

KANTAR

Flitspeiling Cyberweerbaarheid Ondernemers

Bart Koenen en Manuel Kaal

15 oktober 2020

244408446



Achtergrond en doel van het onderzoek

Kleine ondernemers, ondernemers met minder dan 10 werknemers en ZZP'ers, dienen als organisatie ook op het gebied van IT hun eigen zaken goed voor elkaar te hebben. Het ministerie van Economische Zaken en Klimaat (EZK) wil ervoor zorgen dat deze ondernemers minder kwetsbaar zijn voor cyber gerelateerde dreigingen.

Om dat voor elkaar te krijgen werkt de Directie Communicatie van het ministerie EZK samen met het Digital Trust Center. Doel van deze samenwerking is om de cyberweerbaarheid van kleine Nederlandse ondernemers te verhogen door onder andere tools aan te bieden om reputatie- en economische schade voor bedrijven te voorkomen.

Een van de trajecten richt zich op het maken van kwalitatief goede back-ups. Door het maken van periodieke back-ups en deze zowel in een digitale- en fysieke omgeving te bewaren en een back-up test te doen is de ondernemer altijd weerbaar tegen cyberdreigingen omdat deze een back-up heeft van eigen bestanden.

Dit onderzoek geeft inzicht in welke factoren belangrijk zijn voor kleine ondernemers om zelfstandig goede back-ups te kunnen maken. Het onderzoek is een fase in een gedragstraject opgezet door het ministerie van EZK.

Management summary

Bijna alle ondernemers maken back-ups

Van alle kleine ondernemers die back-ups maken doen de meeste ondernemers dit zelf (75%), 10% laat dit doen door hun software leverancier en 5% heeft een bedrijf ingehuurd. De back-ups worden vooral gemaakt omdat ondernemers zich verantwoordelijk voelen voor klantgegevens (56%). De kleine groep ondernemers die aangeeft geen back-ups te (laten) maken (10%) doet dit vooral omdat zij niet of nauwelijks werken met computers of smartphones.

Back-ups maken wordt als efficiënt gezien

Het maken van back-ups wordt door 93% van alle ondernemers gezien als een (zeer) efficiënte beveiligingsvorm tegen cybercrime. Bovendien geven acht op de tien ondernemers aan dat zij het maken van back-ups makkelijk vinden. Andere beveiligingsvormen die als (zeer) efficiënt worden gezien zijn verstandig e-mail gebruik (85%) en het tijdig updaten van software (83%).

Externe harde schijf wordt het vaakst als opslaglocatie gebruikt

Van bestanden met financiële gegevens (63%) en privacy gevoelige informatie van klanten (54%) word het vaakst een back-up opgeslagen. Een externe harde schijf wordt door 65% van de ondernemers - die back-ups (laten) maken - gebruikt als opslaglocatie voor de back-ups. Daarnaast worden cloud storage (37%) en een USB-stick (22%) redelijk vaak als opslaglocatie genoemd.

Er kan nog een stap worden gezet in het maken van kwalitatief goede back ups

Ruim acht op de tien ondernemers voelt zich verantwoordelijk voor het maken van back-ups van bestanden met bedrijfs- en klantinformatie. Daarnaast is 61% bang om gegevens kwijt te raken door cybercrime.

In het meest veilige scenario wordt dagelijks een back-up gemaakt, wordt de back-up bewaard op een fysieke en digitale locatie en is een back-up test uitgevoerd.

Wanneer men zelf back-ups maakt doet 30% van de ondernemers dit dagelijks en als dit wordt uitbesteed is dit 62%. In totaal bewaart 53% van de ondernemers (die back-ups maken) de back-up op meer dan één opslaglocatie, ongeveer een kwart van de ondernemers bewaart een back-up zowel op een fysieke als een digitale plek. Iets meer dan de helft (56%) van de ondernemers heeft wel eens een back-up test uitgevoerd. Ondernemers die nog nooit een back-up test hebben gedaan, geven met name aan daar nog nooit over te hebben nagedacht.

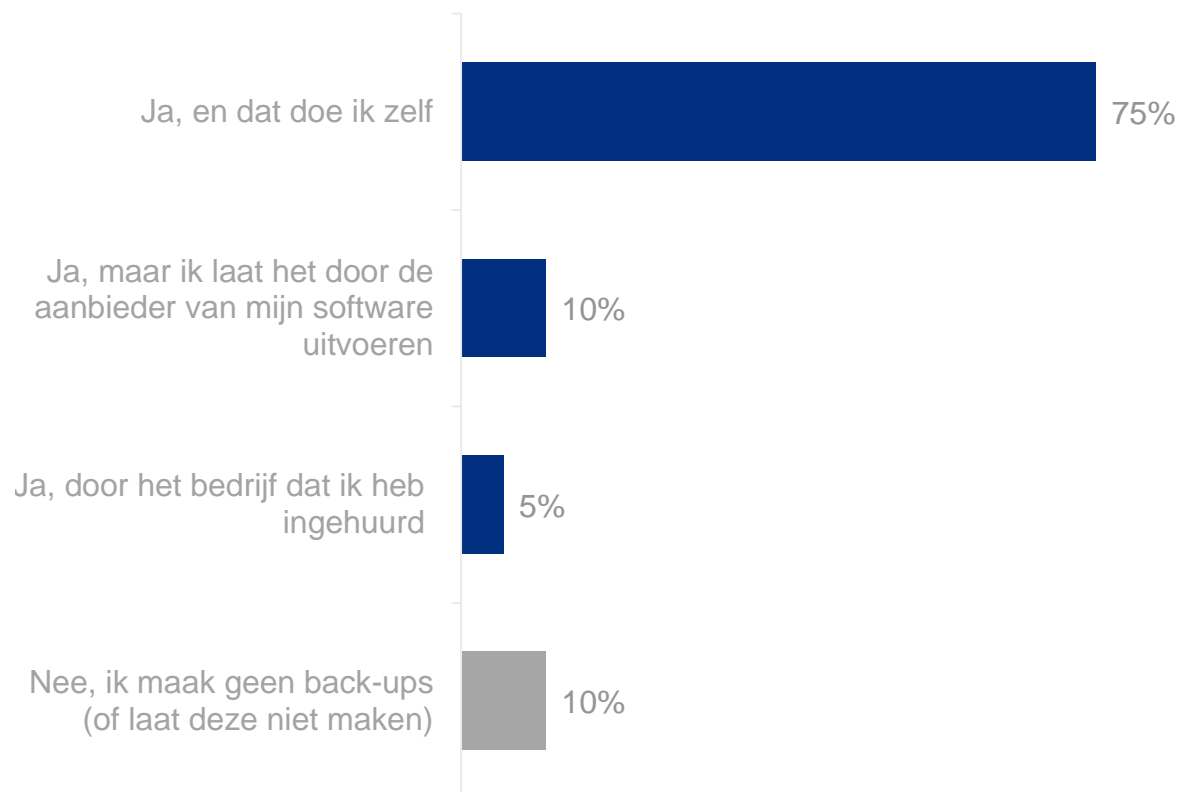
1

Maken van back-ups in de dagelijkse praktijk



Negen op de tien ondernemers maakt (al dan niet zelf) back-ups van bestanden met bedrijfsinformatie

- Van alle kleine ondernemers die back-ups maken doen de meeste ondernemers dit zelf (75%), 10% laat dit doen door hun software leverancier en 5% heeft een bedrijf ingehuurd.



