging aan hun leden, opgenomen in nieuwsbrieven of gedeeld op de webpagina van de brancheorganisatie. Door deze verschillende manieren van verspreiden is het niet mogelijk een indicatie te geven van het bereik van deze uitnodigingen en daarmee de respons per branche.

In totaal zijn er 799 volledige vragenlijsten ingevuld, door directeuren (79,1%), IT eindverantwoordelijken/medewerkers (11,4%), of overige medewerkers (9,5%). In onderstaande tabel is te zien hoeveel respondenten per branche hebben geparticipeerd en welk percentage van de totale respons deze branche vertegenwoordigd.

Tabel 1: Aantal respondenten per branche.

Brancheorganisaties	Aantal	Percentage
KHN	35	4,4%
ADFIZ	61	7,6%
BGNU	19	2,4%
HISWA	43	5,4%
NBOV	23	2,9%
UNETO-VNI	112	14,0%
VHG	59	7,4%
FME	24	3,0%
Nederlandse Veiligheidsbranche	10	1,3%
AEDES	54	6,8%
Verbond van Verzekeraars	21	2,6%
Koninklijk Nederlands Vervoer	2	0,3%
BOVAG	120	15,0%
LTO	57	7,1%
RECRON	42	5,3%
VAN	7	0,9%
VGB	4	0,5%
VACO	51	6,4%
Metaalunie	55	6,9%
Totaal	**799**	**100,0%**

De totale groep van 799 respondenten wordt in dit rapport aangeduid met "mkb Nederland", maar betreft feitelijk een afspiegeling de 19 deelnemende brancheorganisaties. Bij een respons van 799 mkb bedrijven uit deze brancheorganisaties, die gezamenlijk ruim 200.000 leden vertegenwoordigen moet rekening worden gehouden met een mogelijke selectiviteit van de steekproef. In dit onderzoek is uitgegaan van een betrouwbaarheidsniveau van 95% voor de resultaten van deze studie, hierbij moet rekening gehouden worden met een foutmarge van 3,46%. Dit betekent dat de lezer een mogelijke spreiding van 3,64% kan aanhouden op de vermeldde percentages in dit rapport. Gegeven de respons, en de mogelijke selectiviteit dienen resultaten voorzichtig te worden geïnterpreteerd.

De afspiegeling van bedrijven op basis van het aantal medewerkers verschilt van de brede populatie van mkb-ers in Nederland. In dit onderzoek wordt onderscheid gemaakt tussen micro- (<10 medewerkers), klein- (10-49 medewerkers) of midden-klein (>50) bedrijven. In tabel 2 is weergegeven in welke proporties deze groepen vertegenwoordigd zijn in dit onderzoek, afgezet tegen het percentage dat deze groep uitmaakt van het totaal van mkb-bedrijven in Nederland.[14] De klein en midden-kleinbedrijven zijn in dit onderzoek oververtegenwoordigd, microbedrijven zijn ondervertegenwoordigd. De ondervertegenwoordiging van micro bedrijven is met name te verklaren door het lage percentage eenmansbedrijven (zzp'ers) in de respons van dit onderzoek (9,1%) ten opzichte van het aandeel eenmansbedrijven in de gehele onderzoekspopulatie (74%).

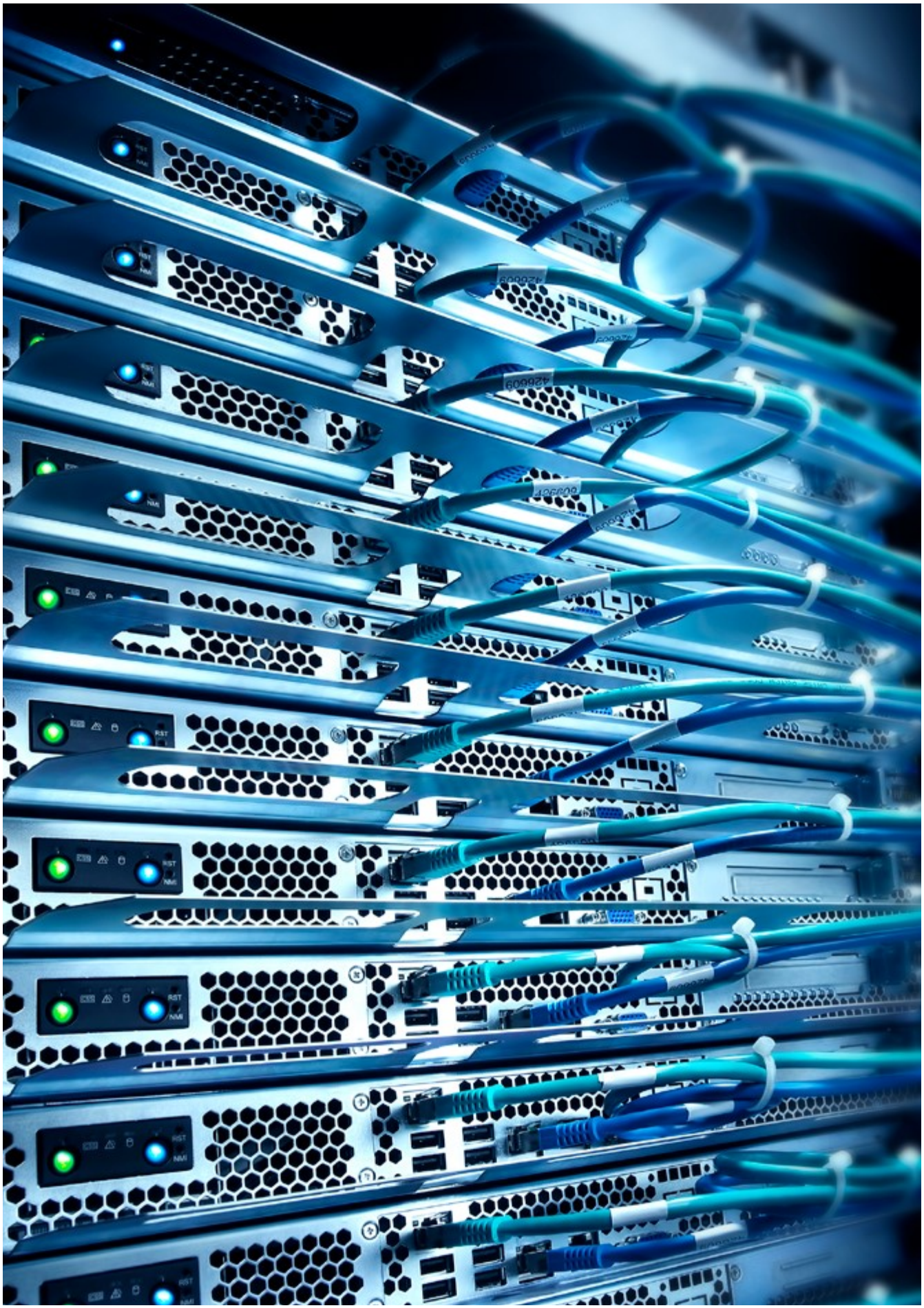
Tabel 2. Grootte van bedrijven in de steekproef en algemene populatie

	Respons 0-meting		CBS (2018)
	Aantal	Percentage	Percentage
Micro (<10 medewerkers)	457	57,6%	96,1%
Klein (10 – 49 medewerkers)	244	30,7%	3,2%
Midden-klein (50 – 250 medewerkers)	93	11,7%	0,7%

2.4 Data analyse

Dit rapport maakt grotendeels gebruik van beschrijvende statistieken om de onderzoeksvragen te beantwoorden. Daarnaast is gebruik gemaakt van enkele correlatie analyses om de samenhang tussen slachtofferschap en kenmerken van mkb bedrijven te onderzoeken. In het statistische softwareprogramma SPSS zijn analyses gedaan om Pearson's R te berekenen, een correlatiecoëfficiënt. Een correlatiecoëfficiënt ligt altijd tussen 0 en 1 (of -1) en geeft de mate weer waarmee twee factoren samenhangen. Een r van rond de 0 geeft aan dat twee factoren niets met elkaar te maken lijken te hebben, terwijl een r van (bijna) 1 aangeeft dat twee factoren volledig samenhangen. Of een correlatie ook betekenisvol is hangt af van het significantieniveau. Wanneer een correlatie significant is kan met 95% (*, p<0.05) of 99 procent (**, p<0.01) zekerheid worden vastgesteld dat het gevonden verband niet aan toeval te wijten is. Daarnaast is dit onderzoek een statistische analyse gedaan van verschillen tussen bedrijven op basis van het aantal medewerkers, zoals verdeeld in de groepen micro, klein en midden-klein door gebruik te maken van de chi-kwadraattoets. Deze verschillen zijn wanneer significant (p<0.05) weergegeven.

14 CBS (2018). *Statline; Bedrijven & Bedrijfstak, 3e kwartaal 2018*. Geraadpleegd via: https://opendata.cbs.nl/statline/#/CBS/nl/dataset/81589NED/table?ts=1536150654830



3. Resultaten

In dit hoofdstuk zijn de resultaten uit de kwantitatieve dataverzameling weergeven. Hierbij is, waar mogelijk, onderzocht of er significante verschillen bestaan tussen micro- (<10 medewerkers), klein- (10-49 medewerkers) of midden-klein (>50) bedrijven. Indien significante verschillen zijn gevonden, is hiervan melding gemaakt.

3.1. Infrastructuur

In deze pararaaf volgt een beschrijving van de IT-infrastructuur van het midden-kleinbedrijf.

