# Van vertrouwen geven naar eigen verantwoordelijkheid nemen

## De 3 belangrijkste cybersecuritytrends voor ondernemers

Jouw wereld. Ons domein.

# Inhoud

# 1 Inleiding

In april 2020 deed marktonderzoeksbureau GfK onderzoek onder mkb'ers. Hierbij werden zo'n 50 vragen beantwoord door 577 respondenten (ondernemers) die meer dan 10 fulltime medewerkers in dienst hebben. Dit onderzoek gaat onder andere in op: Zijn ondernemers zich bewust van de cybersecurityrisico's en welke maatregelen nemen zij? Maken zij zich zorgen om hun bedrijf?

Na het lezen van dit rapport ken je de belangrijkste conclusies van het marktonderzoek. Zo gaan we onder andere in op het feit dat het aantal ondernemers dat te maken had met cybercrime toenam ten op zichte van ons onderzoek 'Trends in Online Security & e-Identity' uitgevoerd in 2018. Ook verdiepen we ons in de rol van de IT-leverancier. Want verwacht het mkb misschien te veel van z'n IT-partners?

Er lijkt een vreemde situatie te ontstaan, waarbij we zien dat er een stijgend aantal slachtoffers is, terwijl men zich geen zorgen maakt over het gevaar en de impact van cybercrime. Hoe serieus neem jij jouw cyberweerbaarheid? Heb je inzicht in de digitale kwetsbaarheden van je bedrijf of vertrouw je blindelings op een ander? Neem de cyberweerbaarheid van je bedrijf serieus en maak er werk van!

# 2 Managementsamenvatting

Onlangs deed GfK in opdracht van SIDN onderzoek naar de security-awareness bij het midden- en kleinbedrijf (mkb). In dit rapport delen we de belangrijkste conclusies.

**Conclusie #1: Het aantal mkb'ers dat slachtoffer werd van cybercrime steeg van 19 naar 22%.**
Het blijft een hardnekkig misverstand dat vooral grote ondernemingen doelwit zijn van cybercrime. Want juist het mkb vormt een makkelijk én interessant doelwit. Deze bedrijven hebben namelijk vaak onvoldoende middelen, kennis en/of toegang tot kennis om dreigingen te onderkennen en zich weerbaar te maken. Mede hierdoor steeg het aantal slachtoffers van cybercriminaliteit met 3%.

Onder de vormen van cybercrime die als het meest bedreigend worden ervaren, steekt ransomware er met kop en schouders bovenuit. Betalen van het geëiste losgeld blijkt geen garantie voor het terugkrijgen van jouw gegevens. En een lek zit vaak bij medewerkers, die in een derde van de gevallen, veelal onbewust, 'aanleiding' zijn voor een aanval. Dit komt voornamelijk door de verspreiding van phishing-mails.

**Conclusie #2: Cybercriminaliteit wordt voor ondernemers steeds meer een zorgenkindje.**
Het blijkt dat cybercriminaliteit steeds hoger scoort als bron van zorgen. Zo is er sprake van een lichte stijging onder mkb'ers; op dit moment ervaart 22% cybercrime als 'vrij bedreigend'. De meest genomen cybersecuritymaatregelen zijn: een antivirusprogramma, een sterk spamfilter voor e-mail en het regelmatig updaten of vervangen van apparaten.

Bij het organiseren van cybersecurity lopen bedrijven vooral op tegen de snelle ontwikkelingen die ze nauwelijks kunnen bijhouden. Ook is er sprake van een gebrek aan budget.

