Cyberweerbaarheid Onderzoek MKB Brabant 2022

# ‘Cyberweerbaarheid MKB in Brabant nog ver onder de maat’

## Colofon

**Datum**
Oktober 2022

**Uitgave**
ACA IT-Solutions
Beukenlaan 40-50
5651 CD Eindhoven
040-8800100
info@aca-it.nl

**Auteurs**
Geert Rademakers, Directeur
Michael Waterman, Cybersecurity Architect
Remco Wefels, Marketing & Communicatie

**Partners**
Fontys ICT Hogeschool
MKB Eindhoven
Microsoft
Fortinet
Dell Technologies

**Ondersteuning in de realisatie**
Splend

## Managementsamenvatting:

Hoe is het gesteld met de cyberweerbaarheid van MKB-organisaties in de provincie Noord-Brabant? Dat is de centrale vraag in het Cyberweerbaarheids-onderzoek MKB Brabant, georganiseerd door ACA IT-Solutions, met medewerking van netwerkorganisatie MKB Eindhoven en Fontys ICT Hogeschool. Directie, management en IT-(mede)verantwoordelijken van bijna 200 Brabantse organisaties (2-999 FTE) hebben een vragenlijst doorlopen, waarbij zij hun visie op cybersecurity gaven en de wijze waarop dit in hun organisatie is gerealiseerd. Dit onderzoek heeft plaatsgevonden in de periode juni tot en met september 2022.

**Overall conclusie**

De cyberweerbaarheid van het MKB in Brabant is nog ver onder de maat.

Het cybersecuritybeleid is bij het merendeel van de respondenten nog onderbelicht. Dit komt vooral door het ontbreken van betrokkenheid en prioriteit bij de directie. Dit leidt weer tot het ontbreken van adequaat cybersecurity beleid en uitvoering binnen organisaties.

Ook de techniek loopt op te veel vlakken nog achter de feiten aan. Dit komt door een gebrek aan kennis op het gebied van cybersecurity en actueel inzicht in de methodieken van cybercriminelen. Zo is er bijvoorbeeld onvoldoende aandacht voor de technische basisprincipes van cybersecurity, zoals back-up en MFA (multi-factor authenticatie).

Daarnaast wordt de rol van de medewerkers nog te vaak onderbelicht en onderschat. De mens is vaak de zwakste schakel binnen het cybersecurity-spectrum. Er is veel ruimte voor verbetering door de inzet van bijvoorbeeld opleidingen.

Navolgend vermelden wij de belangrijkste resultaten uit het onderzoek, onderverdeeld in de pijlers Beleid, Techniek en Mens.

**Beleid**

- Bij slechts 50,8% van de respondenten staat cybersecurity periodiek op de agenda van de directie. Deze score is zorgwekkend laag, want cyberaanvallen zijn een zeer groot gevaar voor de continuïteit en reputatie van organisaties.
- Wanneer het misgaat, dan beschikt slechts 56,3% van de ondervraagden over procedures omtrent informatiebeveiliging en cyberincidenten. In het geval van calamiteiten is het essentieel om in de eerste uren te kunnen schakelen. Dan wordt namelijk het grootste deel van de schade aangericht, dan wel voorkomen. Het hebben en volgen van de juiste procedures is dan cruciaal.
- Het management is zich onvoldoende bewust van de rechten en bevoegdheden in het ICT-domein. Het is belangrijk dat het management de kaders stelt voor de (IT-)organisatie. Zo weet bijvoorbeeld slechts 39,2% van de respondenten welke rechten/bevoegdheden op ICT-niveau gecombineerd mogen worden om cyberrisico's in te perken.
- Het grootste deel van de respondenten (49,7%) heeft geen cyberverzekering of weet niet of deze is afgesloten (22,1%). Een cyberverzekering is in veel gevallen essentieel om de juiste externe expertise in te vliegen van disaster-recovery specialisten. Het dekt niet alleen de directe schade (zoals losgeld), maar ook tal van andere kostenposten zoals schadevergoeding van de downtime, financiële compensatie van eventuele omzet-derving en schadeherstel van de IT-omgeving.


Beukenlaan 40-50 | 5651 CD Eindhoven
T +31 (0)40 - 8 800 100 | info@aca-it.nl | www.aca-it.nl

**Techniek**

- Patches en updates zijn te vaak onderbelicht. Bij meer dan de helft van de respondenten wordt dit niet adequaat uitgevoerd en/of krijgt het niet de prioriteit die het nodig heeft. Dit is een ware ‘snoepwinkel voor cybercriminelen’ en verdient daarom de hoogste urgentie.
- Back-ups zijn een waar pijnpunt zo blijkt: het positieve nieuws is dat ze worden gebruikt door een meerderheid van de organisaties. Echter, maar liefst 43,7% van de respondenten geeft aan niet te testen op bruikbaarheid en nog eens 30,2% weet dit niet. 28,1% weet niet of de back-ups bestand zijn tegen een cyberaanval.
- De meeste organisaties zijn goed onderweg om MFA/2FA te omarmen. 20,6% van de respondenten werkt echter nog niet met MFA. Dat percentage is hoog, want deze vorm van preventie behoort tegenwoordig tot de basismaatregelen die elke organisatie dient te treffen.

**Mens**

- De controle op inkomende externe e-mails is onder de maat. Maar liefst 72,9% van respondenten kan op linkjes klikken in elke ontvangen e-mail, terwijl dat een veel voorkomende manier is voor cybercriminelen om binnen te komen. Daarnaast is bijna 55% van de ontvangers onvoldoende getraind om malafide mails te herkennen.
- Accounts van medewerkers met hogere rechten worden bij veel respondenten onvoldoende afgeschermd. Bij 40% is dit niet op orde. Wanneer een cybercrimineel toegang weet te krijgen tot een dergelijk account dan is de schade niet te overzien.