3.1.1. Serverbeheer

De server van het bedrijfsnetwerk is de centrale plek van waaruit diensten aan clients (desktops, laptops en andere devices) worden aangeboden. De meerderheid van de bedrijven geeft aan dat zij de server laten beheren door een externe IT-specialist (62,4%). Kleine bedrijven laten de server vaker beheren door een externe IT-specialist (76,4%) dan micro bedrijven (54.9%) (p<.001). Slechts een kleine groep heeft een interne IT-specialist (8,0%), de midden-klein bedrijven hebben dit overigens vaker (21,5%) dan micro bedrijven (3,8%) (p<.001), mogelijk omdat zij meer middelen beschikbaar hebben om dit intern te organiseren (p<.001).

Tabel 3: Hoe wordt de server van uw bedrijf beheerd? (N=790)

Antwoordoptie	Percentage
Dat doe ik zelf	23,5%
Door een interne IT-specialist	8,0%
Door een externe IT-specialist	62,4%
Anders	6,1%

3.1.2. Wi-Fi

De draadloze netwerkverbinding is het toegangspunt tot het eigen bedrijfsnetwerk en is belangrijke knooppunt voor de cybersecurity van het bedrijf. De toegang tot het eigen bedrijfsnetwerk moet goed beveiligd zijn Respondenten is daarom gevraagd of derden ook toegang hebben tot het eigen bedrijfsnetwerk en of dit op een veilige manier gebeurt.

De meerderheid van de bedrijven (62,9%) stelt derden zoals klanten of gasten in staat om van het internet gebruikt te maken. Een overgrote meerderheid van deze bedrijven (41,2%) geeft deze klanten of gasten direct toegang tot het eigen bedrijfsnetwerk. Ongeveer een kwart van de bedrijven (21,7%) geeft aan dit via een speciaal gasten netwerk mogelijk te maken, de meest veilige vorm om deze dienst aan gasten te leveren. Midden-klein bedrijven bieden vaker Wi-Fi aan via een speciaal gasten netwerk (55,9%) dan kleine en micro bedrijven (p<.001). Bijna de helft van de bedrijven (41,2%) staat dus toe dat gasten direct het bedrijfsnetwerk kunnen benaderen, een groot potentieel risico voor de digitale veiligheid.

Tabel 4: Kunnen derden (zoals klanten) via het netwerk van uw bedrijf internet benaderen? (N=784)

Antwoordoptie	Percentage
Nee, wij bieden geen Wi-Fi aan	23,6%
Nee, wij hebben een speciaal gastennetwerk hiervoor	21,7%
Ja	41,2%
Weet ik niet	13,5%

3.1.3. Bring Your Own Device

Gasten of klanten zijn niet de enigen die een bedrijf toegang kan verlenen tot zijn bedrijfsnetwerk. De meerderheid van de bedrijven stelt eveneens haar medewerkers in staat om gebruik te maken van privé apparaten in het bedrijf (Bring Your Own Device). Iets minder dan de helft van de bedrijven staat toe dat deze apparaten direct gekoppeld worden aan het bedrijfsnetwerk (46,9%). Het risico hiervan is dat deze medewerkers malafide software die zij op een (mogelijk onbeveiligd) thuisnetwerk hebben gedownload, mee kunnen nemen het bedrijfsnetwerk in. Binnen micro bedrijven kunnen privé apparaten vaker aan het bedrijfsnetwerk gekoppeld worden (51,9%) dan in kleine (41,6%) en midden-klein bedrijven (38,7%) (p<.001).

Tabel 5: Maakt men binnen het bedrijf gebruik van privé apparaten die gekoppeld worden aan het bedrijfsnetwerk? (N=798)

Antwoordoptie	Percentage
Ja	46,9%
Nee	53,1%

Ook het privé gebruiken van zakelijke apparatuur kan, volgens de zelfde argumentatie, een risico vormen. De grootste groep bedrijven staat eveneens toe dat zakelijke apparaten in het bedrijf voor privé doeleinden worden gebruikt (71,2%).

Tabel 6: Worden zakelijke apparaten in uw bedrijf privé gebruikt? (N=562)

Antwoordoptie	Percentage
Ja	71,2%
Nee	24,4%
Weet ik niet	4,4%

3.1.4. IoT

Behalve apparaten die voornamelijk bedoeld zijn voor kantoorautomatisering en/of communicatie is in kaart gebracht of bedrijven ook andere apparaten hebben die met internet zijn verbonden. Deze zogenaamde 'Internet of things' (IoT) apparatuur brengt, zoals in hoofdstuk 2 beschreven, veel mogelijkheden en nieuwe toepassingen met zich mee. Anderzijds bestaat er grote zorg over de beveiliging van deze apparatuur. Meer dan de helft van de bedrijven (59%) geeft aan met IoT apparatuur te werken, voor verschillende doeleinden.

Tabel 7: Zijn er binnen uw bedrijf nog andere apparaten verbonden zijn met internet? (N=437)

Antwoordoptie	Percentage
Ja	59%
Nee	41%

De meest gebruikte vorm van IoT apparatuur in het mkb blijkt op dit moment gebouwbeheer systemen, zoals online beveiligingscamera's en hek- en sluitwerk. Micro bedrijven hebben minder vaak IoT apparatuur voor gebouw beheer systemen (36,3%) dan bedrijven met meer medewerkers (p<.001).

Eén op de vijf bedrijven heeft IoT apparaten die specifiek gebruikt worden voor het primair productieproces aangesloten op het netwerk, zoals bijvoorbeeld een online machine om staal te smelten of 3D printer. Midden-kleine bedrijven hebben vaker IoT apparatuur ten behoeve van het primaire proces (36,4%) dan bedrijven met minder medewerkers (p<.001).

Tenslotte gebruikt een kleine minderheid IoT apparatuur voor industriële controle of procesbeheersing (bestuur- en bewaking van productieprocessen). Slechts één op de drie bedrijven geeft aan geen IoT apparatuur te willen gaan gebruiken - dit percentage ligt hoger (45,3%) bij micro bedrijven (p<.001).

Mkb bedrijven werken vaak (nog) niet volgens security by design, waarbij er bij de aanschaf en implementatie van nieuwe systemen vooraf nagedacht wordt over de veiligheid hiervan. Midden-klein bedrijven geven vaker aan al volgens security by design (28,2%) te werken dan kleinere bedrijven (p<.001). In combinatie met het eerder beschreven gebruik van IoT kan het gebrek aan security by design een groot beveiligingsrisico vormen.

Tabel 8: Wordt er binnen uw bedrijf gewerkt volgens security by design? (N=444)

Antwoordoptie	Percentage
Ja	18,0%
Nee	54,5%
Weet ik niet	27,5%

3.2. Cybersecurity maatregelen

In dit hoofdstuk wordt gekeken naar de maatregelen die bedrijven nemen om digitale informatie te beveiligen en het bedrijf te beschermen tegen cyberaanvallen- of incidenten. Hierin wordt onderscheid gemaakt tussen technische maatregelen (zoals hard- en software) en beleids- en organisatiemaatregelen (zoals regels, protocollen en maatregelen gericht op het gedrag van personeel). Allereerst wordt gekeken naar de technische maatregelen die al dan niet door mkb'ers zijn genomen, vervolgens wordt apart gekeken naar de beleids- en organisatiemaatregelen.

3.2.1. Technische maatregelen

Technische maatregelen zijn onder te verdelen in preventieve maatregelen (om te voorkomen dat een incident zich voordoet), detectieve maatregelen (om een incident waar te kunnen nemen) en repressieve maatregelen (om de impact van een incident te verkleinen) (van Houten & Spruit, 2015). In deze paragraaf wordt per cluster aangegeven welke maatregelen genomen worden.

Preventieve maatregelen

Resultaten duiden op een basis set aan technische preventieve maatregelen, die door het overgrote merendeel van de bedrijven wordt genomen. Het gaat hierin enerzijds om het hebben van een virus/malwarescanner, firewall en een beveiligd draadloos netwerk. Anderzijds is het van belang dat deze maatregelen up-to-date en dus effectief worden gehouden. Een ruime meerderheid van de bedrijven (>85%) geeft aan al deze maatregelen te nemen. Het niet nemen van deze maatregelen betekent een zeer groot risico en één op de tien bedrijven is feitelijk dus niet beschermd tegen een incident. De meer geavanceerde preventieve maatregelen worden door minder bedrijven genomen.

Tabel 9: Technische preventieve maatregelen genomen door mkb'ers

	N	Ja	Nee	Weet ik niet
De computers van het bedrijf zijn voorzien van een virusscanner	783	97,3%	1,4%	1,3%
De virusscanners zijn up to date	781	94,0%	1,8%	4,2%
De computers / het netwerk van het bedrijf is voorzien van een firewall	778	90,9%	1,9%	7,2%
De firewall is up to date	776	85,7%	2,4%	11,9%
De software op het bedrijfsnetwerk wordt up-to-date gehouden	777	90,2%	2,7%	7,1%
Heeft uw bedrijf een website met een beveiligingscertificaat (https://)?	704	20,2%	79,8%	0%
Het draadloze netwerk is beveiligd	773	89,5%	3,2%	7,2%
Er wordt gebruik gemaakt van biomedische beveiligingsmethoden, zoals vingerafdruklezers	750	4,1%	89,6%	6,3%

Detectieve maatregelen

Naast de preventie van incidenten is het van belang een incident tijdig te detecteren zodat je kunt interveniëren. Hiervoor is het monitoren van het bedrijfsnetwerk noodzakelijk. Slechts 38% van de bedrijven registreert de activiteiten op het bedrijfsnetwerk. Micro bedrijven registreren minder vaak activiteiten op het bedrijfsnetwerk (29,8%) dan de bedrijven met meer medewerkers (p<.05).

Tabel 10: Internetactiviteiten op het bedrijfsnetwerk worden gemonitord / gelogd (N=769)

Antwoordoptie	Percentage
Ja	38,0%
Nee	33,0%
Weet ik niet	29,0%

Enkel registreren van datgene wat er gebeurd op het bedrijfsnetwerk is echter niet voldoende, deze informatie moet ook continue gemonitord worden om actie te kunnen ondernemen in het geval van een incident. Dit wordt door slechts een 19,1% van de bedrijven gedaan. Micro bedrijven nemen ook deze maatregel minder vaak (13,6%) (p<.05).