**Conclusie #3: Mkb'ers vertrouwen massaal op hun IT-leverancier als het om cybersecurity gaat.**
Het vertrouwen in IT-leveranciers is groot als het om cybersecurity gaat; 79% van de mkb'ers vertrouwt erop dat zijn of haar IT-leverancier de zaken op orde heeft wat betreft cybersecurity. IT-leveranciers geven op hun beurt aan dat 58% van hun mkb-klanten onvoldoende beschermd is.
Veel mkb'ers gaan ervan uit dat de IT-beheerder een bepaalde zorgplicht heeft en hen in zekere zin beschermt tegen cyberrisico's. In slechts 22% van de gevallen is hier daadwerkelijk ook een afspraak over gemaakt. Daarnaast zijn IT'ers niet per definitie cybercrime-experts; veiligheid vergt een andere expertise dan performance en beschikbaarheid.

# 3 Conclusie #1 Het aantal mkb'ers dat slachtoffer werd van cybercrime steeg van 19 naar 22%

Het blijft een hardnekkig misverstand dat vooral grote ondernemingen het doelwit zijn van cybercrime. Want juist het mkb vormt een makkelijk én interessant doelwit. Deze bedrijven hebben namelijk vaak onvoldoende middelen, kennis en/of toegang tot kennis om dreigingen te onderkennen en zich weerbaar te maken. Het aantal slachtoffers van cybercriminaliteit steeg mede hierdoor dan ook met 3%. De 5 vormen van cybercrime die het meest worden genoemd in het onderzoek van GfK zijn: malware, phishing, ransomware, datalekken en datadiefstal.

En onder de vormen die als het meest bedreigend worden ervaren steekt ransomware er met kop en schouders bovenuit. Dit blijkt ook uit een onderzoek naar deze gijzelsoftware van Help Net Security.

Het rapport van Help Net Security is gebaseerd op een enquête gehouden onder ruim 500 leidinggevenden werkend in het mkb. Het blijkt dat 78% van de mkb'ers - werkzaam in de B2B-markt - weleens losgeld heeft betaald. Ditzelfde geldt voor 63% van de ondervraagden in de B2C-markt.

**Wat is ransomware?**
*Ransomware is een bepaald type malware, ook wel 'kwaadaardige software' genoemd. Het kan je computer blokkeren of bestanden versleutelen. Ransom betekent letterlijk losgeld. Veelal wordt bij een ransomware-aanval een betaling geëist in de digitale munteenheid Bitcoin. Alleen als je dit losgeld betaalt, krijg je weer toegang tot je computer en/of bestanden. Ransomware wordt ook wel cryptoware of gijzelsoftware genoemd.*

**Een volledig dataherstel wanneer je betaalt?**
Wanneer je als slachtoffer van een ransomware-aanval besluit te betalen, betekent dit niet automatisch dat je al je bestanden – al dan niet zonder schade - terug kan verwachten. Dit blijkt ook uit het onderzoek State of the Phish van beveiliger Proofpoint. Voor het betreffende onderzoek werden de ervaringen van ruim 600 IT-beveiligingsprofessionals uit verschillende landen (onder andere de Verenigde Staten, Engeland en Duitsland) meegenomen. Ondanks dat 69% van de betalende slachtoffers toegang kreeg tot de systemen, bleek dat 22% voor niets betaalde. Deze groep kon niet meer bij de gegijzelde gegevens of de gegevens waren op zo'n manier beschadigd waardoor ze onbruikbaar waren geworden.