“ ” Toelichting waarom men zelf back ups maakt

“Weet hoe het moet dus geen moeite.”

“Wij doen alles zelf, we hebben maar kleine bedrijfsbestanden online.”

“Ik wil geen dataverlies als mijn pc crasht of wordt aangevallen. Ik heb ook een back-up buiten mijn bedrijf want brand kan ook alles vernietigen.”

“Gaat automatisch. Zorgen dat bij crash of ransomware alles veilig is.”

“ ” Toelichting waarom men back ups laat maken

“Veiliger, constanter (zij plannen dat structureel in, terwijl ik moet er als eenpitter echt een taak van maken), als het niet lukt om wat voor reden dan ook, dan gaan zij gelijk aan de slag om het probleem op te lossen en zorgen dat die back-up toch gemaakt wordt.”

“Omdat ik een digibeet ben.”

“Met dit soort dingen moet je zekerheid en expertise boven alles stellen.”

Nu volgt een aantal vragen die specifiek gaan over het maken van back-ups. Maakt u weleens back-ups van bestanden met bedrijfsinformatie? (n=449)
U gaf aan dat u de back-ups van uw bedrijfsbestanden zelf maakt. Wat zijn de belangrijkste reden(en) om dit zelf te doen?

Een kleine groep ondernemers (10%) maakt geen back-ups, de meest genoemde reden is dat zij nauwelijks met computers of smartphones werken

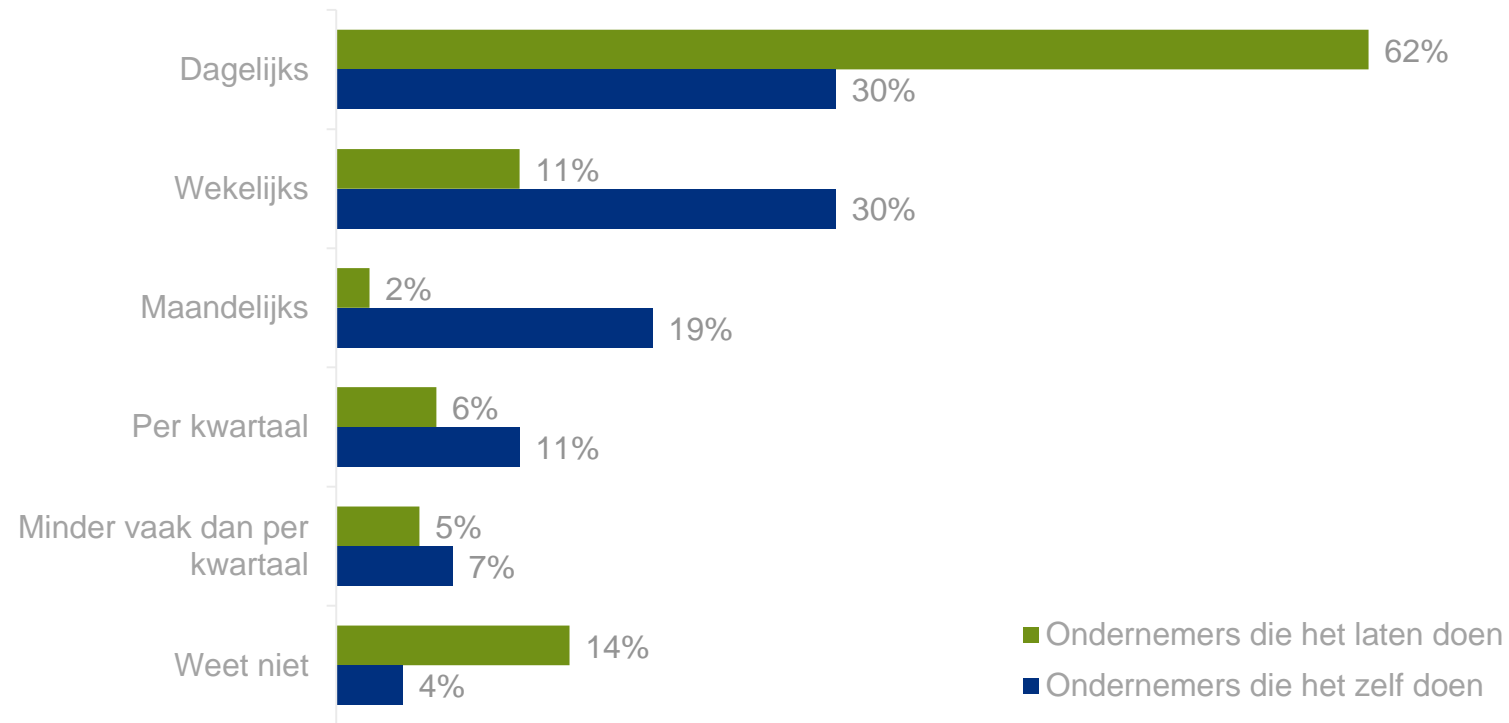
- Daarnaast geeft één op de vijf ondernemers aan niet te weten wat cybercriminelen aan hun bedrijfsinformatie hebben en/of weten ze niet van welke bestanden zij een back-up zouden moeten laten maken.



U gaf aan dat er in uw bedrijf geen back-ups worden gemaakt van bestanden met bedrijfsinformatie. Wat zijn de drie belangrijkste redenen om dit niet te (laten) doen? ? (n=47)

Ondernemers die het maken van back-ups hebben uitbesteed maken vaker dagelijkse back-ups dan ondernemers die het zelf doen

- Ondernemers die zelf back-ups maken doen dit dagelijks (30%) of wekelijks (30%). Daarentegen wordt 62% van de back ups dagelijks gemaakt als dit is uitbesteed.