Tabel 11: De monitoring/logs worden regelmatig bekeken / geëvalueerd (N=760)

Antwoordoptie	Percentage
Ja	19,1%
Nee	54,6%
Weet ik niet	26,3%

Repressieve maatregelen

Op het moment dat een incident zich toch voordoet is het van belang dat vooraf repressieve maatregelen genomen zijn, zodat de schade na een incident zoveel mogelijk beperkt wordt. Zo is het van belang dat bedrijven noodzakelijke informatie ook buiten het netwerk opslaan (back-ups maken), zodat deze informatie nooit helemaal verloren gaat. De meeste respondenten (93,5%) geven aan een vorm van back-up te maken, om de toegang tot informatie te garanderen. Micro bedrijven maken vaker geen back-ups (91,0%) (p<.05). Driekwart van de bedrijven geeft aan deze back-ups buiten het pand op te slaan, zodat in het geval van bijvoorbeeld een brand of overstroming de informatie niet verloren gaat.

Naast repressieve maatregelen die de beschikbaarheid van informatie garanderen kan het van belang zijn maatregelen te nemen die de integriteit van informatie garanderen, oftewel zorgen dat belangrijke informatie niet inzichtelijk is voor derden die daar geen recht op hebben. Slechts een klein gedeelte van de bedrijven geeft aan vertrouwelijke informatie versleuteld op te slaan (19,8%) en te versturen (16,3%).

Tabel 12: Technische repressieve maatregelen

	N	Ja	Nee	Weet ik niet
Heeft uw bedrijf back-up voorzieningen?	792	93,5%	4,9%	1,7%
Back-ups worden ook buiten het bedrijfspand opgeslagen	776	76,7%	20,9%	2,4%
Bestanden met vertrouwelijke informatie worden versleuteld opgeslagen	776	19,8%	51,7%	28,5%
Bestanden met vertrouwelijke informatie worden versleuteld verstuurd	484	16,3%	56,8%	26,9%

3.2.2. Beleids- en organisatiemaatregelen

Naast technisch te implementeren maatregelen voor de cyber security van het bedrijf, is het noodzakelijk eveneens beleids- en organisatiemaatregelen te nemen. Maatregelen die bijvoorbeeld zijn gericht op het gedrag van personeel. Het nemen van dergelijke maatregelen is cruciaal; eerder onderzoek toont aan de het merendeel van de cyber incidenten binnen bedrijven te wijten zijn aan vergissingen van medewerkers.[15] Deze beleids- en organisatiemaatregelen zijn in dit hoofdstuk geclusterd op strategisch niveau, gericht op bewustwording en op operationeel niveau. Per cluster zullen de genomen maatregelen worden besproken.

Strategisch niveau

Voor de cyber security van een bedrijf is het van belang dat op strategisch en/of directie niveau nagedacht wordt over de digitale veiligheid van het bedrijf. Dergelijke maatregelen worden echter door een klein aantal bedrijven genomen. Om zich effectief te kunnen beveiligen zou een bedrijf een overzicht moeten hebben van de aanwezige IT (29,2%) en in kaart moeten brengen op welke manier het bedrijf slachtoffer zou kunnen worden van cybercriminaliteit (5,3%). Op basis hiervan kan beleid opgesteld worden om deze risico's te verkleinen (19,1%) en een protocol worden opgesteld die alle betrokkenen duidelijk maakt hoe te handelen in het geval van een incident (7,4%). Tussen haakjes staat telkens het percentage bedrijven weergegeven dat deze bedrijven heet genomen.

Micro bedrijven hebben minder vaak scenario's waarop slachtofferschap zich zou kunnen voordoen (2,1%) of protocollen opgesteld hoe zij zouden moeten handelen in het geval van slachtofferschap (1,8%) (p<.001). Micro bedrijven hanteren minder vaak een informatiebeveiligingsbeleid (10,2%) dan bedrijven met meer medewerkers (p<.001). Midden-klein bedrijven voeren vaker dit soort (veiligheids)audits uit (34,4%). Samenvattend is te concluderen dat het merendeel van de onderzochte bedrijven maatregelen op strategisch niveau niet neemt.

Tabel 13: Beleid- en organisatiemaatregelen op strategisch niveau

	N	Ja	Nee	Weet ik niet
Er is een schriftelijke weergave aanwezig van de huidige IT infrastructuur	774	29,2%	59,2%	11,6%
Er zijn scenario's ontwikkeld waarin is beschreven hoe het bedrijf slachtoffer kan worden van online criminaliteit	772	5,3%	87,7%	7,0%
Er is een protocol opgesteld waarin is beschreven hoe te handelen bij online criminaliteit	774	7,4%	87,2%	5,4%
Er is informatiebeveiligingsbeleid aanwezig	775	19,1%	74,2%	6,7%
Er worden regelmatig (veiligheids)audits uitgevoerd	799	15,9%	75,7%	8,4%

Bewustwording

Zoals eerder vermeld is een veiligheidsbreuk in veel gevallen het gevolg van menselijk handelen. Het is daarom van belangrijk dat medewerkers op de hoogte zijn van risico's en onveilige gedragingen, zodat zij deze kunnen voorkomen. De meerderheid van de bedrijven (59,6%) geeft aan dat medewerkers op de hoogte zijn gebracht van online risico's. Dit betekent dat dit voor een relatief grote groep nog niet het geval is. Deze groep wordt met name gevormd door micro bedrijven, werknemers binnen micro bedrijven worden minder vaak bewust gemaakt van online risico's (50,7%) en hebben minder vaak geleerd geen e-mail van potentieel onbetrouwbare afzenders te openen (78,3%) (p<.001).

Tabel 14: Beleid- en organisatiemaatregelen gericht op bewustwording

	N	Ja	Nee	Weet ik niet
Werknemers worden bewust gemaakt van online risico's	777	59,6%	36,9%	3,5%
Werknemers hebben geleerd om geen e-mail van potentieel onbetrouwbare afzenders te openen	780	82,4%	14,2%	3,3%
Werknemers hebben geleerd om goed op te letten bij het doen van online betalingen	775	69,9%	24,0%	6,1%
Werknemers hebben geleerd geen gevoelige informatie op internet te verstrekken	773	75,3%	20,1%	4,7%

Operationeel niveau

Het daadwerkelijk opstellen van regels voor veilig gedrag van medewerkers wordt door een beperkt aantal organisaties als maatregel genomen, variërend van 30% tot 75% over verschillende regels. Micro bedrijven hebben minder vaak regels opgesteld voor het gebruik van ICT voor privé doeleinden (13,4%), het doen van online betalingen (16,6%), het omgaan met vertrouwelijke informatie (27,1%), het openen van onbekende bestanden (25,5%) en het afgeven van bedrijfsgegevens (28,8%) (p=<.001). Ook het hebben van verschillende sterke wachtwoorden wordt in een minderheid van de bedrijven op operationeel niveau verplicht gesteld (30,5%).

15 IBM (2018). *IBM X-Force Threat Intelligence Index 2018: Notable security events of 2017, and a look ahead.* IBM security: New Orchard Rd New York.

Tabel 15: Beleid- en organisatiemaatregelen op operationeel niveau

	N	Ja	Nee	Weet ik niet
Werknemers moeten verschillende, sterke wachtwoorden voor online accounts gebruiken	774	65,0%	27,0%	8,0%
Het is verplicht om wachtwoorden met regelmaat te wijzigen	774	39,8%	57,1%	3,1%
Er zijn (schriftelijke) regels opgesteld over het gebruik van IT voor privé doeleinden	775	27,5%	69,4%	3,1%
Er zijn (schriftelijke) regels opgesteld voor het doen van online betalingen	774	23,5%	72,2%	4,3%
Er zijn (schriftelijke) regels opgesteld over het omgaan met vertrouwelijke informatie, zoals persoonsgegevens van u, uw medewerkers en klanten	774	37,0%	58,9%	4,1%
Er zijn (schriftelijke) regels opgesteld over het openen van onbekende bestanden (zoals bijlagen in e-mails)	775	30,6%	65,7%	3,7%
Er zijn (schriftelijke) regels opgesteld over het (op verzoek) afgeven van bedrijfsgegevens	775	32,9%	62,6%	4,5%

3.3. Risicoperceptie

Cyberrisicomanagement is, zoals in hoofdstuk 2 al beschreven, een belangrijk aspect in het vergroten van de informatiebeveiliging van een organisatie. De inschatting van risico's is voor cyberrisicomanagement van groot belang. Om de risicoperceptie van mkb directeuren in kaart te kunnen brengen is gekeken naar de waarschijnlijkheid dat slachtofferschap zich voor doet en de impact dat een incident zou hebben.

Met betrekking tot de impact van online criminaliteit is gevraagd in hoeverre het eigen bedrijf, in dit geval de bedrijfsprocessen, (volledig) afhankelijk is van IT. 63,1% van de respondenten geeft aan dat bedrijfsprocessen in (zeer) grote mate afhankelijk zijn van computers en internet. Deze afhankelijkheid geeft aan dat inbreuken op- of verstoringen van deze IT een *ernstige* impact zal hebben op de organisatie. Midden-klein bedrijven geven vaker aan het (51,6%) volledig eens te zijn met de stelling (p<.001).

Tabel 16: De bedrijfsprocessen in mijn bedrijf zijn volledig afhankelijk van computers en internet (IT) (N=792)

Antwoordoptie	Percentage
Volledig mee oneens	13,9%
Gedeeltelijk mee oneens	13,4%
Niet mee eens, niet mee oneens	9,6%
Gedeeltelijk mee eens	32,2%
Volledig mee eens	30,9%

Om de waarschijnlijkheid van het risico te beoordelen is gevraagd naar de kans dat het bedrijf van de respondent in de komende 12 maanden slachtoffer wordt van online criminaliteit. Respondenten schatten deze kans gemiddeld in op 20.9%.