**De belangrijkste adviezen in het kort**

Er is dus nog veel ruimte voor verbetering. Hieronder zijn de belangrijkste aanbevelingen naar aanleiding van dit onderzoek op een rijtje gezet, aan de hand van een set basisprincipes:

1. Beleg cybersecurity bij de directie en zet het frequent op de agenda.
2. Maak regelmatig back-ups en test deze, ook op cyberveiligheid.
3. Pas MFA toe op alle systemen en applicaties.
4. Installeer patches en updates, zo snel mogelijk na release.
5. Bepaal wie toegang dient te krijgen tot data en applicaties.
6. Segmenteer netwerken.
7. Zorg voor een calamiteitenplan.

# Inleiding

**Doel van het onderzoek**

Het onderzoeksrapport geeft waardevolle inzichten in de digitale dreiging, weerbaarheid en tot slot de cyberrisico's, waarmee organisaties uit de regio te maken hebben.

Met dit marktonderzoek willen we (MKB-)ondernemers, IT-verantwoordelijken én hun medewerkers bewust maken van de mate van cyberweerbaarheid van het bedrijfsleven. Ofwel:

- Welke facetten spelen een rol bij het realiseren van cyberweerbaarheid en wat is het actuele niveau van bedrijven in de omgeving?
- Hoe goed zijn bedrijven in staat om de vele en gevarieerde aanvallen van cybercriminelen te pareren?

Voor de oplevering van dit marktonderzoek hebben wij bewust gekozen voor de maand oktober, omdat dit de internationale maand van de cybersecurity is: het moment om aandacht te vragen voor dit onderwerp.

**Onderzoeksvraag en verantwoording**

De hoofdvraag van dit marktonderzoek is: hoe is het gesteld met de cyberweerbaarheid van MKB-bedrijven in de provincie Noord-Brabant? Aan dit onderzoek hebben circa 200 organisaties deelgenomen. De respondenten zijn voornamelijk directie, management en IT-(eind)verantwoordelijken. Zij hebben onderzoeksvragen beantwoord binnen de drie pijlers die van belang zijn: beleid, techniek en mens.

**Vervolgstappen**

Aan het einde van het onderzoek hebben deelnemers het aanbod gekregen om deel te nemen aan een additioneel onderzoek, waarin de openbare veiligheidsrisico's van de organisaties worden getoetst middels een zogeheten OSINT-scan. We onderzoeken of en hoe betreffende organisaties op het open, dark- en deepweb zichtbaar zijn voor kwaadwillenden en daardoor een verhoogd risico lopen om aangevallen te worden. Dit onderzoek wordt uitgevoerd door HBO-studenten van Fontys ICT Hogeschool, ondersteund door cybersecurityspecialisten van ACA IT-Solutions. Deze tweede fase van het onderzoek wordt in het najaar van 2022 uitgevoerd.

ACA IT-Solutions en haar partners hebben de ambitie om dit marktonderzoek na twee jaar te herhalen, teneinde een beeld te geven van de voortgang en de verschillen ten opzichte de vorige onderzoeksperiode en de nieuwe ontwikkelingen op het gebied van cybercrime en het effect op het MKB in Noord-Brabant.

**Partners in het onderzoek**

Dit onderzoek is tot stand gekomen en uitgevoerd met behulp van diverse partners die het belang van dit onderzoek onderschrijven:

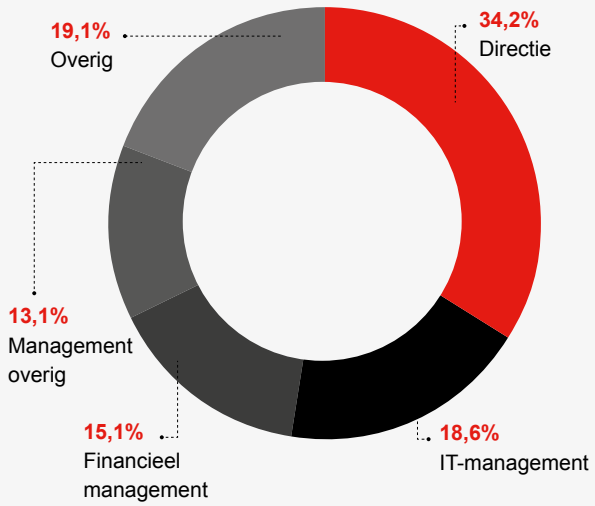
- MKB Eindhoven (brancheorganisatie voor werkgevers in Brabant en als focusgebied Zuidoost-Brabant)
- Fontys ICT Hogeschool. De HBO-studenten van Fontys ICT Hogeschool zijn tevens nauw betrokken bij de vervolgfase van dit marktonderzoek
- IT-partners: Microsoft, Dell Technologies en Fortinet

Op de volgende pagina's van dit rapport zijn de onderzoeksvragen grafisch weergegeven, waarbij ook conclusies zijn toegevoegd van de ervaren cybersecurityspecialisten van ACA IT-Solutions.

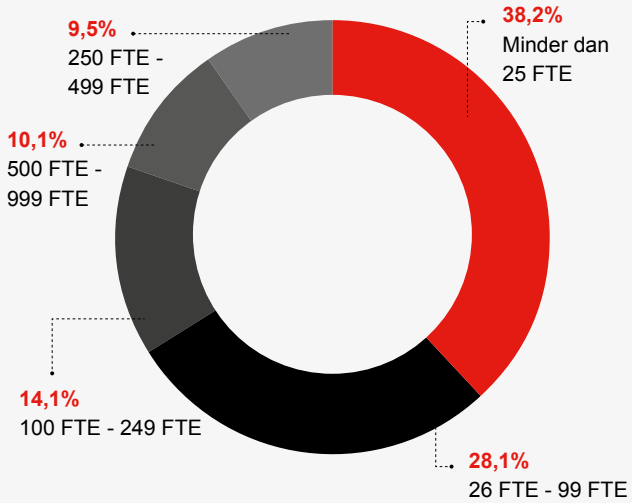

Beukenlaan 40-50 | 5651 CD Eindhoven
T +31 (0)40 - 8 800 100 | info@aca-it.nl | www.aca-it.nl

# Respondenten

## Wat is jouw functie?




## Hoeveel medewerkers (FTE) heeft jouw MKB-bedrijf in dienst?




**Functie:**
De respondenten van dit onderzoek zijn allemaal betrokken bij de IT van hun organisatie. Of dit nu op beleidsniveau is, of uitvoerend. Dit zijn de meest gekozen functies.