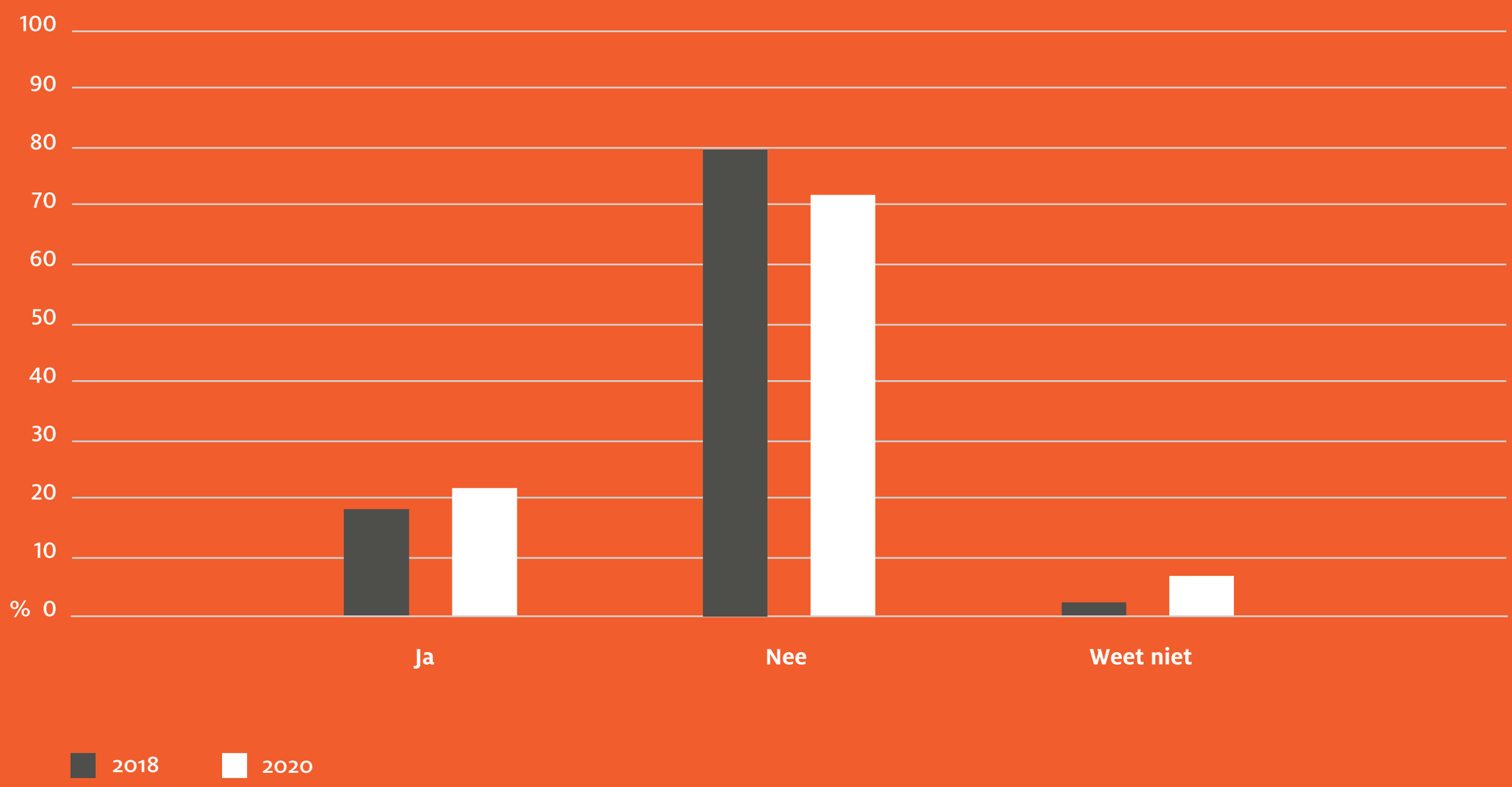
**Wie of wat vormt het lek?**
Uit het onderzoek Trends in Online Security & e-Identity dat wij in 2018 lieten uitvoeren door GfK, kwam naar voren dat er in eerste instantie veel te winnen valt bij de medewerkers. Maar liefst 32% van de cyber-incidenten die worden gemeld bij SecureMe2 (een organisatie met als doel hoogwaardige bescherming te bieden tegen cybercrime voor het mkb) is geïnitieerd door de mens. Dit betekent dat jouw medewerkers voor een derde deel 'aanleiding' zijn voor een aanval. Dit gebeurt voornamelijk door de verspreiding van de zogenaamde phishingmails met daarin verwerkte ransomware- of malwarelinkjes. En deze vorm van cybercriminaliteit voorkom je niet alleen met een goed antivirusprogramma.