Tabel 17: Hoe groot schat u de kans dat uw bedrijf in een periode van 12 maanden zelf slachtoffer wordt van online criminaliteit (pogingen niet meegerekend)? (N=781)

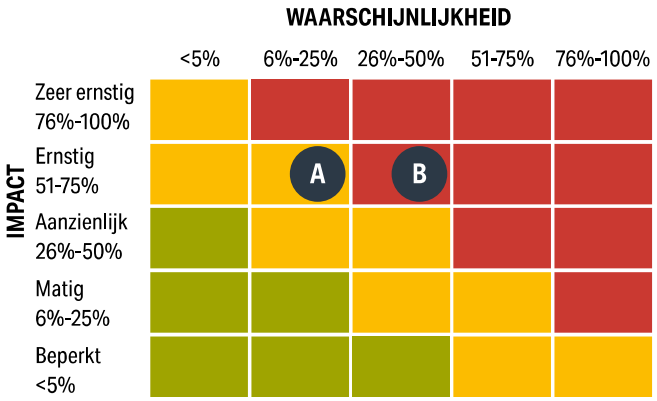
Antwoordoptie	Percentage
0 t/m 20%	71,8%
21 t/m 40%	12,0%
41 t/m 60%	11,9%
61 t/m 80%	2,3%
81 t/m 100%	1,9%

Daarnaast is gevraagd naar de perceptie van de kans dat een ander bedrijf, vergelijkbaar met het eigen, slachtoffer wordt. Opvallend is dat bedrijven het risico voor een ander bedrijf hoger inschatten dan het risico dat het eigen bedrijf loopt. De kans dat het eigen bedrijf slachtoffer wordt, wordt met gemiddeld 20,9% ingeschat. Het risico dat een ander bedrijf slachtoffer wordt, wordt een stuk hoger ingeschat, namelijk 42%.

Tabel 18: Hoe groot schat u de kans dat een mkb in Nederland in een periode van 12 maanden slachtoffer wordt van online criminaliteit (pogingen niet meegerekend)? (N=780)

Antwoordoptie	Percentage
0 t/m 20%	43,1%
21 t/m 40%	19,2%
41 t/m 60%	20,1%
61 t/m 80%	8,3%
81 t/m 100%	9,2%

Risicoperceptie kan worden weergegeven in een grafiek waar de kans en impact tegen elkaar afgezet worden. Op basis van deze combinatie wordt een risico als laag (groen), midden (oranje) of groot (rood ingeschat. Door de resultaten van mkb'ers uit dit onderzoek op een risicomatrix te plotten is de risicoperceptie van deze groep weergegeven, zoals gezegd via een inschatting van de waarschijnlijkheid en impact van online criminaliteit risico's voor het mkb (figuur 1). De inschatting voor het eigen bedrijf is hierin met aan A (midden) aangegeven, die van een vergelijkbaar ander bedrijf met een B. Gelet op de impact van het niet beschikbaar zijn van IT en de geschatte kans dat dit zich voordoet wordt cybercriminaliteit voor het eigen bedrijf als een middelgroot (A) risico gezien, voor een ander bedrijf wordt het risico als groot (B) ingeschat.



Figuur 1. Risicoperceptie midden-kleinbedrijven

De onderzochte bedrijven geven aan dat zij redelijk in staat zijn deze risico's te kunnen beoordelen. De meerderheid van de bedrijven (73,5%) geeft aan gedeeltelijk of volledig bewust te zijn van de online veiligheidsrisico's die het bedrijf loopt.

Tabel 19: Ik ben mij bewust van de online veiligheidsrisico's die mijn bedrijf loopt (N=789)

Antwoordoptie	Percentage
Volledig mee oneens	9,8%
Gedeeltelijk mee oneens	8,4%
Niet mee eens, niet mee oneens	8,4%
Gedeeltelijk mee eens	38,8%
Volledig mee eens	34,7%

Een kwart van de bedrijven geeft aan in meer of mindere mate vertrouwen te hebben in de genomen maatregelen. Een even grote groep geeft echter aan weinig vertrouwen te hebben in de genomen maatregelen. De gemiddelde score is dan ook 2,97 of een vijf-puntschaal. Midden-kleine bedrijven hebben meer vertrouwen (3,41) in de genomen maatregelen dan kleine en micro organisaties. Eerder is omschreven dat deze groep over het algemeen ook meer security maatregelen heeft genomen.

Tabel 20: Hoeveel vertrouwen heeft u in de door het bedrijf genomen maatregelen om online risico's (online criminaliteit) te voorkomen? (N=782)

Antwoordoptie	Percentage
Heel weinig / geen vertrouwen	4,1%
Weinig vertrouwen	25,1%
Niet veel en niet weinig vertrouwen	42,7%
Veel vertrouwen	25,8%
Heel veel vertrouwen	2,3%

3.4 Slachtofferschap

3.4.1. Prevalentie slachtofferschap online criminaliteit in het mkb

Eén op de vijf bedrijven onderzochte bedrijven (19,4%) geeft aan een cyber incident te hebben ervaren, waarvan zij schade hebben ondervonden, zijnde schade in de vorm van het verlies van geld, tijd of middelen. In slachtofferschap is onderscheid gemaakt tussen slachtofferschap van cybercrime en gedigitaliseerde criminaliteit. Onder de noemer cybercrime vallen ' nieuwe' delicten die gericht zijn op ICT. Bijvoorbeeld het hacken van een database. Onder gedigitaliseerde criminaliteit vallen 'traditionele' delicten waarbij ICT van belang is bij de uitvoering van dat delict. Een voorbeeld binnen deze categorie zijn fraude via internet.

De grootste groep slachtoffers geeft aan slachtoffer te zijn geworden van cybercrime (criminaliteit gericht op ICT) (17,9%), in het bijzonder malware (30,9%) en ransomware (17,2%). De kleinste groep geeft aan slachtoffer te zijn geworden van gedigitaliseerde criminaliteit (traditionele criminaliteit waarbij ICT gebruikt wordt om het delict uit te voeren) (8,8%). Deze groep bestaat met name uit slachtoffers van phishing (9,9%). Omdat diverse bedrijven zowel slachtoffer zijn geworden cybercrime als gedigitaliseerde criminaliteit, resulteert het totale groepspercentage op 19,4%.

3.4.2. Samenhang slachtofferschap met achtergrondkenmerken en risicovol gedrag

Om meer inzicht te creëren in het slachtofferschap is onderzocht welke factoren mogelijk samenhangen met slachtofferschap van online criminaliteit. Hiervoor is gekeken naar de correlatie van slachtofferschap met verschillende achtergrondkenmerken van bedrijven en wijze waarop met IT wordt omgegaan.

Achtergrondkenmerken

De grootte van het bedrijf, uitgedrukt in het aantal medewerkers, hangt samen met slachtofferschap van online criminaliteit. Dit geldt met name voor slachtofferschap van cybercrime. Micro bedrijven (<10 medewerkers) lijken minder vaak slachtoffer van online criminaliteit te worden dan kleine bedrijven en midden-klein bedrijven ($p<.001$).

Slachtofferschap kent een zelfde correlatie met de jaaromzet van de onderneming, waarbij ondernemingen met een omzet van meer dan 500.000 euro vaker slachtoffer zijn. Deze samenhang is echter niet langer significant wanneer wordt gecontroleerd voor het aantal medewerkers.

Ten slotte is er gekeken naar de sector waarin het bedrijf werkzaam is. Hierin is onderscheid gemaakt tussen productie, diensten en recreatie. Er is geen significante correlatie gevonden tussen sectoren en slachtofferschap, wat erop duidt dat de prevalentie van slachtofferschap van online criminaliteit niet afhankelijk is van de sector waarin bedrijven werkzaam zijn.

Omgang met ICT

Er is eveneens onderzocht of de wijze van omgang met ICT binnen de organisatie samenhangt met slachtofferschap. Er is specifiek gekeken naar BYOD, IoT, het toestaan dat derden contact kunnen maken met het bedrijfsnetwerk en het toepassen van autorisaties op het bedrijfsnetwerk. De resultaten wijzen erop dat het hebben van IoT apparatuur samenhangt met slachtofferschap van online criminaliteit. Bring Your Own Device (BYOD) hangt echter niet samen met slachtofferschap. Het toestaan dat derden, niet medewerkers, contact kunnen maken het bedrijfsnetwerk vertoont een positieve samenhang met slachtofferschap van online criminaliteit. Ten slotte is een correlatie gevonden tussen slachtofferschap en het niet werken met autorisaties op het bedrijfsnetwerk (waardoor alle medewerkers toegang hebben tot alle bedrijfsinformatie). Bedrijven die op deze manier met bedrijfsgegevens omgaan zijn vaker slachtoffer van online criminaliteit. Samenvattend kan gezegd worden dat de implementatie van IoT apparatuur, derden toestaan op het bedrijfsnetwerk en werken zonder autorisaties op het bedrijfsnetwerk risicovolle ICT gedragingen zijn, die samenhangen met slachtofferschap van cybercriminaliteit.