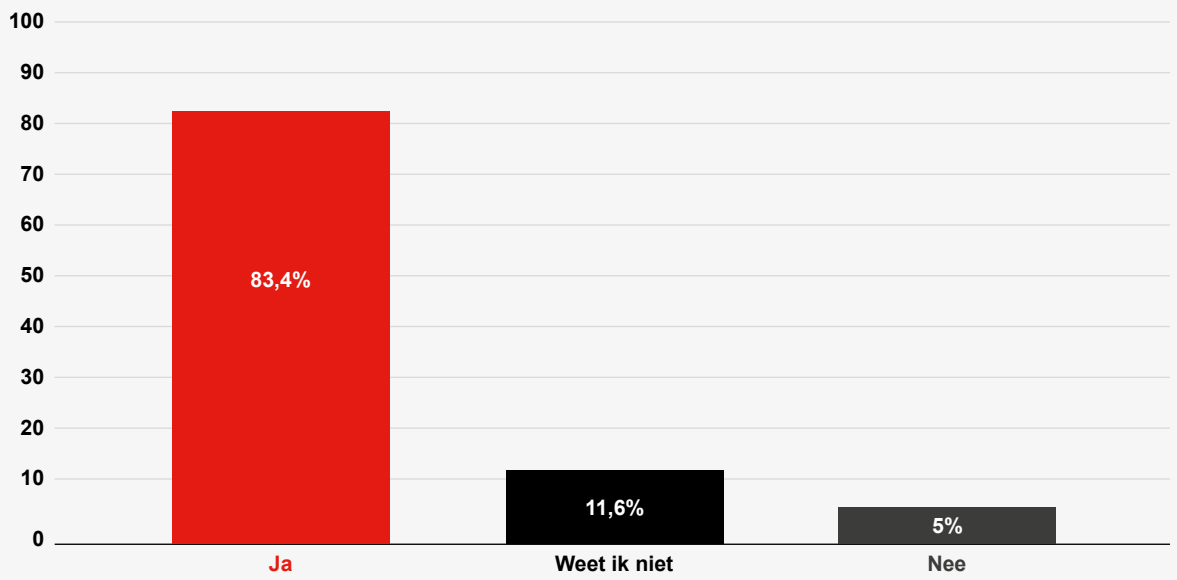
**Typen organisaties:**
Allerlei typen MKB-organisaties uit de provincie Noord-Brabant hebben meegedaan aan dit onderzoek. Van kleine bedrijven (< 25 FTE) tot grote bedrijven (tot 999 FTE). Van handelsbedrijven tot gezondheidszorg en welzijn.

## In welke branche is jouw organisatie actief?

| | |
|---|---|
| 34,2% | Handel en dienstverlening |
| 18,6% | Techniek, productie en bouw |
| 12,1% | ICT |
| 9% | Gezondheidszorg en -welzijn |
| 6% | Transport en logistiek |
| 3,5% | Milieu en agrarische sector |
| 2,5% | Media en communicatie |
| 2% | Onderwijs, cultuur en wetenschap |
| 0,5% | Justitie, veiligheid en openbaar bestuur |
| 0,5% | Toerisme, recreatie en horeca |
| 11,1% | Overig |

# Algemeen

## Ik zie cyberaanvallen als een groot risico voor het bedrijfsleven in Noord-Brabant




**Conclusie:**
We zien dat er een grote groep organisaties bewust is van de risico's op het gebied van cybersecurity, maar dat er ook organisaties zijn die denken dat ze niet of nooit te maken gaan hebben met een cyberincident. Daarom zeggen we bij ACA IT-Solutions dan ook altijd: 'Het is niet de vraag of je ooit te maken gaat hebben met een cybersecurity incident, maar wanneer.'

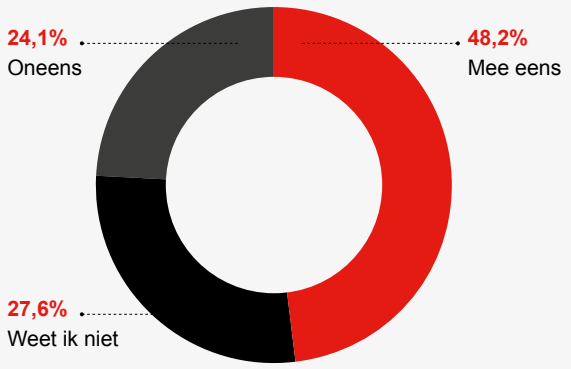
## Ik zie cyberaanvallen als een groot risico voor mijn organisatie (op een schaal van 1 tot 10)


Meest gegeven beoordeling

**Conclusie:**
Gelukkig ziet het overgrote deel van de respondenten een cyberaanval als een groot risico. Feit is dat 2 op de 5 Nederlandse organisaties per jaar geraakt wordt door een vorm van een cyberaanval.