# 3 Conclusie #1

Eigenlijk is het best ‘goed nieuws’ dat medewerkers relatief vaak een zwakke schakel vormen in de mate van jouw cybersecurity. Dit gedrag kun je namelijk beïnvloeden door kennis te verspreiden. Vragen als: “Welke vormen van cybercrime zijn er?”, “Hoe herken ik het?” én “Hoe ga ik ermee om?”, moeten voor iedere medewerker worden beantwoord. Ben je benieuwd? Gelukkig hebben wij al deze vragen beantwoord in de whitepaper Zo wordt het mkb cyberweerbaar!

In de volgende paragraaf gaan we dieper in op de vraag of mkb’ers zich eigenlijk wel zorgen maken over cybercrime. Vaak wordt gezegd van niet, maar hier lijkt toch verandering in te komen. En welke maatregelen worden er op dit moment toegepast door het mkb?

> Grafiek 1: Is uw bedrijf in de afgelopen 12 maanden in aanraking gekomen met cybercrime?




Grafiek 1: Is uw bedrijf in de afgelopen 12 maanden in aanraking gekomen met cybercriminaliteit? (bron: GfK, n=512 (2018) n=577 (2020))

# 4 Conclusie #2 Cybercriminaliteit wordt voor ondernemers steeds meer een zorgenkindje

In het eerder genoemde onderzoek dat GfK onlangs voor ons uitvoerde, werd de respondenten ook de volgende vraag gesteld: “In hoeverre ervaart u cybercriminaliteit voor uw bedrijf als bedreigend?”

Het blijkt dat cybercriminaliteit steeds hoger scoort als bron van zorgen. Zo is er sprake van een lichte stijging onder mkb’ers; op dit moment ervaart namelijk 22% cybercrime als ‘vrij bedreigend’ en 57% vindt deze vorm van criminaliteit ‘een beetje bedreigend’. In het onderzoek dat GfK in 2019 uitvoerde, kwam naar voren dat 9,9% van de respondenten cybercrime als ‘vrij bedreigend’ zag. Er is dus sprake van een aanzienlijke stijging in een relatief korte periode.

In het meest recente onderzoek kwam ook naar voren dat één op de 10 mkb’ers cybercriminaliteit zodanig bedreigend vindt, dat er zelfs gevreesd wordt voor de continuïteit van het bedrijf.

**Welke securitymaatregelen nemen ondernemers?**

1. 62% heeft een goed antivirusprogramma
2 52% heeft een sterk spamfilter voor e-mail
3. 47% vervangt/updatet regelmatig zijn of haar apparaten
4. 43% heeft een extra beveiligd wifi-netwerk
5. 40% heeft een streng beleid met betrekking tot wachtwoorden
6. 40% heeft een externe data-opslag via de cloud