Tabel 21: Correlatie van slachtofferschap met risico- en achtergrondfactoren

Factor (A)	Slachtofferschap cybercriminaliteit		Slachtofferschap cybercrime		Slachtofferschap gedigitaliseerde criminaliteit	
	Pearson's r	sign	Pearson's r	sign	Pearson's r	sign
MKB < 10 medewerkers	-.15	**	-.16	**	-.03	
MKB > 49 medewerkers	.13	**	.15	**	.05	
Omzet > 500.000 euro	.13	**	.15	**	-.00	
Branche – productie	.02		.03		.02	
Branche – diensten	.01		.01		-.02	
Branche – recreatie	-.04		-.05		-.00	
IOT	.10	*	.11	*	.07	
Privé apparaten op netwerk	.00		-.02		.01	
Derden op netwerk – ja	.13	**	.12	**	.09	*
Derden op netwerk – ja, gastennetwerk	.08	*	.11	**	.04	
Derden op netwerk – ja, overig	.06		.03		.05	
Https website	.06		.06		.03	
Medewerkers toegang alle bedrijfsinformatie	.14	**	.15	**	.05	

(A) Elke factor kan gelezen worden als ja/nee
* p<0.05 ** p<0.01

3.5. Hulpbehoefte

Een van de doelstellingen van het lectoraat is mkb-bedrijven weerbaarder te maken tegen online risico's en daardoor de schade van online criminaliteit te verkleinen. Hiervoor is het van belang om een koppeling te maken tussen onderzoeksresultaten en praktisch toepasbare initiatieven voor het mkb. Essentieel hiervoor is de interesse van het mkb in zulk soortige hulp. Een overgrote meerderheid van de respondenten geeft aan geïnteresseerd te zijn in deze hulp.

Tabel 22: Bent u geïnteresseerd in handvatten om de veiligheid van uw IT- gekoppelde bedrijfsvoering te verbeteren? (N=389)

Antwoordoptie	Percentage
Nee	11,6%
Ja	88,4%

Bedrijven geven aan het meeste geholpen te zijn met informatie, enerzijds passief in de vorm van voorlichting of een (digitale) cursus, anderzijds actief in de vorm van een online of telefonische vraagbaak. Midden-kleine bedrijven geven nog vaker aan geholpen te zijn met voorlichting (77,4%) dan micro bedrijven (53,0%). Daarnaast bestaat er ook een grote wens naar, met name gratis, tooling en expert hulp in de vorm van een bedrijfsanalyse of een penetratietest. Micro bedrijven geven vaker aan geholpen te zullen zijn met gratis tools (55,2% versus 28,2%/27,5%), kleine en midden-kleine bedrijven verlangen vaker een penetratietest (46,4%/50% versus 25,6%), een bedrijfsanalyse (40,6%/47,7% versus 18,6%), een expertgesprek (20,3%/29,5% versus 7%).

Tabel 23: In welke vorm zou u de handvatten willen krijgen om uw bedrijfsvoering veiliger te krijgen? (N=350)

Antwoordoptie	Percentage
Gratis tools	42,0%
Betaalde tools	20,8%
Voorlichting	60,6%
Cursus op locatie	14,8%
Digitale cursus	22,8%
Inloop spreekuur	3,6%
Een balie	2,4%
Een online vraagbaak	30,0%
Een telefonische vraagbaak	17,1%
Een expertgesprek	16,3%
Een bedrijfsanalyse	32,7%
Een penetratietest	37,6%

Deelnemende mkb ondernemingen zijn het ook in grote mate eens over de partij van wie zij hulp, voor het weerbaarder maken van de eigen organisatie, zouden willen ontvangen. De meerderheid geeft aan hulp via de brancheverenigingte willen ontvangen. Daarnaast worden een landelijke website en betaalbare commerciële partijen als partijen gezien die hulp zou kunnen geven. Midden-kleine bedrijven geven vaker aan via concullega's (11,8%) (p<.05) of betaalbare commerciële partijen (33,3%) (p<.05) concrete handvaten te willen ontvangen.

Tabel 24: Via welke weg kan dit het beste aangeboden worden? (N=366)

Antwoordoptie	Percentage
Brancheverenigingte	85,0%
Landelijke website	22,0%
Concullega's	4,8%
Lokale helpdesk	8,9%
Betaalbare commerciële partijen	21,1%
Anders, namelijk	7,4%

Het merendeel van de bedrijven (89,1%) is bereid zelf extra te investeren om de cybersecurity te verbeteren, micro bedrijven willen vaker niets extra investeren (15,2%) dan kleine (7%) en midden-klein (2,8%) bedrijven.

Tabel 25: Bent u bereidt extra te investeren in de cybersecurity van uw bedrijf? (N=450)

Antwoordoptie	Percentage
Ja	89,1%
-Tijd	63,9%
-Geld	57,3%
-Middelen	57,3%
Nee	10,9%

Over het algemeen zijn midden-kleine bedrijven bereid meer tijd (83,6%), geld (87,7%) en middelen (79,5%) te besteden dan micro bedrijven (resp. 55,4%, 43,3%, 46,8%) (p<.001).

4. Conclusie

In dit hoofdstuk wordt teruggekeken op de resultaten van de nulmeting en antwoord gegeven op de in de inleiding geformuleerde deelvragen. Hiermee wordt invulling gegeven aan de doelstelling van de nulmeting: inzicht in de stand van zaken met betrekking tot cybersecurity en slachtofferschap van online criminaliteit in het Nederlandse mkb.

Deze studie zet een eerste stap door een beeld te schetsen van de cybersecurity in 799 Nederlandse midden-kleinbedrijven. De resultaten dienen echter voorzichtig te worden geïnterpreteerd vanwege de mogelijke selectiviteit van de steekproef, waardoor resultaten mogelijk zijn vertekend. Vervolgstudies zullen moeten uitwijzen in welke mate de resultaten in dit rapport van toepassing zijn op de bredere doelgroep.

Welke technische en organisatorische cybersecuritymaatregelen worden genomen om slachtofferschap te voorkomen?

Om een onderneming te kunnen beschermen tegen cybercriminelen kunnen technische en organisatorische maatregelen worden genomen. In de onderzochte bedrijven zijn beide vormen maatregelen genomen, de hoeveelheid bedrijven die een maatregelen neemt verschilt naar gelang je kijkt naar de soorten maatregelen.

Technische maatregelen

Een ruime meerderheid van de bedrijven (>85%) geeft aan basis technische *preventieve* maatregelen te nemen. Het niet nemen van deze maatregelen betekent een zeer groot risico, een kleine groep bedrijven (~10%) is hierdoor feitelijk niet beschermd tegen een incident of aanval.

Om te kunnen zien of het bedrijf onder aanval ligt van een cyber aanval zijn technische detectieve maatregelen noodzakelijk. Zoals het registreren van datgene er gebeurt op het bedrijfsnetwerk, uitgevoerd door een kleine minderheid(38%). Enkel registreren is echter niet voldoende, deze informatie moet ook regelmatig bekeken worden om actie te kunnen ondernemen en awareness te ontwikkelen. Dit wordt door slechts een 19,1% van de bedrijven gedaan.

Nadat een incident zich voordoet kunnen *repressieve* ertoe leiden dat de schade beperkt blijft. De meeste respondenten (93,1%) geven in dit kader aan een vorm van back-up te maken, om de toegang tot informatie te garanderen. Slechts een klein gedeelte van de bedrijven (<19%) geeft aan vertrouwelijke informatie te versleutelen.

Beleids- en organisatiemaatregelen

Op strategisch niveau kan een bedrijf kan zich wapenen tegen cyberaanvallen door bijvoorbeeld de ICT infrastructuur in kaart te brengen, risico's in kaart te brengen en scenario's te schetsen. Op basis hiervan zou op strategisch niveau beleid moeten worden vormgegeven. Samenvattend is te concluderen dat het merendeel van de onderzochte bedrijven deze maatregelen op strategisch niveau niet neemt.

Deelnemende bedrijven lijken zich met name toe te leggen op *bewustwording*. De meerderheid van de bedrijven (>59%) geeft aan dat medewerkers op de hoogte zijn gebracht van de verschillende risico's.

Voor effectieve maatregelen gericht op het menselijk handelen moeten bedrijven regels op het *operationeel* niveau opstellen. Op het hebben van verschillende sterke wachtwoorden na neemt een minderheid van de bedrijven maatregelen op operationeel niveau. Bedrijven die niet dit soort regels opstellen lopen mogelijk een risico doordat het personeel in lastige en/of onveilige situaties geen voorgeschreven veilig gedrag heeft waar het op terug kan vallen.