**Bron:** www.digitaltrustcenter.nl/nieuws/aanpak-preventie-cyber-crime-bij-mkb

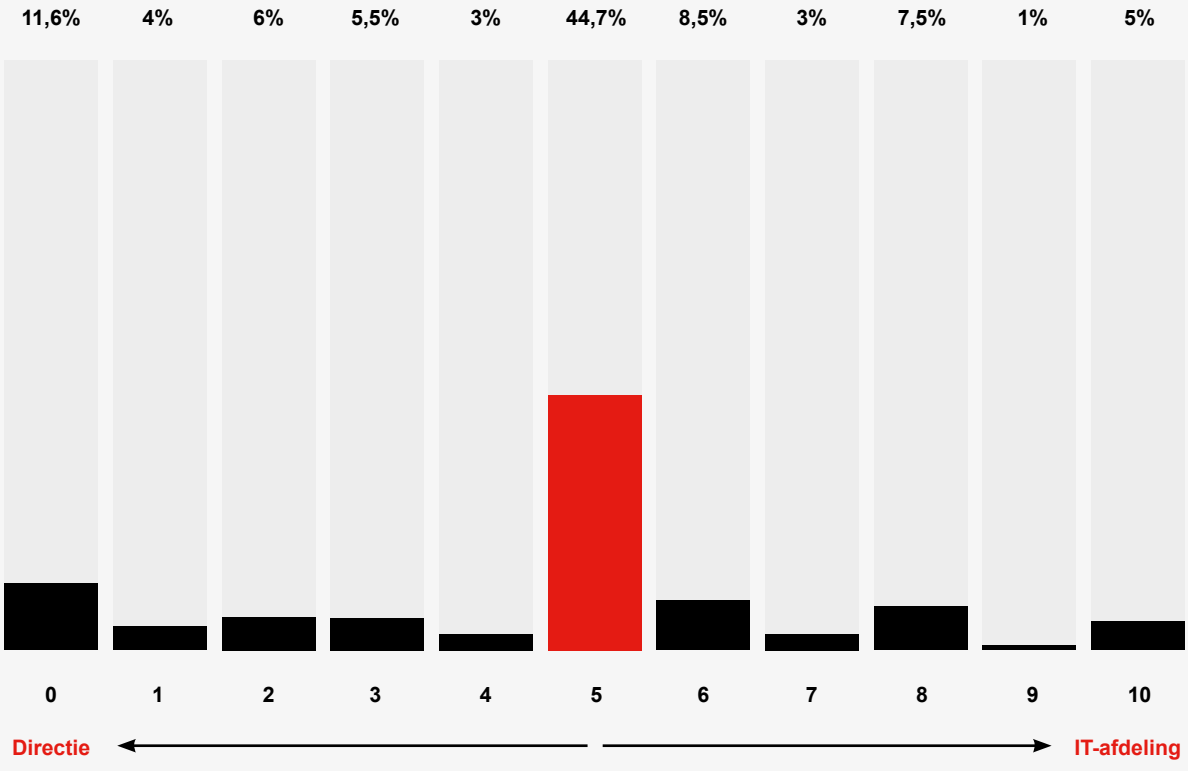
## Ik ben van mening dat mijn organisatie goed voorbereid is op een cyberaanval




**Conclusie:**

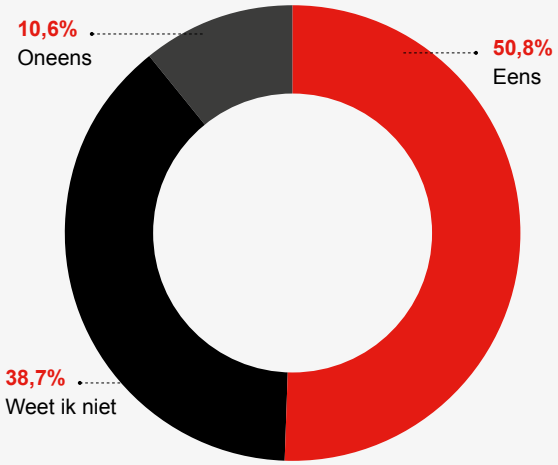
Er is steeds meer bewustwording dat cybersecurity niet alleen op het bordje ligt van IT'ers. En dat is terecht. Wij hebben het onderzoek opgebouwd op basis van de drie pijlers: Beleid, Techniek en Mens. Er moet een beleid inclusief procedures geschreven worden door de directie om uiteindelijk de techniek en de medewerkers optimaal voor te bereiden op eventuele cybersecurity incidenten. Toch zijn nog veel organisaties van mening onvoldoende voorbereid te zijn op een aanval.

## Is een cyberaanval een aangelegenheid van de directie of de IT-afdeling?



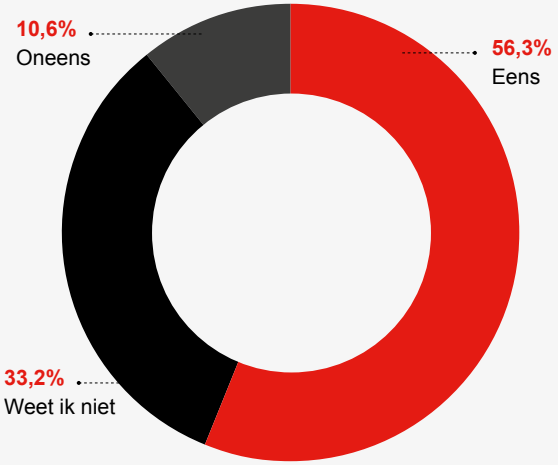
# Beleid

## Staat cybersecurity periodiek op de agenda van de directie?



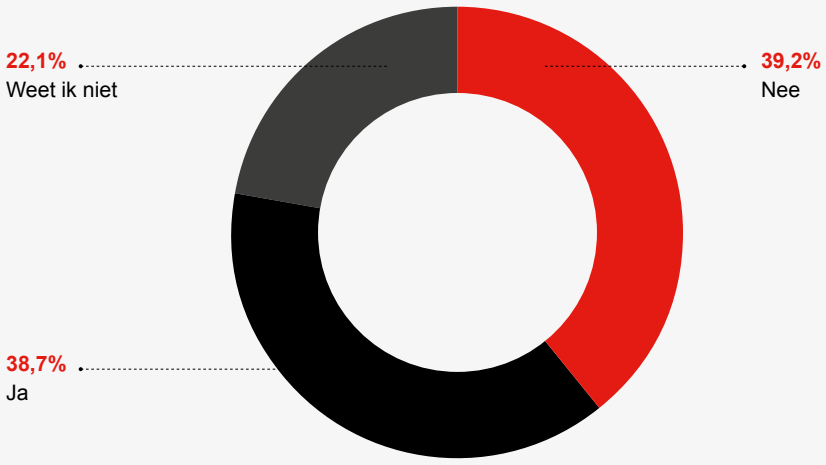

**Conclusie:**
Het is van groot belang dat de directie de koers bepaalt op het vlak van cybersecurity. Dit geeft IT en de individuele medewerker handvatten om op een goede, eenduidige manier met cyberveiligheid om te gaan. Zowel qua procedures, werkwijze als qua tooling.