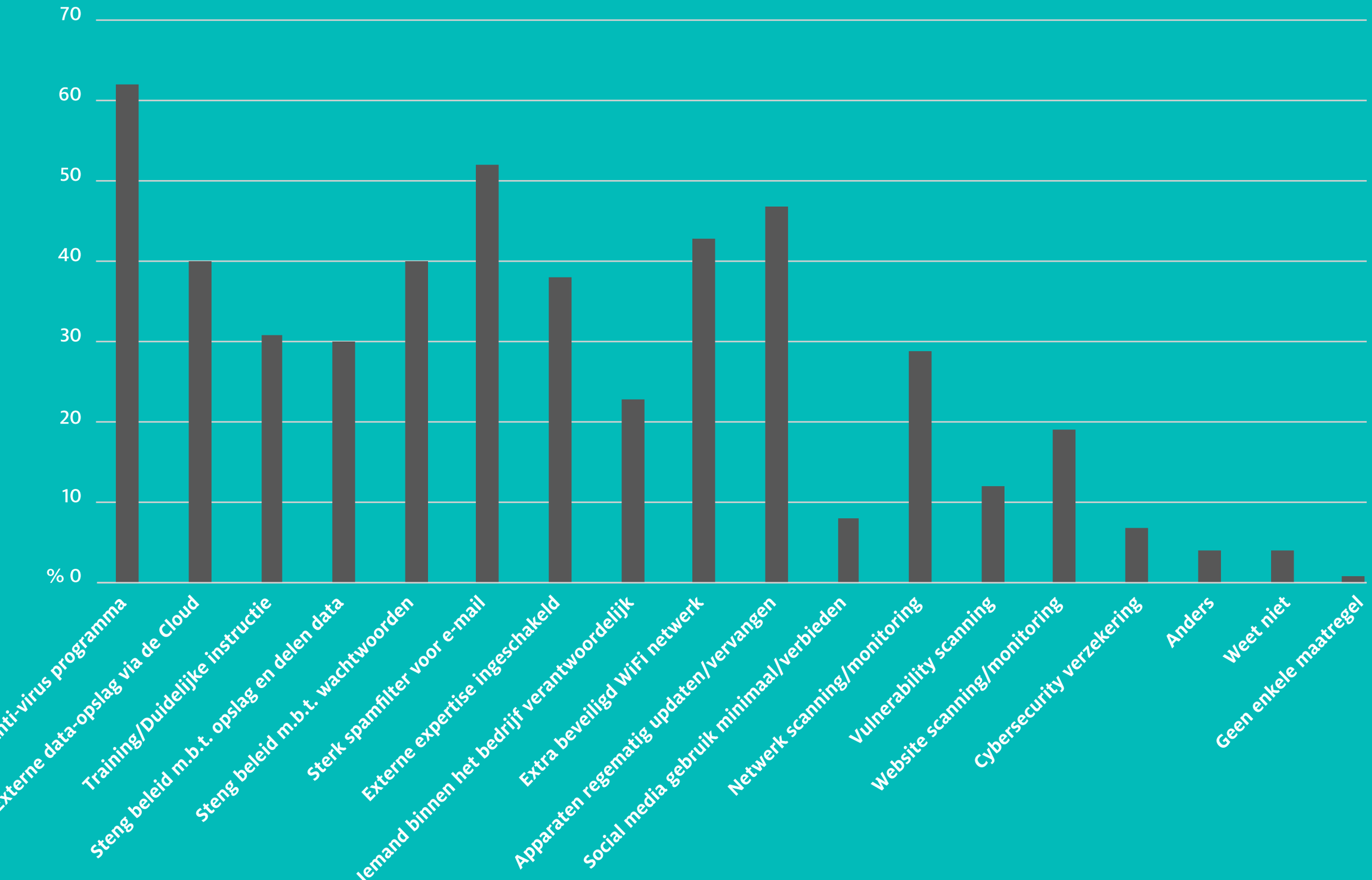
**Waar lopen mkb’ers op vast?**

Bij het organiseren van cybersecurity lopen bedrijven vooral op tegen de snelle ontwikkelingen die ze nauwelijks bij kunnen houden. Ook is er sprake van een gebrek aan budget. Verder wordt aangegeven dat veel security-oplossingen niet op bedrijven van een kleinere omvang zijn afgestemd, wat ook weer te maken heeft met budgettering.
In de volgende paragraaf delen we gegevens over het vertrouwen dat mkb’ers hebben in hun IT-leverancier wat betreft cybersecurity. Wordt er misschien onterecht te veel verwacht vanuit de kant van het mkb?

> Grafiek 2: Welke cybersecuritymaatregelen heeft uw bedrijf genomen?