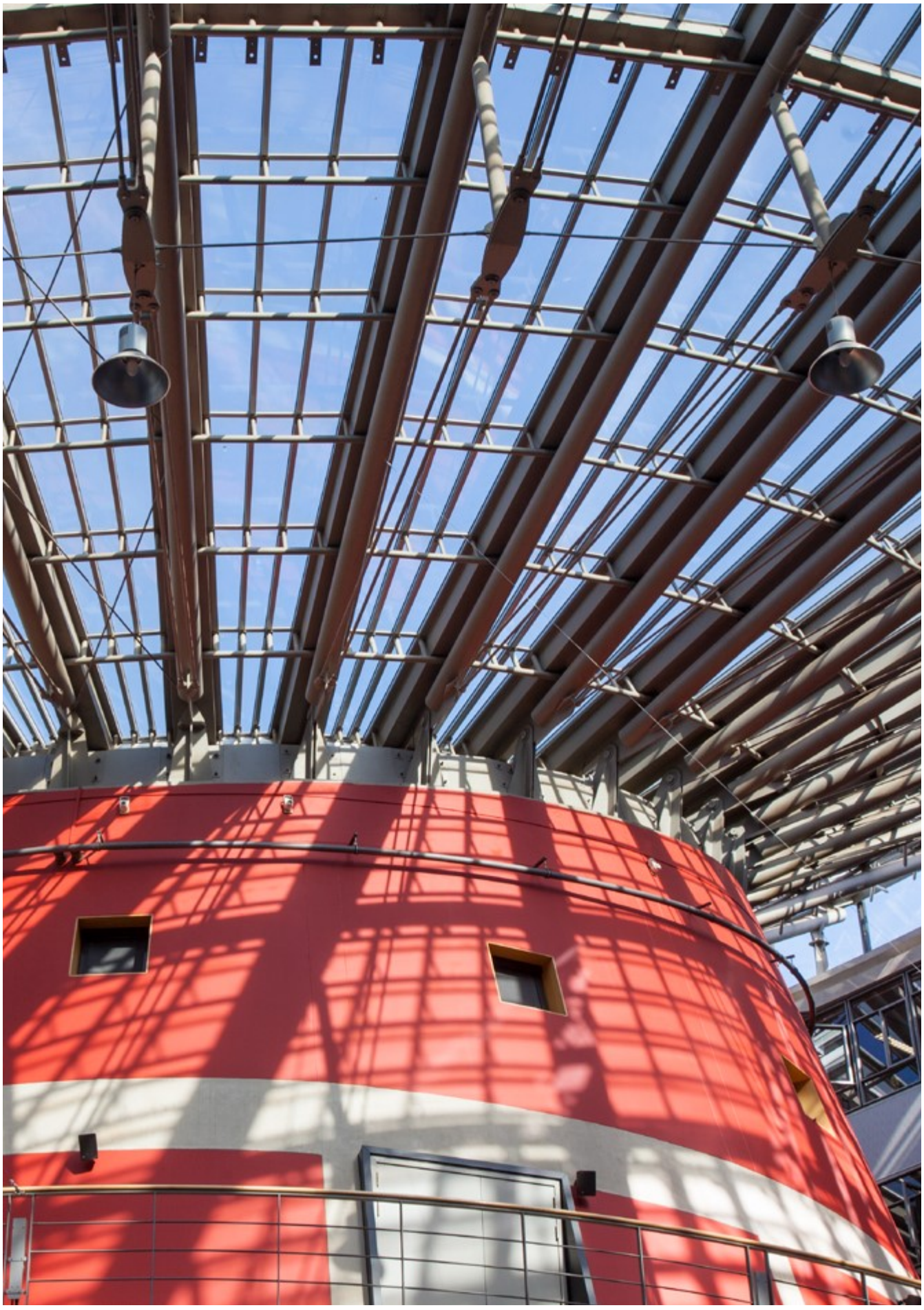
Wat is de prevalentie van slachtofferschap van online criminaliteit in het midden- kleinbedrijf?

Eén op de vijf bedrijven onderzochte bedrijven (19,4%) geeft aan een cyber incident te hebben ervaren, waarvan zij schade hebben ondervonden. In slachtofferschap is onderscheid gemaakt tussen slachtofferschap van cybercrime (17,9%) en gedigitaliseerde criminaliteit (8,8%).

Welke organisatiekenmerken of risicovol gedrag zijn van invloed op het slachtofferschap van midden- kleinbedrijven?

Het aantal medewerkers van een bedrijf hangt samen met slachtofferschap van online criminaliteit. Bedrijven met minder dan 10 medewerkers (15%) zijn minder vaak slachtoffer dan bedrijven met 10 à 50 (22%) of meer dan 50 (39%) medewerkers.

Sommige ICT gedragingen of apparatuur hangen eveneens samen met slachtofferschap en kunnen als risicovol worden benoemd. Het hebben van IoT apparatuur dat is verbonden aan het bedrijfsnetwerk correleert met slachtofferschap, ditzelfde geldt voor het toestaan dat alle medewerkers toegang hebben tot alle bedrijfsinformatie en ten slotte toestaan dat gasten via de Wi-Fi verbinding kunnen maken met het bedrijfsnetwerk.



Bijlage: vragenlijst

1) Hoeveel medewerkers telt uw bedrijf, inclusief de eigenaar(en) / directie?

(met medewerkers bedoelen we het aantal medewerkers, niet fte)
(numerieke waarde invullen)

2) Wat is de jaaromzet van uw bedrijf, in euro's?

- ○ 0 - 100.000 €
- ○ 100.000 - 500.000 €
- ○ 500.000 - 1.000.000 €
- ○ 1.000.000 - 2.500.000 €
- ○ 2.500.000 - 5.000.000 €
- ○ Meer dan 5.000.000 €
- ○ Zeg ik liever niet
- ○ Weet ik niet

3) Over hoeveel locaties/vestigingen is uw bedrijf verdeeld (inclusief productie- en administratievestigingen)?

(numerieke waarde invullen)

4) Waar is uw bedrijf actief?

- ○ Lokaal
- ○ Regionaal
- ○ Nationaal
- ○ Internationaal
- ○ Weet ik niet

5) Begeeft uw bedrijf zich op de consumenten- en/of bedrijvenmarkt?

- ○ Consumentenmarkt
- ○ Bedrijvenmarkt (zowel profit en non-profit)
- ○ Consumenten- en bedrijvenmarkt

6) Wat is uw functie binnen het bedrijf waarvoor u werkt?

- ○ Directeur (bestuurder)
- ○ Eindverantwoordelijke IT
- ○ Anders, namelijk..

7) Bent u uitvoerend belast met en/of bent u verantwoordelijk voor de veiligheid van IT binnen het bedrijf?

- ○ Wel verantwoordelijk voor de veiligheid van de IT, niet uitvoerend belast
- ○ Verantwoordelijk voor de veiligheid van de IT en uitvoerend belast
- ○ Niet verantwoordelijk voor de veiligheid van de IT, wel uitvoerend belast
- ○ Niet verantwoordelijk voor de veiligheid van de IT en ook niet uitvoerend belast
- ○ Ik ben niet op de hoogte wie verantwoordelijk is voor de veiligheid van de IT
- ○ Onze IT is volledig uitbesteed

8) Heeft uw bedrijf een functionaris voor informatiebeveiliging? (Met informatiebeveiliging worden maatregelen bedoeld die gericht zijn op beschikbaarheid, integriteit en exclusiviteit van informatie)

- ○ Ja, een interne medewerker
- ○ Ja, een extern ingehuurde medewerker/ organisatie
- ○ Nee, wij hebben geen functionaris (intern dan wel ingehuurd) voor informatiebeveiliging
- ○ Ik weet niet of wij een functionaris hebben of inhuren voor de informatiebeveiliging

9) In hoeverre beschouwt u cybercrime (in al zijn verschijningsvormen) als een probleem voor uw bedrijf?

- ○ Zeer groot problem
- ○ Groot problem
- ○ Geen groot problem / geen klein probleem
- ○ Klein problem
- ○ Geen probleem
- ○ Hier heb ik geen zicht op

10) Hoeveel van de onderstaande apparaten zijn (ongeveer) in het bezit van uw bedrijf?

- ○ Desktop (vaste computer)
- ○ Laptop
- ○ Tablet
- ○ Smartphone

11) Zijn deze apparaten met het internet verbonden?

	Ja, deze is/ zijn allemaal aan het internet verbonden	Sommigen zijn aan het internet verbonden, niet allemaal	Nee, deze is/ zijn niet aan het internet verbonden
Desktop (vaste computer)	○	○	○
Laptop	○	○	○
Tablet	○	○	○
Smartphone	○	○	○

12) Zijn er binnen uw bedrijf nog andere apparaten aanwezig die verbonden zijn met het internet?

- ○ Ja, apparaten voor het primair productieproces
- ○ Ja, apparaten voor gebouw beheer systemen (zoals bijvoorbeeld camera's, hek- en sluitwerk)
- ○ Ja apparaten voor industriële controlesystemen of procesbeheersing. (zoals bijvoorbeeld het bestuur en bewaking van productieprocessen)
- ○ Nee, dit ben ik op dit moment aan het ontwikkelen
- ○ Nee, dit ben ik op de lange termijn van plan
- ○ Nee, dit ben ik niet van plan
- ○ Anders, namelijk: ...
- ○ Weet niet

13) Welke van deze apparaten zijn te besturen vanaf het internet?

- ○ De apparaten voor het primair productieproces
- ○ De apparaten voor gebouw beheer systemen (zoals bijvoorbeeld camera's, hek- en sluitwerk)
- ○ De apparaten voor industriële controlesystemen of procesbeheersing. (zoals bijvoorbeeld het bestuur en bewaking van productieprocessen)
- ○ Geen
- ○ Weet niet

14) Stelling: Ik ben mij bewust van de online kwetsbaarheid van deze aan het internet verbonden apparaten.

- ○ Volledig mee oneens
- ○ Gedeeltelijk mee oneens
- ○ Niet mee eens, niet mee oneens
- ○ Gedeeltelijk mee eens
- ○ Volledig mee eens

15) Wordt er binnen uw bedrijf gewerkt volgens security by design?

- ○ Ja
- ○ Nee, dat zijn wij wel van plan
- ○ Nee
- ○ Weet niet

16) Maakt men binnen het bedrijf gebruik van privé apparaten (inclusief desktop, laptop, tablet en/of telefoon) (bring your own device)?

- ○ Ja, deze kunnen gekoppeld worden aan het bedrijfsnetwerk (wifi of anders)
- ○ Ja, maar deze kunnen niet aan het bedrijfsnetwerk gekoppeld worden
- ○ Nee

17) Worden privé apparaten in uw bedrijf zakelijk gebruikt?

- ○ Ja
- ○ Nee
- ○ Weet ik niet

18) Worden zakelijke apparaten in uw bedrijf privé gebruikt? (enkelvoudige selectie)

- ○ Ja
- ○ Nee
- ○ Weet ik niet

19) Van welk platform / besturingssysteem wordt er binnen uw bedrijf gebruik gemaakt op serverniveau?

- ○ OS X (Apple)
- ○ Linux
- ○ Windows Server 2012R2
- ○ Windows 2012
- ○ Windows Server Essentials
- ○ Windows Essentials Business Server
- ○ Windows 10
- ○ Windows 8
- ○ Windows 7
- ○ Windows Vista
- ○ Windows XP
- ○ Wij gebruiken een cloudoplossing
- ○ Anders, namelijk ...
- ○ Weet ik niet

20) Hoe wordt de server van uw bedrijf beheerd?