## Zijn er procedures omtrent informatie-beveiliging en cyberincidenten opgesteld?

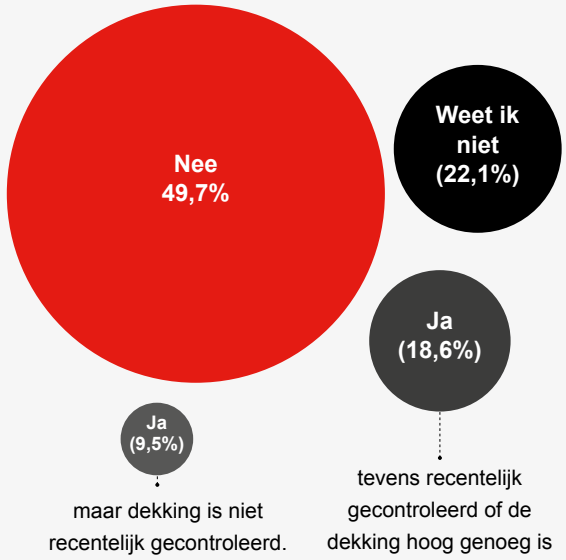



**Conclusie:**
Bij een significant deel van de onderzochte organisaties zijn geen procedures aanwezig. Dat is nodig om zowel preventief als bij een calamiteit adequaat te kunnen handelen.

## Weet het management welke rechten/bevoegdheden op ICT-niveau gecombineerd mogen worden om cyberrisico's in te perken?

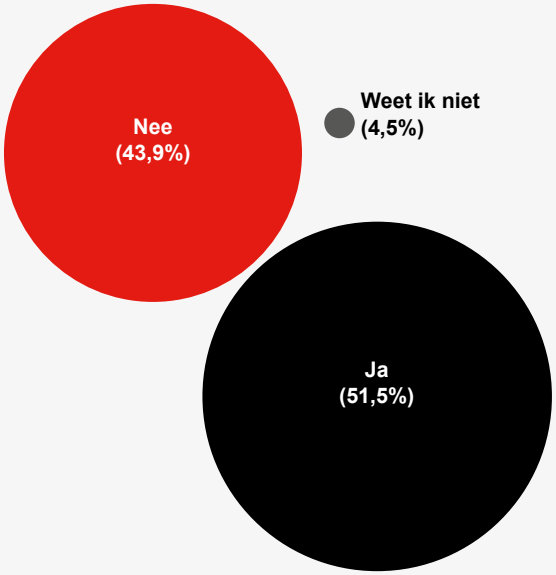


## Heeft jouw organisatie een cyberrisicoverzekering?



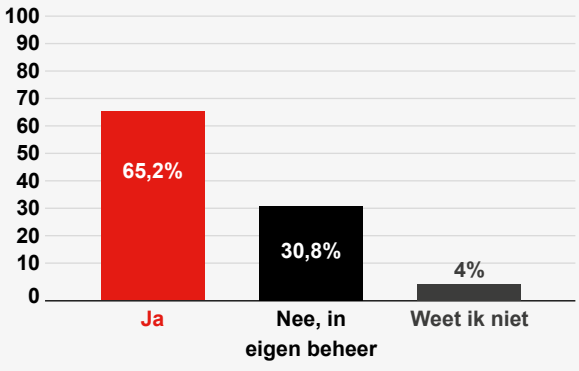

**Conclusie:**
Het is in algemene zin belangrijk om zaken te verzekeren, waarvan de financiële schade niet door de organisatie gedragen kan worden bij een incident. Dat is bij een cyberaanval zeker het geval en een cyberrisicoverzekering afsluiten wordt daarom sterk geadviseerd. Een cyberrisico-verzekering bevat vaak een vergoeding van de downtime, financiële compensatie van eventuele omzetderving en schadeherstel van de IT-omgeving.

## Heeft er wel eens een (cyber)security incident plaatsgevonden in jouw organisatie?



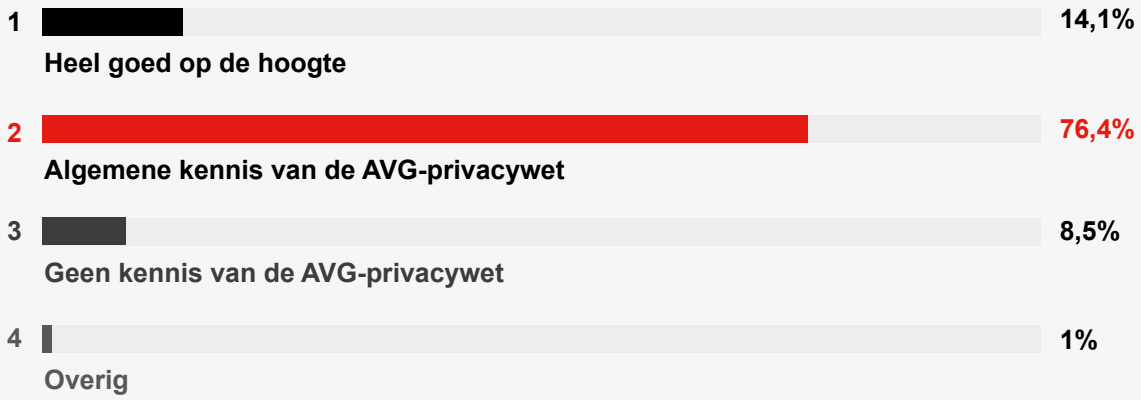

**Conclusie:**
Bij ruim de helft van de respondenten heeft er een cybersecurity incident plaatsgevonden. De cijfers zeggen het al. Cybercriminelen weten ook Noord-Brabant te vinden.

## Wordt cybersecurity door een externe partij beheerd of geadviseerd?




**Conclusie:**
Ongeacht of een organisatie een externe IT-beheerder heeft, is en blijft de organisatie zelf verantwoordelijk voor het beschermen van data en IT-infrastructuur.