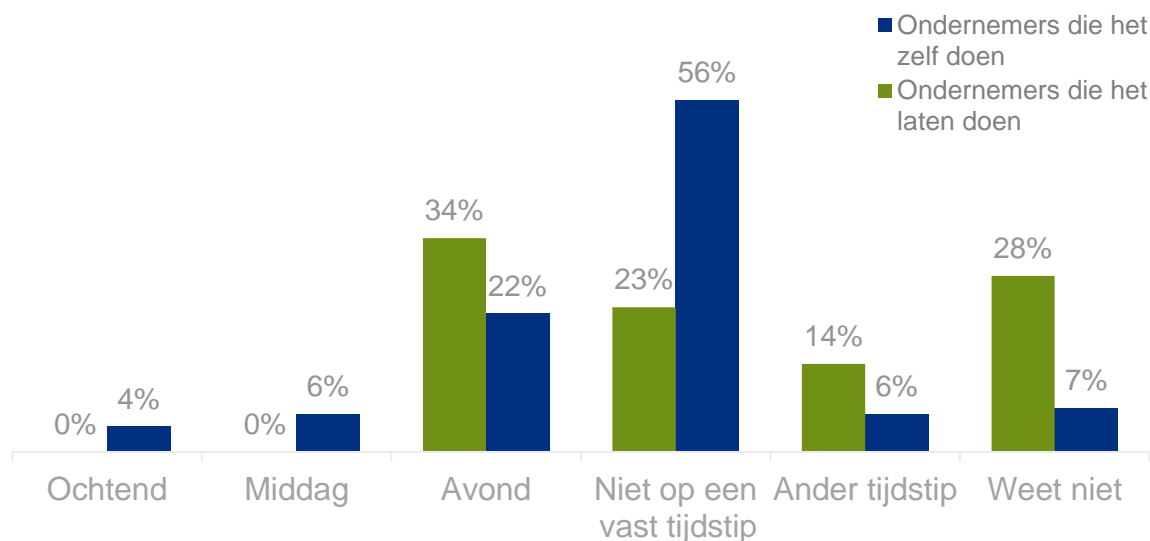


Hoe vaak maakt u back-ups van bestanden met bedrijfsinformatie? (n=338) / Hoe vaak worden in uw bedrijf back-ups gemaakt van bestanden met bedrijfsinformatie? (n=64)

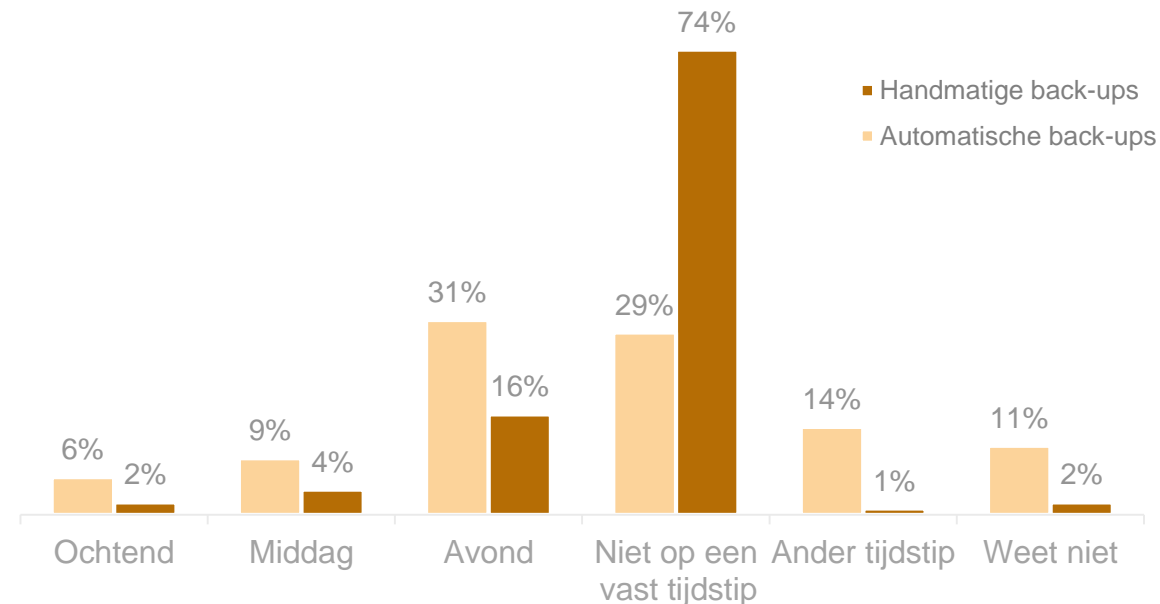
Driekwart van de ondernemers die handmatig een back-up uitvoeren, doen dit niet op een vast tijdstip

- Ondernemers die een back-up laten uitvoeren, doen dit veelal in de avond (34%), of geven aan niet te weten wanneer dit gebeurt (28%).

Dagdeel dat de back-ups worden gemaakt



Dagdeel dat de back-ups worden gemaakt

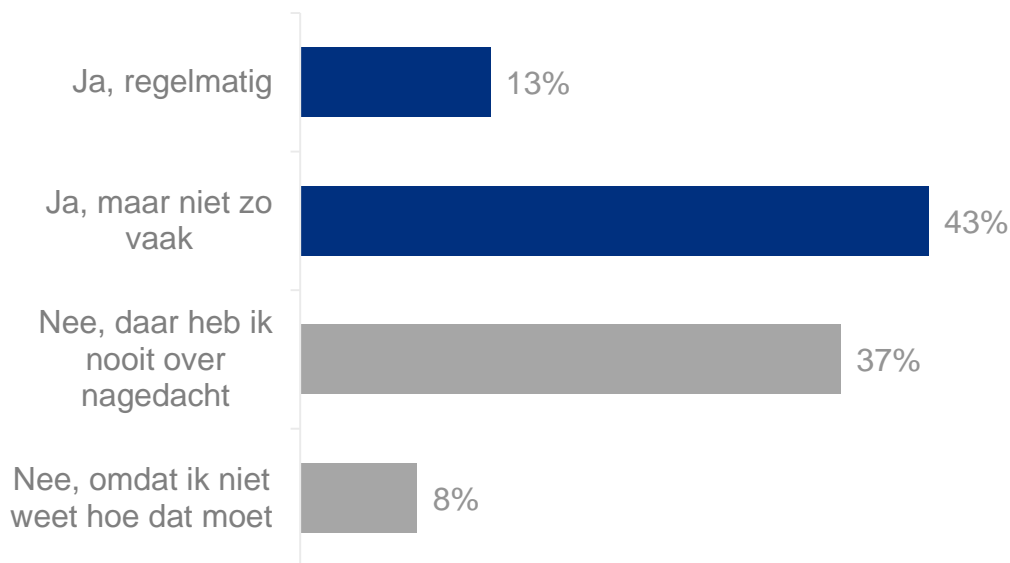


Hoe vaak maakt u back-ups van bestanden met bedrijfsinformatie? (n=338) Hoe vaak worden in uw bedrijf back-ups gemaakt van bestanden met bedrijfsinformatie? (n=64)
 Op welk dagdeel maakt u back-ups of worden die voor u gemaakt? (n=402) Maakt u de back-ups handmatig of automatisch? (n=338)