- ○ Dat doe ik zelf
- ○ Door een interne IT-specialist / afdeling
- ○ Door een externe IT-specialist
- ○ Anders namelijk: …

(meerdere mogelijkheden kunnen worden aangekruist)

21) Op welke wijze zijn de IT-systemen binnen uw bedrijf verbonden met het Internet?

- ○ Via een eigen ADSL/kabel/glas verbinding
- ○ Via een (W)LAN verbinding (wifi en/of bekabeld)
- ○ Via het mobiele netwerk (4G, UMTS,…)
- ○ Weet ik niet

(meerdere mogelijkheden kunnen worden aangekruist)

22) Welke netwerkvoorzieningen komen voor in het bedrijfsnetwerk van uw bedrijf?

- ○ Wi-Fi access point
- ○ Firewall
- ○ ADSL-access point
- ○ VPN (virtual private netwerk)
- ○ Geen van allen
- ○ Anders, namelijk: …
- ○ Weet ik niet

(meerdere mogelijkheden kunnen worden aangekruist)

23) Kunnen derden (zoals gasten) via het netwerk van uw bedrijf het internet benaderen?

- ○ Ja, via WiFi access geen wachtwoord nodig
- ○ Ja, via WiFi access met een vast wachtwoord dat voor ieder-een gelijk is
- ○ Ja, via WiFi access met een wisselend wachtwoord dat voor iedereen gelijk is en blijft.
- ○ Ja, via WiFi access met een persoonlijke inlog naam en code
- ○ Ja, er is hiervoor een speciaal gasten netwerk
- ○ Nee
- ○ Ja, anders namelijk: …

Weet ik niet(meerdere mogelijkheden kunnen worden aangekruist)

24) Welke van de volgende voorzieningen komen voor in de IT-infrastructuur van uw bedrijf?

- ○ UPS (noodstroomvoorziening)
- ○ Dubbele verbinding naar het internet (als de ene verbinding uitvalt, neem een andere verbinding het over / redundantie)
- ○ Serverruimte
- ○ Toegangsbeveiliging serverruimte (bijv. slot, inbraakalarm, …)
- ○ Brand-preventie / detectie in de serverruimte
- ○ Koeling in de serverruimte
- ○ Geen van bovenstaande voorzieningen
- ○ Anders, namelijk: …

(meerdere mogelijkheden kunnen worden aangekruist)

25) Welke back-up voorzieningen worden in uw bedrijf gebruikt?

- ○ We kopiëren belangrijke data naar meerdere systemen
- ○ Externe mobiele storage (externe harde schijf, USB-stick, DVD,…)
- ○ Windows Backup&Restore
- ○ MAC Time Machine Backup
- ○ Cloud storage (Google drive, Dropbox,…)
- ○ Gespecialiseerde back-up via externe partij
- ○ Aparte interne server
- ○ Aparte externe server
- ○ Niet van toepassing (wij maken geen back-ups)
- ○ Anders namelijk: …

Weet ik niet(meerdere mogelijkheden kunnen worden aangekruist)

26) Welke computervoorzieningen heeft uw bedrijf buiten de bedrijfsmuren?

- ○ Mijn website wordt extern gehost
- ○ Ik gebruik cloud /internet applicaties namelijk: ….
- ○ Ik heb een of meerdere dedicated servers in een datacenter
- ○ Niet van toepassing
- ○ Weet ik niet
- ○ (meerdere mogelijkheden kunnen worden aangekruist)

27) Als uw bedrijf een website heeft, wat past dan bij de situatie van uw bedrijf?

- ○ Website draait binnen de bedrijfsmuren
- ○ Gehost bij een externe partij
- ○ In eigen beheer
- ○ In eigen beheer door interne IT-specialist(en)
- ○ Beheerd door een externe partij
- ○ Eenvoudige website met statische content
- ○ Complexe website met zeer veranderlijke content
- ○ HTTPS (dus met beveiligingscertificaat; uw website begint met https://www)
- ○ Inlogaccounts voor klanten
- ○ Inlogaccounts voor meerdere medewerkers
- ○ Webshop
- ○ Niet van toepassing (mijn bedrijf heeft geen website)
- ○ Weet ik niet

28) Maken medewerkers binnen uw bedrijf gebruik van social media?

- ○ Ja, uitsluitend voor bedrijfsdoeleinden
- ○ Ja, uitsluitend voor privédoeleinden
- ○ Ja, zowel voor bedrijfs- als privédoeleinden
- ○ Nee
- ○ Weet ik niet

29) Hebben de medewerkers binnen uw bedrijf toegang tot de digitale bedrijfsinformatie?

- ○ Ja, alle medewerkers hebben toegang tot alle digitale informatie
- ○ Gedeeltelijk, medewerkers hebben alleen toegang tot die digitale informatie die zij nodig hebben voor het uitvoeren van hun werkzaamheden
- ○ Nee, de medewerkers hebben geen toegang tot de digitale informatie van het bedrijf
- ○ Weet ik niet

(meerdere mogelijkheden kunnen worden aangekruist)

30) Zijn er partijen die niet in dienst zijn bij uw bedrijf, maar die wel toegang hebben tot de digitale bedrijfsinformatie van uw bedrijf (zoals bv. ketensamenwerkingen / ICT service providers / IT dienstverleners of administratie kantoren)?

- ○ Ja, adviseurs /consultants
- ○ Ja, extra tijdelijk ingehuurd personeel / uitzendkrachten
- ○ Nee, er zijn geen mensen of partijen die niet bij mijn bedrijf werken en die wel toegang tot de digitale (gevoelige) bedrijfs-informatie van het bedrijf hebben
- ○ Ja, anders namelijk …
- ○ Weet ik niet

31) Wordt de toegang tot de digitale bedrijfsinformatie geblokkeerd nadat de gebruiker deze niet meer nodig heeft (Bijvoorbeeld na uitdiensttreding, functieverandering of afronding van de opdracht/ dienstuitvoering door een derde)?

- ○ Ja, direct
- ○ Ja, binnen een vooraf vastgestelde periode
- ○ Nee
- ○ Anders, namelijk..
- ○ Weet ik niet

32) Welke bronnen van inkomsten of waardevolle bezittingen van uw bedrijf moeten volgens u zeker beschermd zijn (de kroonjuwelen)?

Hierbij is te denken aan persoonsgegevens van personeel en/of gasten, creditcardgegegevens, offertes, ideeën voor nieuwepro-ducten of diensten, projecten, de veiligheidsmaatregelen die het bedrijf heeft ingesteld.

- ○ Personeelsadministratie
- ○ Klantgegevens / persoonsgegevens / polisgegevens
- ○ CRM
- ○ Financiële administratie / boekhouding (van de eigen onderneming)
- ○ Bedrijfsinformatie ten behoeve van het primaire proces
- ○ Kassasysteem
- ○ Voorraadbeheer
- ○ Projectgegevens
- ○ Webshop
- ○ Vermogensbeheer
- ○ Geen
- ○ Anders, namelijk: …
- ○ Weet ik niet

33) Stelling: De bedrijfsprocessen in mijn bedrijf zijn volledig afhankelijk van computers en internet (IT).

- ○ Volledig mee oneens
- ○ Gedeeltelijk mee oneens
- ○ Niet mee eens, niet mee oneens
- ○ Gedeeltelijk mee eens
- ○ Volledig mee eens

34) Stelling: Ik ben mij bewust van de online veiligheidsrisico's (cybercrime) die mijn bedrijf loopt.

- ○ Volledig mee oneens
- ○ Gedeeltelijk mee oneens
- ○ Niet mee eens, niet mee oneens
- ○ Gedeeltelijk mee eens
- ○ Volledig mee eens

35) In welke mate staat op het bedrijfsnetwerk (of op de computers) van uw bedrijf informatie opgeslagen, zoals gast-, administratiegegevens en/of informatie over productontwikkeling?

- ◯ In zeer grote mate
- ◯ In grote mate
- ◯ Niet in grote, maar ook niet in kleine mate
- ◯ In kleine mate
- ◯ In zeer kleine mate
- ◯ Niet

(meerdere mogelijkheden kunnen worden aangekruist)

36) Stel, er wordt ingebroken in de systemen van uw bedrijf, wat zou de schade kunnen zijn?

- ◯ Er wordt geld gestolen
- ◯ Er worden gastgegevens gestolen
- ◯ Er worden bedrijfsgegevens gestolen
- ◯ Bedrijfsprocessen liggen stil
- ◯ Er kan imagoschade optreden
- ◯ Er kunnen juridische en/of contractuele problemen ontstaan
- ◯ Anders, namelijk...

37) Hoe groot schat u de kans dat een MKB-bedrijf in Nederland in een periode van 12 maanden slachtoffer wordt van een cybercrime (pogingen niet meegerekend)?

….% (numerieke waarde van 1 tot en met 100 laten invullen)

38) Hoe groot schat u de kans dat uw bedrijf in een periode van 12 maanden zelf slachtoffer wordt van een cybercrime (pogingen niet meegerekend)?

….% (numerieke waarde van 1 tot en met 100 laten invullen)

39) Hoe groot schat u het percentage van het totale IT budget in dat uw bedrijf aan cyber security besteedt?

….% (numerieke waarde van 1 tot en met 100 laten invullen)

40) Wat bent u bereidt extra te investeren in de cyber security van uw bedrijf?

- ◯ Tijd
- ◯ Geld
- ◯ Middelen
- ◯ Niets
- ◯ Anders, namelijk: ...

41) Welke technische maatregelen heeft uw bedrijf genomen om online risico's (zoveel mogelijk) uit te sluiten?