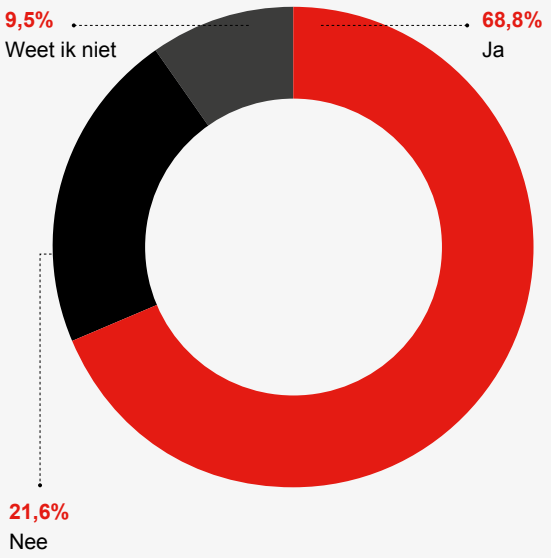
## Onze medewerkers zijn goed op de hoogte van de AVG-privacywet




**Conclusie:**

Compliant zijn aan regelgeving is altijd een samenspel tussen kennis van medewerkers en de technische faciliteiten die een organisatie biedt. Ben je er bijvoorbeeld van op de hoogte dat de AVG sinds haar introductie in 2018, al weer een aantal wijzigingen heeft gehad? Ook het IT-landschap van organisaties is steeds in beweging en dat vraagt ook om continue aandacht voor dataprivacy, databescherming, het voorkomen van datalekken en het niet onnodig lang bewaren van gevoelige data.

## Is er een duidelijke indienst-/ uitdiensttreding en/of functiewijziging procedure en worden hierbij de rechten aan de medewerker herzien?




**Conclusie:**

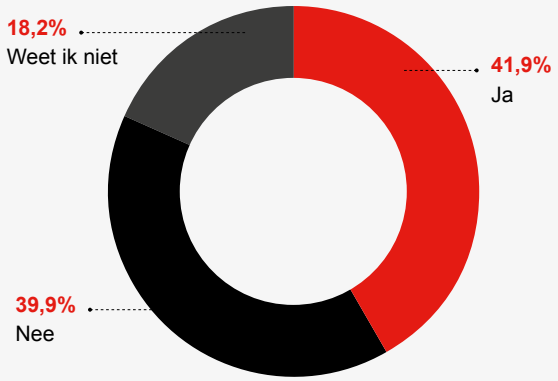
Medewerkers die van positie wijzigen in de organisatie of uit dienst treden zouden altijd een check moeten krijgen of het account nog actief is op vroegere bevoegdheden. Een joiner/leaver procedure biedt uitkomst.

# Techniek

**Kwetsbaarheden door software die niet up-to-date is, zijn een belangrijke reden voor cyberincidenten. Op welke manier vinden updates in jouw organisatie plaats?**


**Denk je dat alle apparaten (hardware en software) in jouw organisatie worden voorzien van updates en patches?**

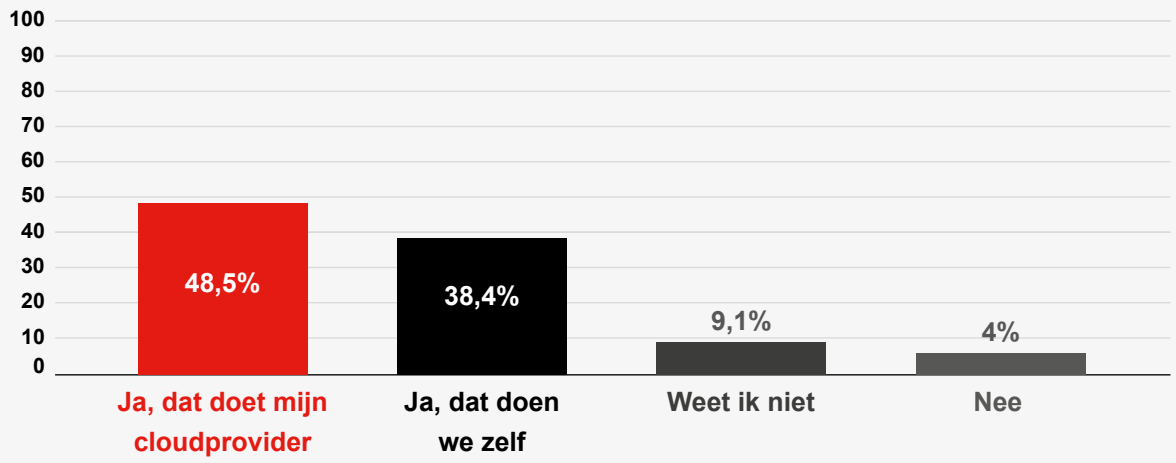
N.B. Denk ook aan IoT apparatuur als TV's, camera's en keukenapparatuur.