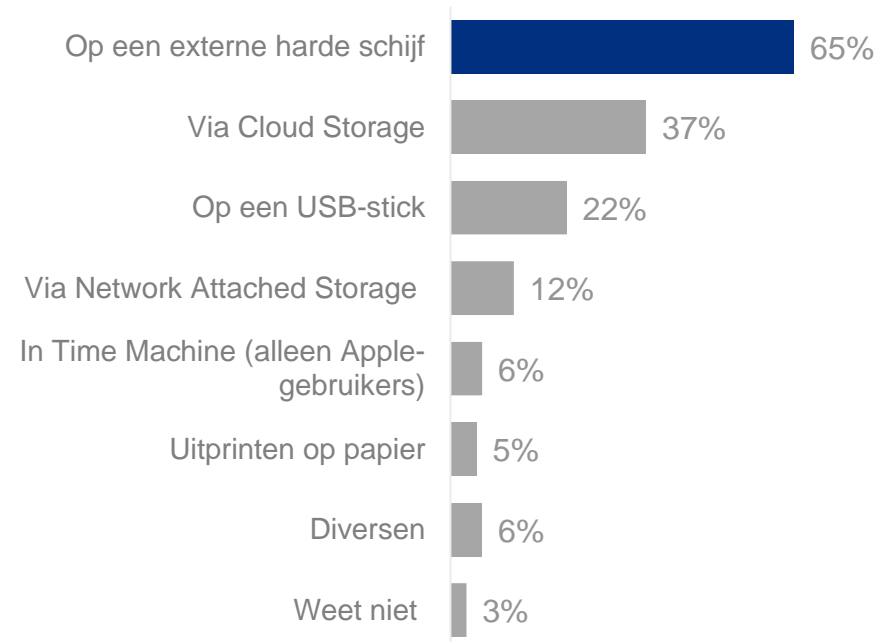
Iets meer dan de helft (56%) van de ondernemers heeft wel eens een back-up test uitgevoerd

- Ondernemers die nog nooit een back-up test hebben gedaan, geven met name aan daar nog nooit over te hebben nagedacht.
- In totaal bewaart 53% van de ondernemers (die back-ups maken) de back-up op meer dan één opslaglocatie, ongeveer een kwart van de ondernemers bewaart een back-up zowel op een fysieke als een digitale plek (dit is niet in de grafiek weergegeven).

De mate waarin back-ups worden getest



Opslaglocaties back-ups



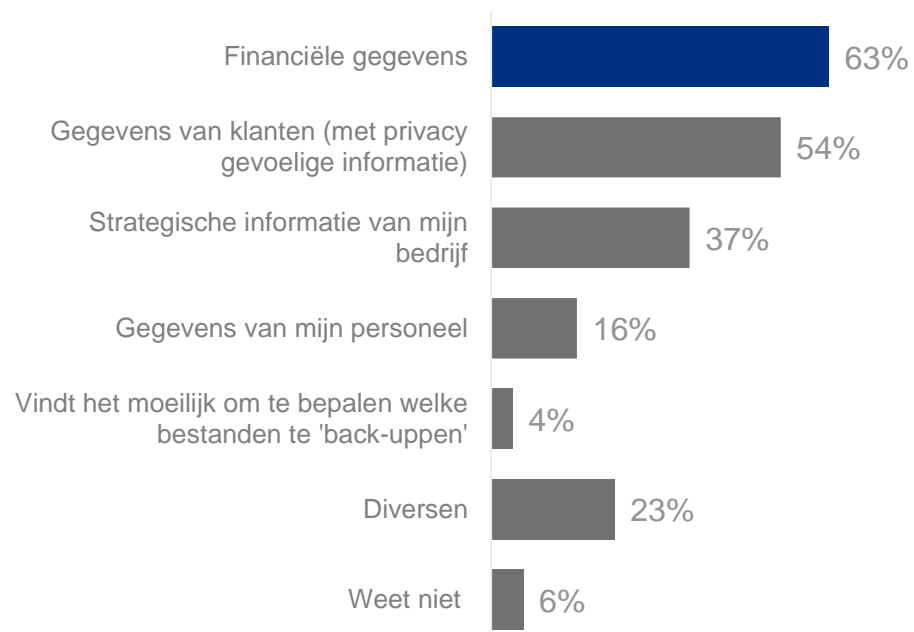
Heeft u ooit een 'back-up test' gedaan door een back-up terug te (laten) zetten op uw computer of netwerk? (n=402)

U kunt op verschillende locaties uw back-ups (laten) opslaan. Op welke locaties worden back-ups van uw bedrijf opgeslagen? (n=402)

Van financiële bestanden en bestanden met privacy gevoelige informatie worden het vaakst back-ups gemaakt

- Van bestanden met strategische bedrijfsinformatie wordt eveneens redelijk vaak een back-up gemaakt.

Van welke bestanden worden back-ups gemaakt?



” Toelichting op de diversen categorie

“Ik back-up alle bestanden op mijn pc.”

“Ik werk in the cloud, dus alle gegevens worden opgeslagen.”

“Van alle bestanden die ik heb of dat nu zakelijk of privé is.”

“Ik maak back-ups van alle bestanden.”

“Maak een volledige back-up van de hele schijf.”

“Dagelijks alle werkbestanden, maandelijks het complete systeem.”

Van welke soort bestanden maakt u back-ups of laat u back-ups maken? (n=402)

2

Houding ten aanzien van het maken van back-ups



Iets meer dan de helft van de ondernemers maakt back-ups omdat zij zich verantwoordelijk voelt voor klantgegevens

- Meeste ondernemers vinden het maken van back-ups gemakkelijk (82%). Er zijn bijna geen ondernemers die aangeven het moeilijk te vinden om een back-up te maken (1%). Zelfs ondernemers die weinig digitaal werken vinden het vaak makkelijk om een back-up te maken.