*“Veel ondernemers denken dat alleen het gebruik van een virusscanner en firewall voldoende is om het bedrijf te beschermen tegen een kwaadwillende. Helaas is dit niet (meer) zo... Een virusscanner signaleert namelijk alleen bekende dreigingen en kijkt daarbij niet naar abnormaal verkeer in je netwerk. Nieuwe dreigingen worden met een virusscanner niet herkend. En ook een firewall kan niet al het gevaarlijke netwerkverkeer buiten houden.”*

*Liesbeth Kempen, IT Security Management Consultant*




Grafiek 2: Welke cybersecuritymaatregelen heeft uw bedrijf genomen? (bron: GfK n=577)

# 5 Conclusie #3 Mkb'ers vertrouwen massaal op hun IT-leverancier als het om cybersecurity gaat

Volgens het onderzoek van GfK is het vertrouwen in IT-leveranciers groot, als het om cybersecurity gaat. Maar liefst 79% is het eens met de volgende stelling: ik vertrouw erop dat mijn IT-leveranciers hun zaken op orde hebben voor wat betreft cybersecurity. Dit vertrouwen is vooral gebaseerd op communicatie over maatregelen, snelheid van informeren over incidenten en reputatie. Maar uit onderzoek van Centraal Beheer komt naar voren dat IT-leveranciers op hun beurt aangeven dat 58% van hun mkb-klanten onvoldoende beschermd is.

**Verwacht het mkb misschien te veel van de IT-beheerder?**
Toch gaan de meeste mkb'ers ervan uit dat hun IT-beheerder een bepaalde zorgplicht heeft en hen in zekere zin beschermt tegen cyberrisico's. Maar in slechts 22% van de gevallen blijken hier ook daadwerkelijke afspraken over te zijn gemaakt. Daarnaast zijn IT'ers niet per definitie cybercrime-experts: veiligheid vergt een andere expertise dan performance en beschikbaarheid.

Securityleveranciers onderscheiden zich vooral van IT'ers door klanten sneller en regelmatiger te informeren over het betreffende onderwerp. Een voorbeeldsituatie: de IT'er is lang niet altijd meer betrokken bij de inkoop van apparaten die verbinding maken met internet. Bovenal gaat cybersecurity verder dan techniek alleen. Hoe gaan medewerkers om met verdachte linkjes en phishingmails? Dit is minstens zo belangrijk als een goed antivirusprogramma. En om ook dit allemaal in goede banen te leiden is er tijd nodig, wat vaak niet genoeg beschikbaar is bij jouw IT-leverancier.

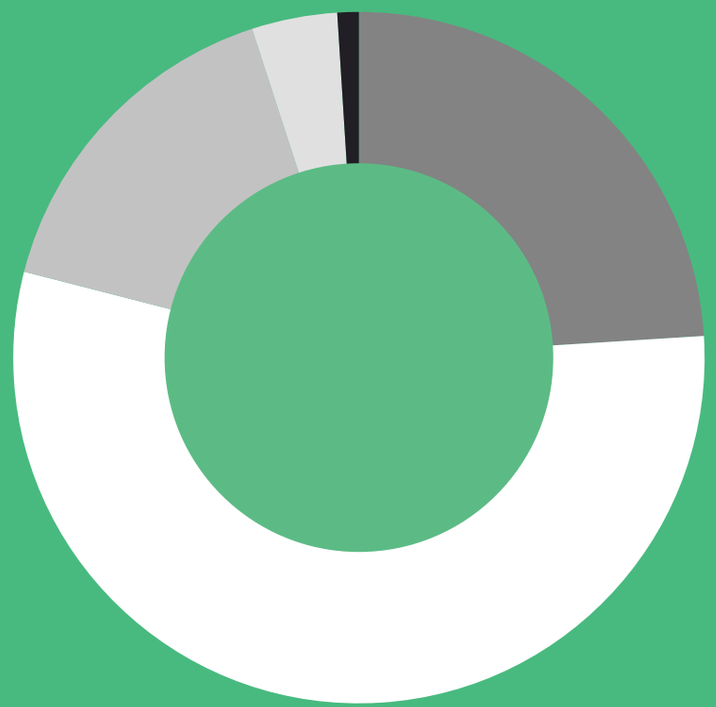
**Hoe serieus neem jij jouw cyberweerbaarheid?**
Na het lezen van al deze ondervindingen heb je misschien wel een idee in hoeverre jij je zorgen moet maken wat betreft de cybersecurity van jouw onderneming. Wellicht hebben 'horrorverhalen' van andere ondernemers in jouw directe omgeving daar ook wel invloed op gehad en vind je het tijd worden om je te gaan weren tegen cybercriminelen.