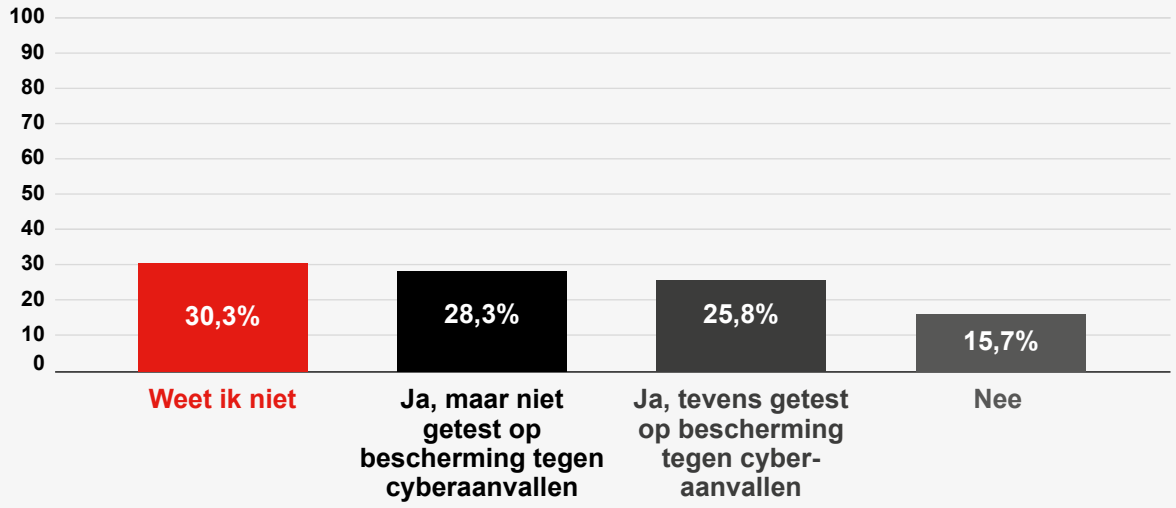

**Conclusie:**

Kwetsbaarheden in software die niet up-to-date is, dat is een belangrijke oorzaak voor cyberincidenten. Wij raden dan ook altijd aan om updates centraal en gecontroleerd te doen. Daarbij voorkomt de organisatie dat de verantwoordelijkheid verschuift naar de eindgebruiker.

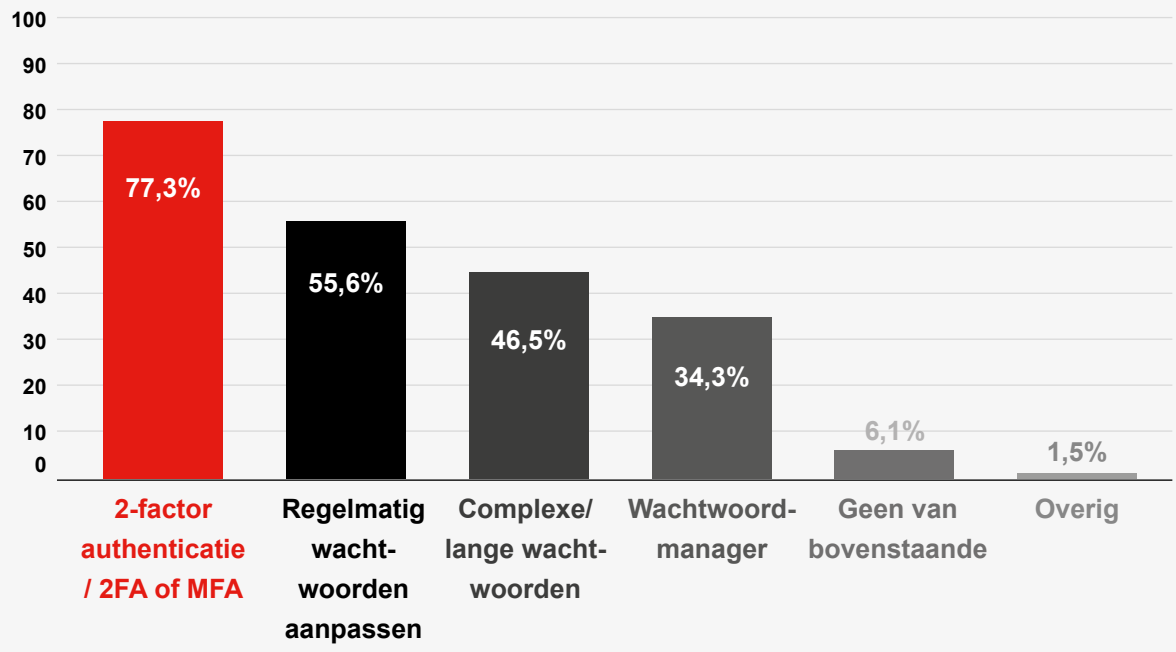
## Worden kritische databases en/of services meegenomen in de dagelijkse back-up?