82%

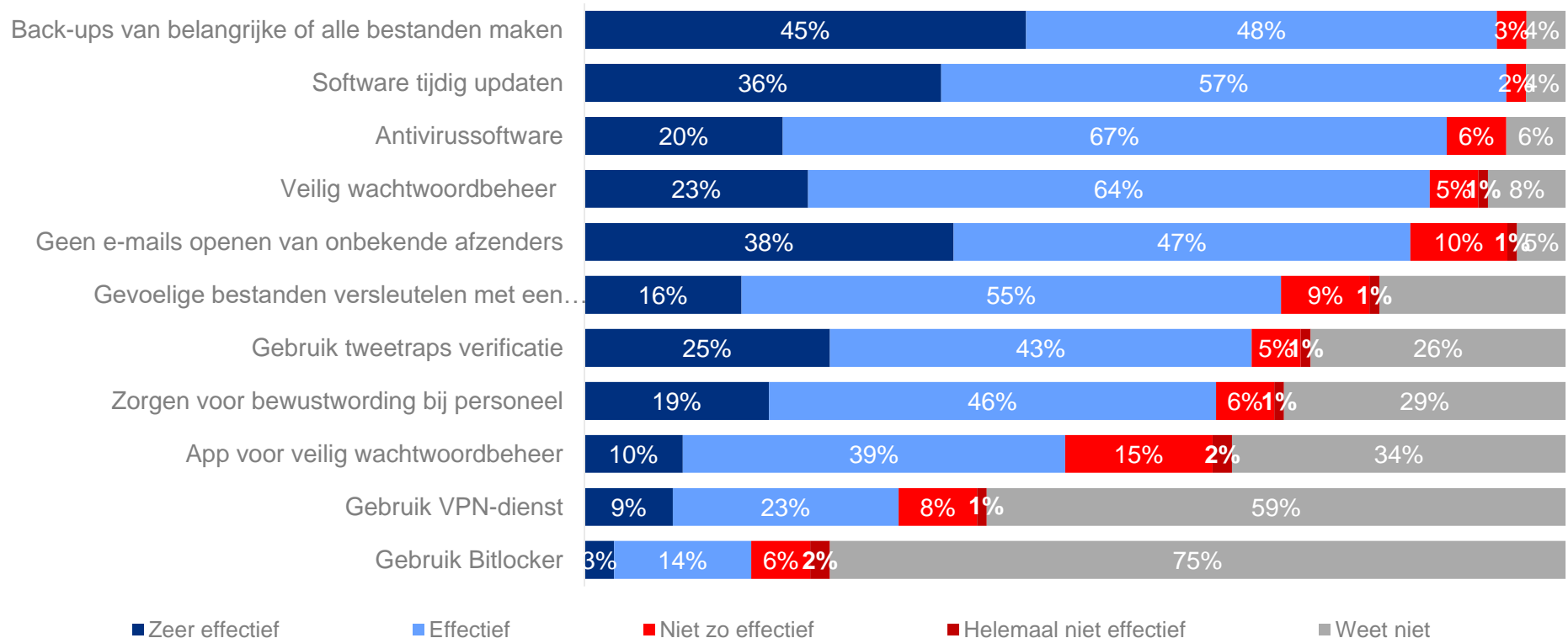
Van de ondernemers vindt het (zeer) makkelijk om een back-up te maken



Kunt u aangeven hoe gemakkelijk of moeilijk u het vindt om deze back-ups te maken? (n=338)
Wat zijn voor u de drie belangrijkste aanleidingen om back-ups van bestanden met bedrijfsinformatie te (laten) maken? (n=402)

Het maken van back-ups, verstandig e-mailgebruik en tijdelijke software updates worden gezien als de meest efficiënte beveiligingsvormen

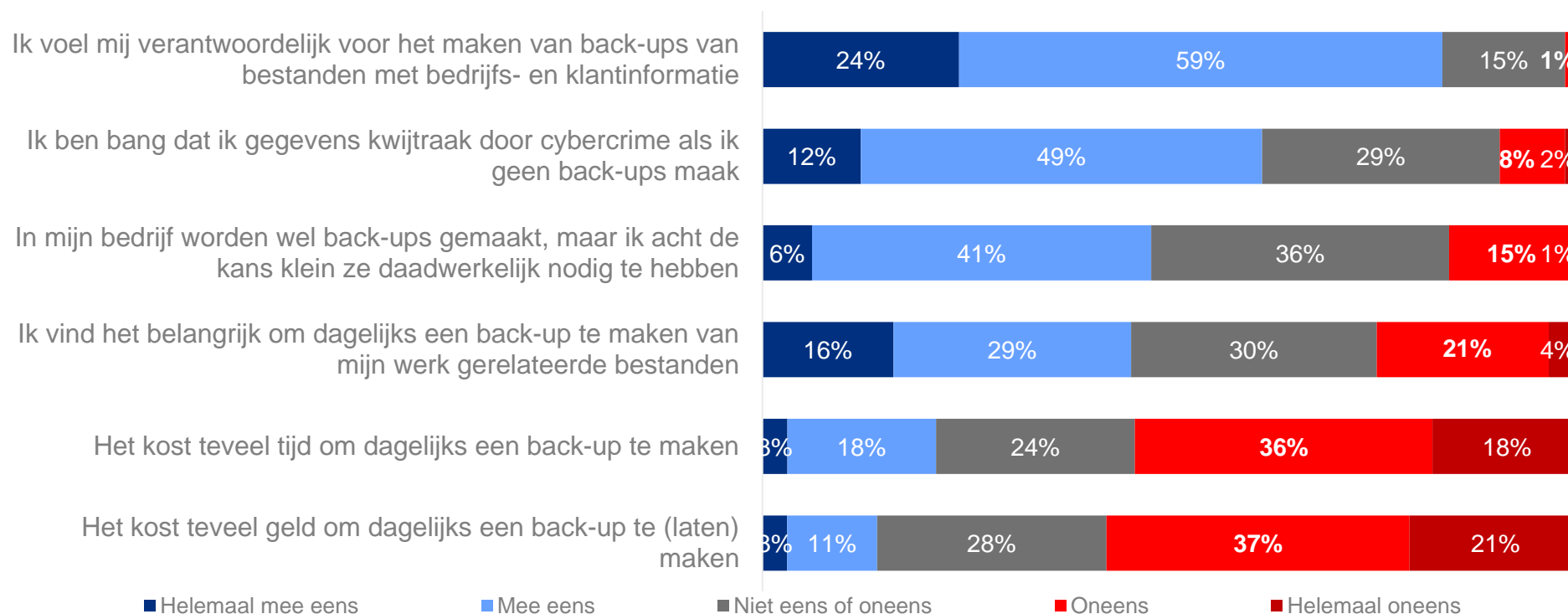
- Het gebruik van een VPN-dienst en Bitlockers zijn twee beveiligingsvormen die relatief vaak onbekend zijn.