Uiteraard is een 100% veiligheidsgarantie in de securitywereld niet mogelijk. Maar je kunt wel een heel eind komen met wat extra stappen naast een virusscanner en firewall. Dit doe je aan de hand van het creëren van inzicht in de online securityrisico's van jouw bedrijf. Want bij elk bedrijf, hoe groot of klein ook, valt wel iets te halen. Daarnaast is elk bedrijf tegenwoordig een target geworden van hackers die geautomatiseerde tools op je website loslaten.

Neem de mate van cyberweerbaarheid serieus, als je de continuïteit van je bedrijf wilt bewaken. Jij bent immers de enige eindverantwoordelijke en aansprakelijke, mocht het mis gaan.

> Grafiek 3: In hoeverre bent u het eens met onderstaande stellingen - Ik vertrouw dat mijn IT-leveranciers hun zaken op orde hebben als het om cybersecurity gaat.

> Grafiek 4: U geeft aan vertrouwen te hebben in uw IT-leverancier(s). Waar is dit vertrouwen op gebaseerd?



Geheel mee eens

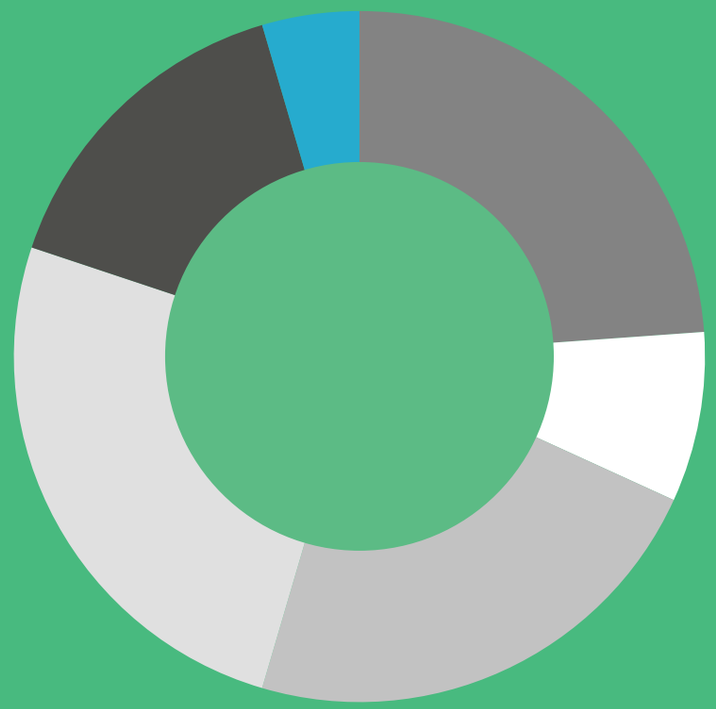
Mee eens

Niet mee eens, maar ook niet oneens

Mee oneens

Geheel mee oneens

Grafiek 3: In hoeverre bent u het eens met onderstaande stellingen – Ik vertrouw dat mijn IT-leveranciers hun zaken op orde hebben als het om cybersecurity gaat (bron: GfK n=577)



- Ze informeren mij regelmatig over cybersecuritymaatregelen
- Ze bieden een dashboard waarop ik continu kan zien wat de status is
- Hun reputatie als expert in de markt
- De snelheid waarmee zij mij informeren over incidenten
- Hun trackrecord als leverancier van ons bedrijf
- Anders