	Ja	Nee	Weet ik niet
De computers van het bedrijf zijn voorzien van een virusscanner	○	○	○
De virusscanner(s) is (/zijn) up-to-date	○	○	○
De computers / het netwerk van het bedrijf zijn/is voorzien van een firewall	○	○	○
De firewall(s) is(/zijn) up-to-date	○	○	○
Het (draadloze) netwerk is beveiligd	○	○	○
De software op het bedrijfsnetwerk wordt up-to-date gehouden	○	○	○
(Internet)activiteiten op het bedrijfsnetwerk worden geregistreerd (gelogd)	○	○	○
De logs worden (regelmatig) bekeken/geëvalueerd	○	○	○
Er worden regelmatig back-ups gemaakt van bestanden op computers en/of het bedrijfsnetwerk	○	○	○
Back-ups worden (ook) buiten het bedrijfspand opgeslagen	○	○	○
Bestanden met vertrouwelijke informatie worden versleuteld opgeslagen (bijvoorbeeld middels encryptie)	○	○	○
Bestanden met vertrouwelijke informatie worden versleuteld verstuurd (bijvoorbeeld middels encryptie)	○	○	○
Er wordt gebruik gemaakt van biometrische beveiligingsmethoden, zoals vingerafdruklezers	○	○	○

42) Welke beleidsmaatregelen heeft uw bedrijf genomen om online risico's (zoveel mogelijk) uit te sluiten?

	Ja	Nee	Weet ik niet
Er is een schriftelijke weergave aanwezig van de huidige ICT infrastructuur (netwerk/computersystemen)	○	○	○
Er zijn scenario's ontwikkeld waarin is beschreven hoe het bedrijf slachtoffer kan worden van cybercrime (een ex-medewerker die bijvoorbeeld inlogt op het bedrijfsnetwerk en vertrouwelijke informatie steelt)	○	○	○
Er is een protocol opgesteld waarin is beschreven hoe te handelen bij cybercrime	○	○	○
Er is informatiebeveiligingsbeleid aanwezig	○	○	○
Werknemers worden bewust gemaakt van online risico's	○	○	○
Werknemers hebben geleerd om geen e-mail van potentieel onbetrouwbare afzenders te openen	○	○	○
Werknemers hebben geleerd om goed op te letten bij het doen van onlinebetalingen (bijvoorbeeld op de 's' achter http of op het slotje in de webbrowser)	○	○	○
Werknemers hebben geleerd om geen gevoelige informatie op internet te verstrekken	○	○	○
Werknemers moeten verschillende, sterke wachtwoorden voor online accounts gebruiken (combinatie van minstens 8 cijfers en letters)	○	○	○
Er worden regelmatig (veiligheids)audits uitgevoerd	○	○	○
Er zijn (schriftelijk) regels opgesteld over het gebruik van ICT voor privé-doeleinden	○	○	○
Er zijn (schriftelijk) regels opgesteld voor het doen van online betalingen	○	○	○
Er zijn (schriftelijk) regels opgesteld over het omgaan met vertrouwelijke informatie, zoals persoonsgegevens van u, uw medewerkers en/of gasten	○	○	○
Er zijn (schriftelijk) regels opgesteld over het openen van onbekende bestanden (zoals bijlagen in e-mails)	○	○	○
Er zijn (schriftelijk) regels op gesteld over het (op verzoek) afgeven van bedrijfsgegevens	○	○	○
Het is verplicht om wachtwoorden met regelmaat te wijzigen	○	○	○

43) Hoeveel vertrouwen heeft u in de door het bedrijf genomen maatregelen om online risico's (cybercrime) te voorkomen?

- ○ Heel weinig/geen vertrouwen
- ○ Weinig vertrouwen
- ○ Niet veel en niet weinig vertrouwen
- ○ Veel vertrouwen
- ○ Heel veel vertrouwen

44) In hoeverre heeft uw bedrijf te maken gehad met de volgende incidenten?

	Weet niet	Niet mee te maken gehad	Een of meerdere mislukte pogingen (dus geen slachtoffer)	Eén keer slachtoffer	Meerdere keren slachtoffer
Afpersing via internet (het moeten afgeven van geld of goederen door bedreiging en/of geweld)	○	○	○	○	○
Chantage via internet (het moeten afgeven van geld of goederen door dreiging met smaad, smaadschrift of openbaarmaking van een geheim)	○	○	○	○	○
Denial of Service (DoS-) aanval (digitale aanvallen op het systeem waardoor dit wordt overbelast en niet meer beschikbaar is, bijvoorbeeld het platleggen van de website)	○	○	○	○	○
Defacing (het zonder toestemming veranderen/bekladden, vervangen of vernielen van de website van uw bedrijf)	○	○	○	○	○
Diefstal van datadragers (zoals pc, laptop, usb-sticks)	○	○	○	○	○
Diefstal van gegevens (Opzettelijk afgetapte of opgenomen gegevens die niet voor de dader bestemd zijn)	○	○	○	○	○
Fraude/oplichting via internet (financiële schade oplopen middels bedrog)	○	○	○	○	○
Hacking (inbraak op de computersystemen van uw bedrijf)	○	○	○	○	○
Identiteitsmisbruik via internet (het misbruik maken van de identiteitsgegevens van uw bedrijf)	○	○	○	○	○
Malware (infectie van computersystemen middels virussen, trojan horses, spyware en/of wormen)	○	○	○	○	○
Ongeautoriseerd gebruik van het bedrijfsnetwerk (bijvoorbeeld voor het downloaden/verspreiden van illegale software, kinderpornografie, SPAM of het plaatsen van berichten van racistische of discriminerende aard)	○	○	○	○	○
Phishing (het via digitale middelen – zoals e-mail – met een verzinsel informatie over uw bedrijf ontfutselen via mensen binnen uw bedrijf)	○	○	○	○	○
Ransomware (een programma dat een computer (of gegevens die erop staan) blokkeert en vervolgens van de gebruiker geld vraagt om de computer weer te "bevrijden'	○	○	○	○	○
Skimming waarbij op onrechtmatige wijze pinpas- of creditcardgegevens van uw bedrijf zijn bemachtigd en gekopieerd	○	○	○	○	○
Skimming waarbij daders het pin-apparaat van uw bedrijf hebben aangepast	○	○	○	○	○
Smaad/laster via internet (het via ICT opzettelijk aantasten van de goede naam van uw bedrijf)	○	○	○	○	○
Spionage via internet (het via digitale middelen verkrijgen van vertrouwelijke bedrijfsinformatie van economische of politieke waarde)	○	○	○	○	○
Vernieling van gegevens via internet (gegevens die opzettelijk veranderd, gewist, onbruikbaar of ontoegankelijk gemaakt worden)	○	○	○	○	○

45) Is uw bedrijf wel eens slachtoffer geworden van een cybercrime?

- ○ Ja, in de afgelopen twaalf maanden
- ○ Ja, meer dan een jaar geleden
- ○ Er is wel een poging tot een cybercrime gedaan, maar het bedrijf is hier geen slachtoffer van geworden
- ○ Nee, het bedrijf is hier geen slachtoffer van geworden en er is ook geen poging tot een cybercrime gedaan
- ○ Weet niet

46) Hoe vaak is uw bedrijf in de afgelopen jaar slachtoffer geworden van cybercriminaliteit voor zover voor u bekend is?

47) Welke schade heeft uw bedrijf in het afgelopen jaar ondervonden van deze cybercrime?

- ○ Geen schade
- ○ Financiële schade
- ○ Verlies en/of beschadiging van gegevens
- ○ Schade in de vorm van tijdverlies
- ○ Imago/reputatieschade
- ○ Vertrek van gasten
- ○ Anders, namelijk…

48) Hoe groot is de financiële schade door cybercriminaliteit bij uw bedrijf in de afgelopen twee jaar ongeveer? Graag afronden op hele bedragen.

- ○ Zeg ik liever niet (maar er was wel sprake van schade)
- ○ Weet ik niet
- ○ … euro

49) Beschrijf hieronder hoe de cybercrime(s) (vermoedelijk) is(zijn) gepleegd bij uw bedrijf?

50) Bent u geïnteresseerd in concrete handvatten om de veiligheid uw ICT-gekoppelde bedrijfsvoering te verbeteren?

- ○ Ja
- ○ Nee

51) In welke vorm zou u de handvatten willen krijgen om uw bedrijfsvoering veiliger te krijgen?

- ○ Gratis tools (zoals virusscanners)
- ○ Betaalde tools (zoals virusscanners)
- ○ Voorlichting
- ○ Life cursus
- ○ Digitale cursus
- ○ Een inloop-spreekuur
- ○ Een balie
- ○ Een online vraagbaak
- ○ Een telefonische vraagbaak
- ○ Een expertgesprek
- ○ Een bedrijfsanalyse
- ○ Een penetratietest (toets van computersystemen op kwetsbaarheden)
- ○ Anders, namelijk …

52) Zo ja, via welke weg kan dit het best aangeboden worden? (meerkeuze vraag)

- ○ Branche vereniging
- ○ Landelijke website
- ○ Concullega's
- ○ Een lokale helpdesk
- ○ Betaalbare commerciële partijen
- ○ Anders, namelijk…

De Haagse Hogeschool
Johanna Westerdijkplein 75
2521 EH Den Haag
www.dehaagsehogeschool.nl

Auteurs:
R.J. (Raoul) Notté, MA MSc
L.K. (Lisanne) Slot, MSc
Dr. M.S. (Susanne) van 't Hoff-de Goede
Dr. E.R. (Rutger) Leukfeldt

Uitgever: Centre of Expertise Cybersecurity, De Haagse Hogeschool
Foto's omslag en binnenwerk: Shutterstock en De Haagse Hogeschool
Vormgeving: Dienst Onderwijs, Kennis & Communicatie

Adres- en contactgegevens

Johanna Westerdijkplein 75
2521 EN Den Haag

dehaagsehogeschool.nl