U krijgt nogmaals een aantal beveiligingsvormen te zien. Kunt u per beveiligingsvorm aangeven in welke mate u deze effectief vindt? (n=449)

Ruim acht op de tien ondernemers voelt zich verantwoordelijk voor het maken van back-ups van bestanden met bedrijfs- en klantinformatie

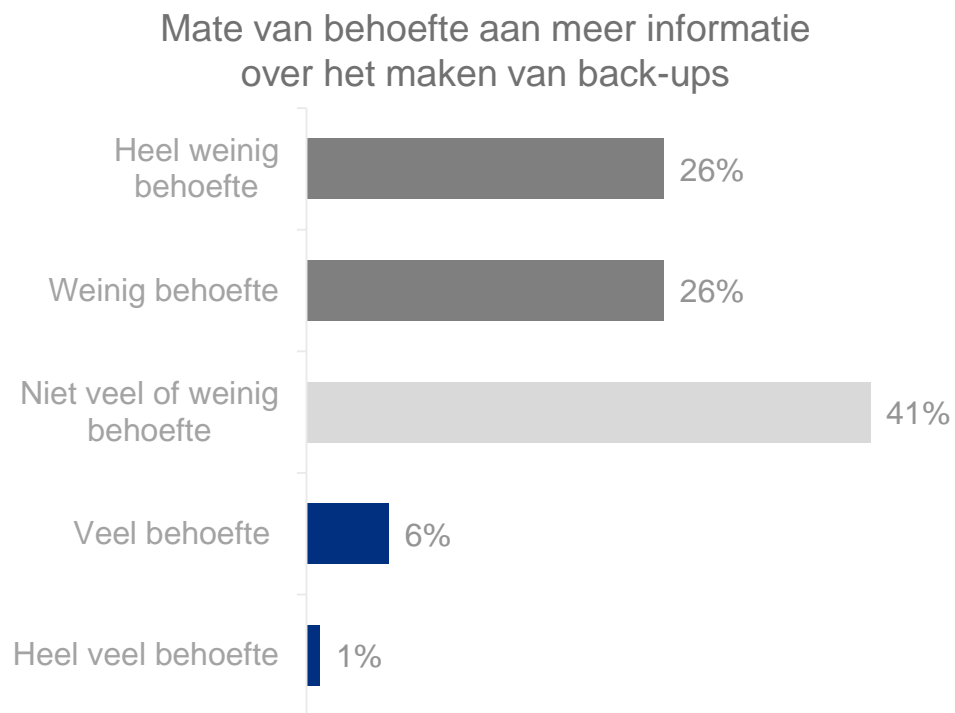
- Daarnaast is 61% bang om gegevens kwijt te raken door cybercrime. Meerderheid van de ondernemers vindt niet dat het dagelijks (laten) maken van back-ups teveel geld kost (58%) of teveel tijd (54%). En een kwart geeft aan het niet belangrijk te vinden om back-ups te maken.



Hieronder staat een aantal uitspraken. Kunt u aangeven in welke mate u het eens of oneens bent met deze uitspraken? (n=449)

Er is weinig behoefte aan meer informatie over het maken van back-ups

- Een kleine groep geeft aan hier wel behoefte aan te hebben (7%) terwijl vier op de tien ondernemers aangeven hier niet veel of weinig behoefte aan te hebben (41%).



” Toelichting aan welke informatie men behoefte heeft

“Wat is de beste manier, hoe vaak moet je het doen.”

“Veilige alternatieven buiten de cloud.”

“Hoe beter automatisch te doen.”

“Status van problemen en aantal cybercrime aanvallen.”

“Hoe je simpel veilig kunt blijven werken.”

“Over het hoe en wat van back-ups.”

“Over de technische processen van een back-up.”

In welke mate heeft u behoefte aan meer informatie over het maken van back-ups als preventiemiddel tegen cybercrime? (n=449)

Open vraag: aan welke informatie heeft u behoefte? (n=31)

Bijna alle ondernemers maken - of laten - back-ups maken, er kan nog een stap worden gezet in het maken van kwalitatief goede back ups

35%

1 Dagelijkse back-ups (laten) maken

Van de ondernemers die back ups maken doet 35% dit dagelijks. Ondernemers die het maken van back-ups hebben uitbesteed maken vaker dagelijkse back-ups dan ondernemers die het zelf doen (62% versus 30%).

25%

2 Back-ups op een digitale en fysieke locatie bewaren

Van de ondernemers - die back-ups (laten) maken – bewaart 25% de back-ups zowel op een fysieke als digitale locatie.

56%

3 Back-up test

Iets meer dan de helft (56%) van de ondernemers heeft wel eens een back-up test uitgevoerd

3

Onderzoeksverantwoording



Onderzoekspecificaties



Doelgroep

Het onderzoek is uitgevoerd onder ZZP'ers en ondernemers met minder dan 10 werknemers die niet werken op, of in, de IT omgeving van één of meerdere (grotere) opdrachtgevers.



Steekproefbron

NIPObase ondernemerspanel.



Respons

Er zijn 650 ZZP'ers en ondernemers uitgenodigd en in totaal hebben 449 personen deelgenomen (response is 69%).



Online methode

Voor dit onderzoek is gebruik gemaakt van een online vragenlijst (CAWI: computer assisted web interviewing). Respondenten ontvingen een e-mail vanuit Kantar Nederland met daarin informatie over het onderzoek en een link naar de online vragenlijst.



Vragenlijst

De vragenlijst is in samenspraak met het ministerie van EZK opgesteld. De invulduur was gemiddeld 10 minuten.



Veldwerkperiode

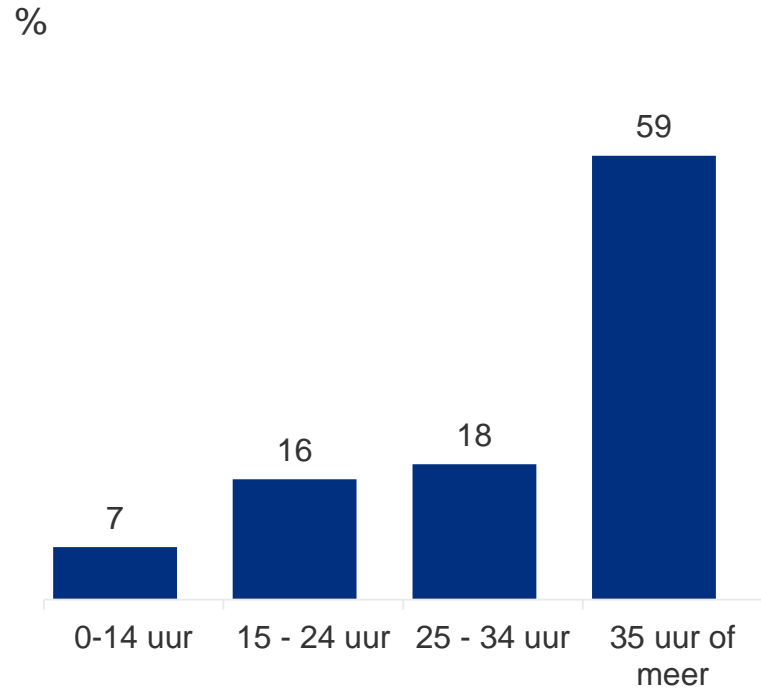
Het veldwerk heeft gelopen van 1 t/m 5 oktober 2020.