Grafiek 4: U geeft aan vertrouwen te hebben in uw IT-leverancier(s). Waar is dit vertrouwen op gebaseerd? (bron: GfK n=458)

# 6 Hoe serieus neem jij jouw cyberweerbaarheid?

Als je als mkb'er cyberdreigingen buiten de deur wilt houden, is de ideale situatie dat kwaadaardig verkeer wordt opgespoord aan het begin van je netwerk. Het verkeer wordt dan geanalyseerd op basis van gedrag, bestemmingen en tijd. Zo ontdek je tijdig uitzonderingen en zit je kort op de bal. Maar vaak zijn meldingen niet leesbaar, althans niet als je geen supertechneut bent. Daarom hebben wij CyberSterk ontwikkeld. CyberSterk geeft je direct inzicht in de online securityrisico's van jouw bedrijf. Je netwerk en je website worden gecontroleerd door onder andere de fysieke CyberSterk-box.

Ook analyseren we realtime je netwerkverkeer. Bij verdachte – en ongewenste – activiteiten slaan we alarm. Rapporteren van risico's gebeurt in begrijpelijke taal in ons dashboard. Zo kun je snel actie ondernemen om veilig en onbezorgd te blijven ondernemen. Omdat je als ondernemer op deze manier snapt wat er mis is, kun je ook echt het gesprek aangaan met je IT-partner en zoeken naar een oplossing. Heb je geen IT-partner dan kun je voor advies en een oplossing contact opnemen met het CyberSterk-supportteam.

SIDN CyberSterk

**Benieuwd naar wat CyberSterk voor jouw bedrijf kan betekenen?**
https://www.cybersterk.nl/
https://www.sidn.nl/cybersterk

**Wat we doen**

- We maken op afstand een wekelijkse scan van je website. Die brengt de risico's van jouw website in kaart.
- De fysieke CyberSterk-box die we in je bedrijfsnetwerk plaatsen, detecteert afwijkend internetverkeer in en aanvallen op je bedrijfsnetwerk. Bij verdachte zaken slaan we alarm.
- De scanresultaten geven we in heldere taal weer op een overzichtelijk dashboard, ook op je mobiel, inclusief notificaties van problemen.
- Periodiek voeren we een phishingsimulatie uit en meten we het klikgedrag van je medewerkers.
- Iedere maand sturen we je een rapportage met de belangrijkste scanresultaten.
- Is er iets aan de hand? Neem contact op met je IT-partner of ons supportteam zodat we samen kunnen kijken hoe we het issue kunnen oplossen

**Wij zijn SIDN**

Wij zijn SIDN (Stichting Internet Domeinregistratie Nederland) en sinds 1996 verantwoordelijk voor het beheer van het .nl-domein. Onze missie: mensen en organisaties verbinden voor een zorgeloos en kansrijk digitaal bestaan. We dragen bij aan de veiligheid van het internet in Nederland en doen onderzoek naar cybersecurity en monitoren verdacht gedrag. Hiervoor ontwikkelen we ook nieuwe diensten, zoals CyberSterk.

# Colofon

Dit rapport bevat de highlights van een onderzoek dat is uitgevoerd door GfK in opdracht van SIDN.
Aan dit onderzoek werkten mee:

**GfK**
Henk Delfos – Industry Lead
Erica Nagelhout – Senior Research Manager Consumer Insights

**SIDN**
Christiene Bouwens – Marketingmanager
Michiel Henneke – Marketingmanager
Martin Sluijter – Communicatieadviseur

**Canvass Company**
Esther Derks – Bedrijfsjournalist

Heb je vragen over het onderzoek, mail dan naar
communicatie@sidn.nl

**Meld je aan voor onze nieuwsbrief**
www.sidn.nl/nieuwsbrief

**SIDN**
Postbus 5022
6802 EA Arnhem
Meander 501
6825 MD Arnhem
T +31 (0)26 352 55 00
www.sidn.nl