BIJLAGE

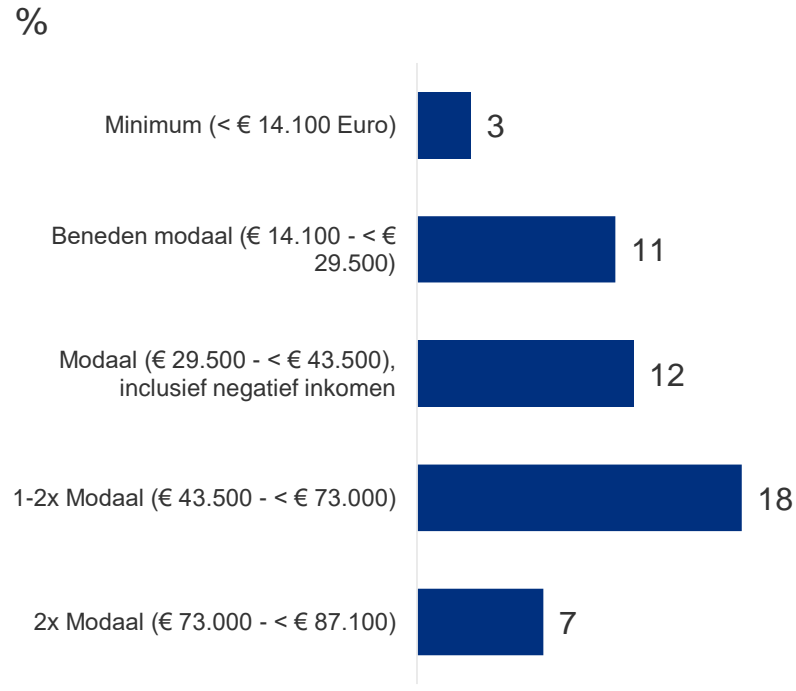



Achtergrondgegevens ZZP en kleine bedrijven (1)

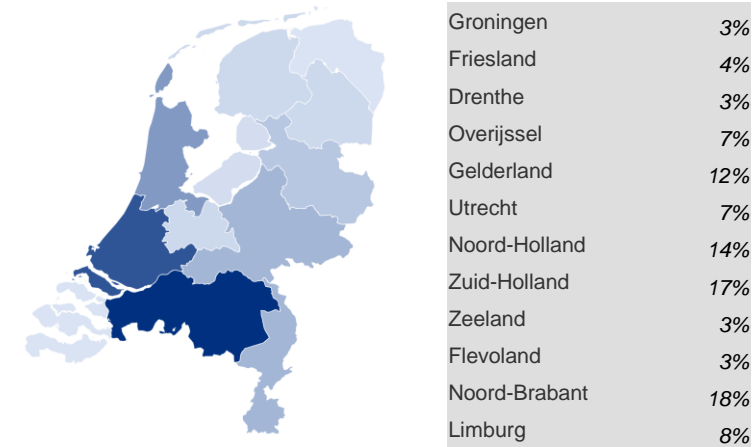
UREN WERKZAAM



INKOMEN



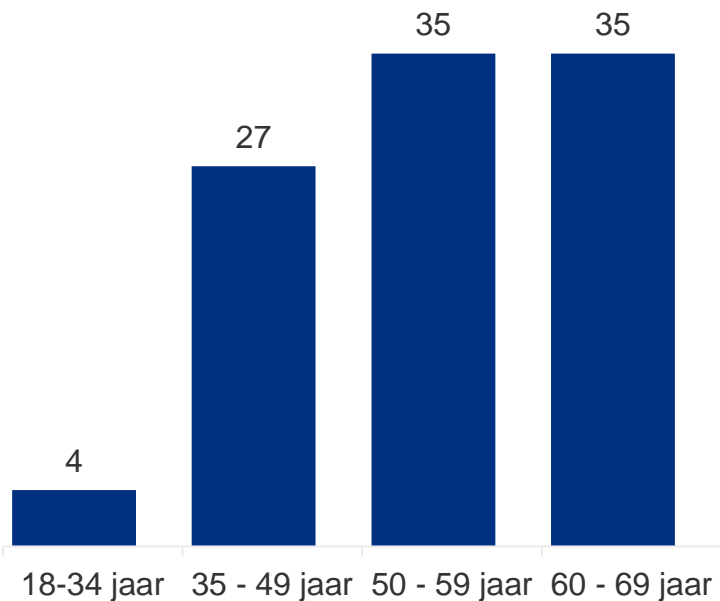
48%  Vrouw



Achtergrondgegevens ZZP en kleine bedrijven (2)

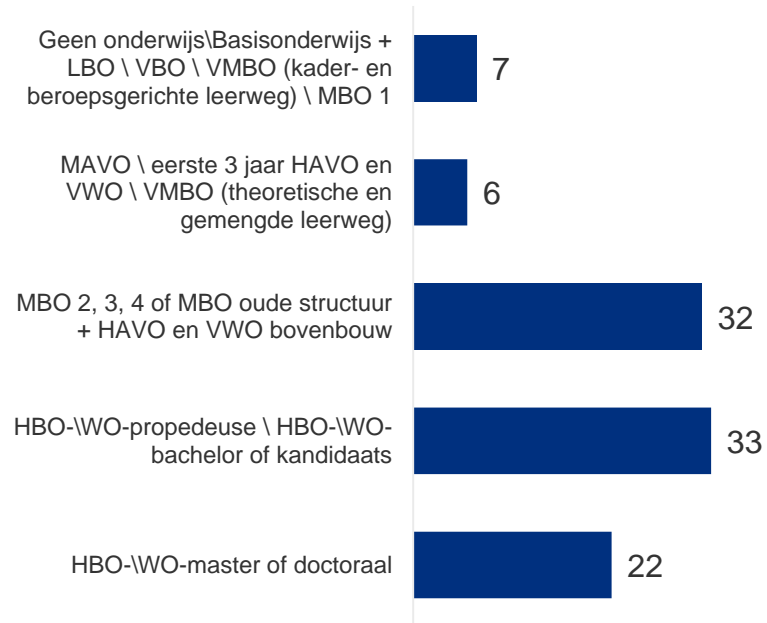
LEEFTIJD

%



OPLEIDING

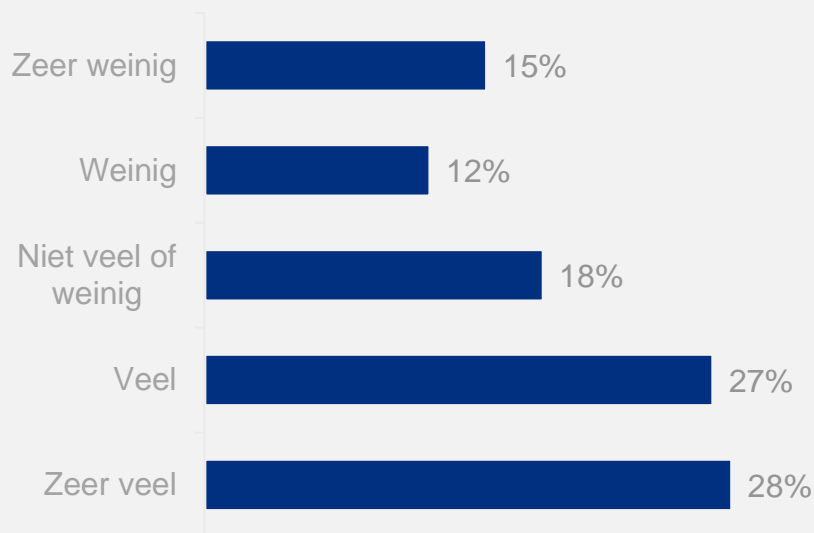
%



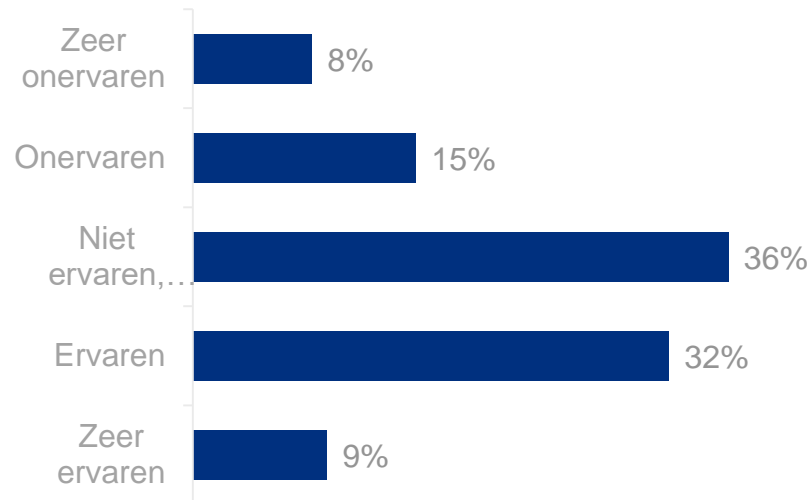
Ruim de helft van de kleine ondernemers werkt (zeer) veel digitaal, ruim vier op de tien geven aan (zeer) veel ervaring te hebben met ICT-producten

- Ruim een kwart van de kleine ondernemers geeft aan (zeer) weinig digitaal te werken (27%). Een iets kleinere groep geeft aan (zeer) onervaren te zijn als het gaat om het werken met ICT-producten in de werk gerelateerde sfeer (22%).

Mate waarin men digitaal werkt



Hoeveel ervaring heeft men met het werken met ICT producten



Verband digitaal werken en ervaring met ICT producten

14%

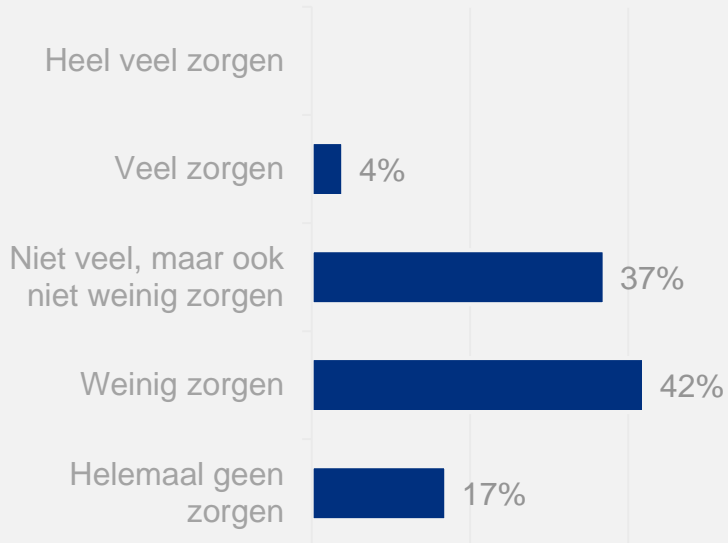
14% van de ondernemers geeft aan én (zeer) weinig digitaal te werken én (zeer) weinig ervaring te hebben met het werken met ICT producten in de werk gerelateerde sfeer.

Als u denkt aan uw dagelijkse werkzaamheden, hoeveel van dit werk doet u dan digitaal? (n=449)
Hoe ervaren of onervaren bent u als het gaat om het werken met ICT producten in de werkgerelateerde sfeer? (n=449)

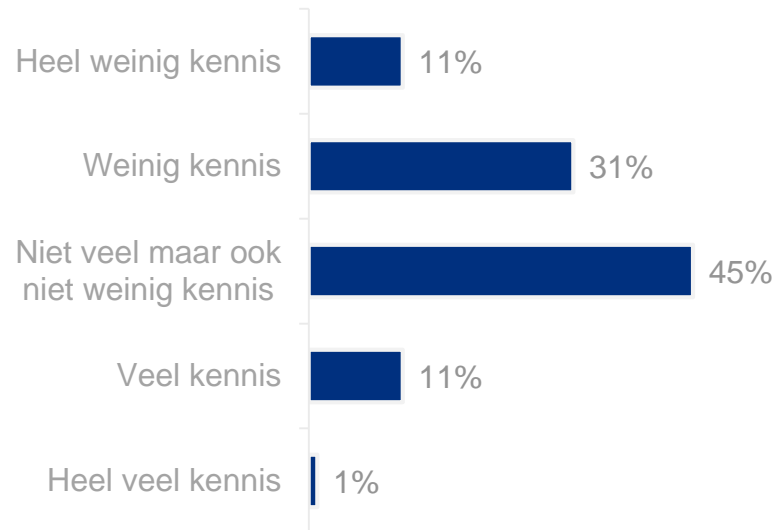
Bijna zes op de tien kleine ondernemers maken zich weinig tot helemaal geen zorgen om de digitale veiligheid van hun bedrijf

- Ondanks de geringe zorgen, is het zelf ingeschatte kennisniveau over digitale beveiliging betrekkelijk laag: 45% geeft aan niet veel of weinig kennis hierover te hebben, terwijl 42% aangeeft hier (heel) weinig over te hebben.

Mate van zorgen over de digitale veiligheid van het bedrijf



Mate van kennis over beveiliging tegen cybercrime



Slachtoffers cybercrime

10%

Een op de tien kleine ondernemers is weleens slachtoffer geworden van een bepaalde vorm van cybercrime.

Maakt u zich wel eens zorgen over de digitale veiligheid van uw bedrijf? In welke mate maakt u zich wel of geen zorgen? (n=449)

Als het gaat om het beveiligen van uw bedrijf tegen verschillende vormen van cybercrime. Hoeveel kennis heeft u zelf als ondernemer over dit onderwerp? (n=449)

Als ondernemer kunt u te maken krijgen met cybercrime. Bijvoorbeeld door phishing, een virus of malware. Is uw bedrijf weleens slachtoffer geworden van een bepaalde vorm van cybercrime? (n=449)