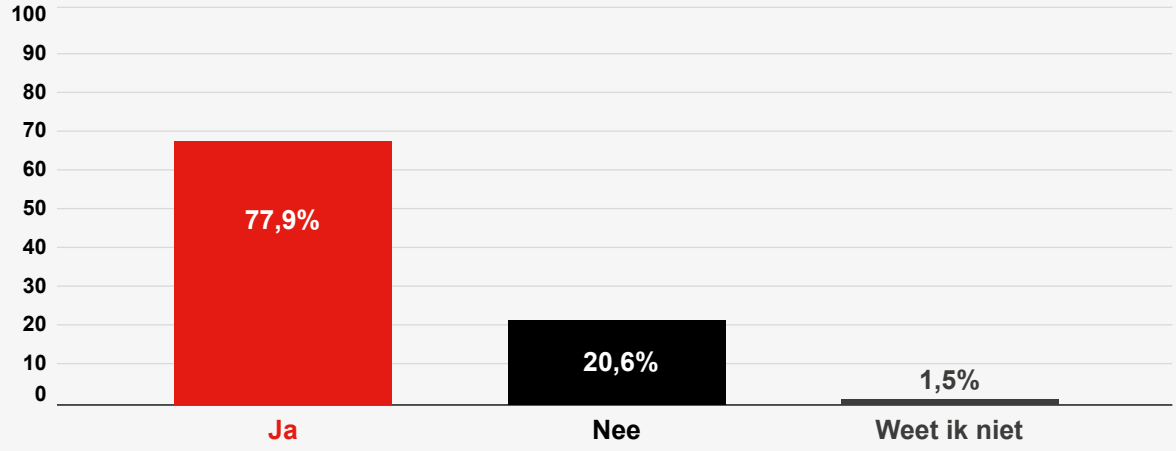

## Worden gemaakte back-ups getest op bruikbaarheid?



## Op welke wijzen zorg je voor veilig inloggen?




## Wordt er bij het inloggen gebruik gemaakt van 2-factor authenticatie (2FA) / Multi-factor authenticatie (MFA)?

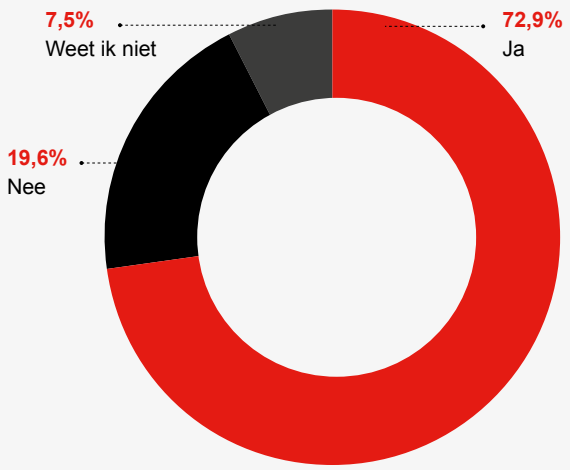



**Conclusie:**

Bijna 25% van de respondenten maakt geen gebruik van multi-factor authenticatie (MFA). Dat terwijl het aantal login misbruikincidenten vermindert met 99% als een organisatie werkt met MFA. MFA behoort daarom tegenwoordig tot de basisbeveiliging van een organisatie. Ons advies: neem ook de inlog van bedrijfskritische applicaties met waardevolle data mee, zoals ERP- en CRM-applicaties.

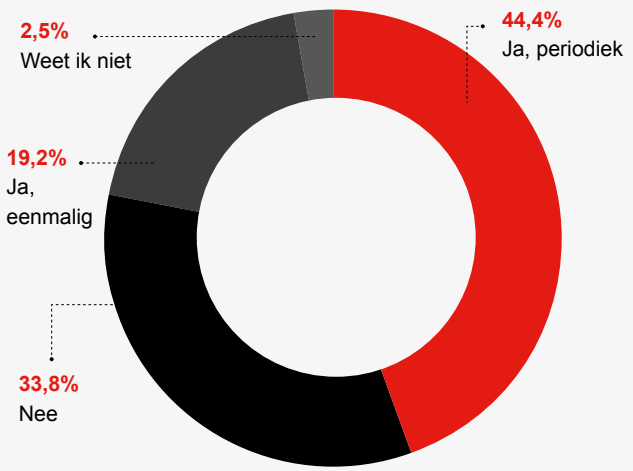
# Mens

**Kan er op elke link in een e-mail worden geklikt, ook als deze van een onbekende zender komt?**



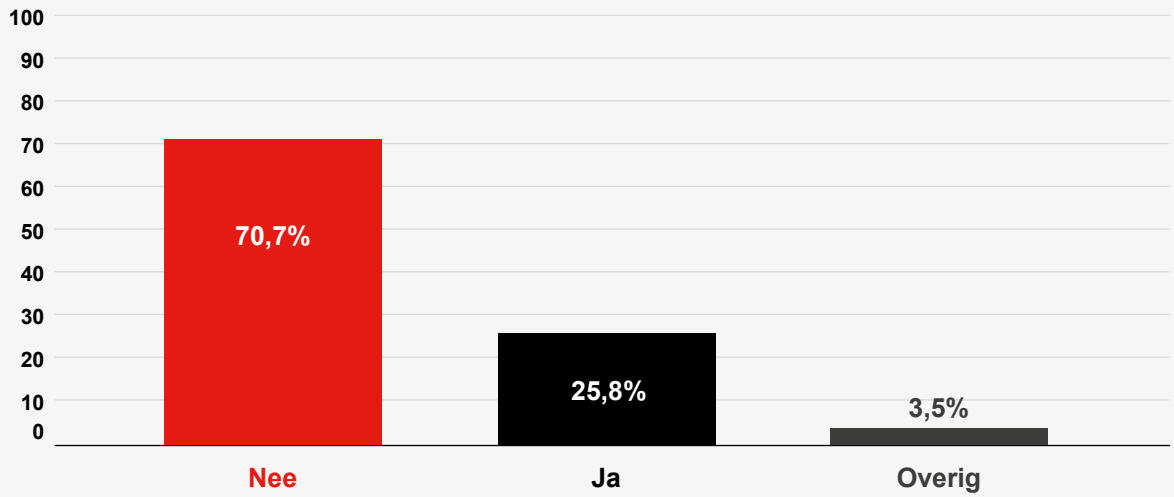

**Conclusie:**
Bij 70% van de organisaties die meededen aan dit onderzoek kan men op alle links klikken in een e-mail. Links die doorverwijzen naar een malafide website zijn oorzaak #1 voor het achterhalen van inloggegevens.

**Worden medewerkers van jouw organisatie getraind om phishing- en ransomware berichten te herkennen?**




**Conclusie:**
Veel organisaties zijn goed onderweg, maar er is nog wel veel winst te behalen. Eenmalig trainen snijdt geen hout. De medewerker is een belangrijke schakel in het geheel. Periodiek trainen zorgt voor top-of-mind bewustzijn. Bovendien worden ze dan ook getraind om nieuwe aanvalsvormen te herkennen en weten alle medewerkers (ook nieuwe) hoe te handelen.

## Kan iedereen jouw bedrijfspand betreden zonder controle?

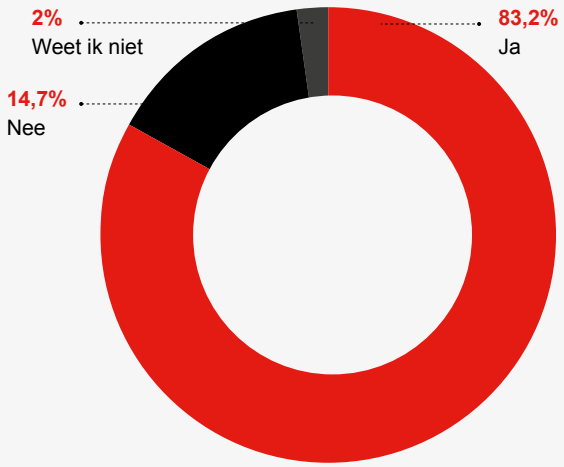



## Wie heeft er toegang tot de serverruimte van jouw organisatie?

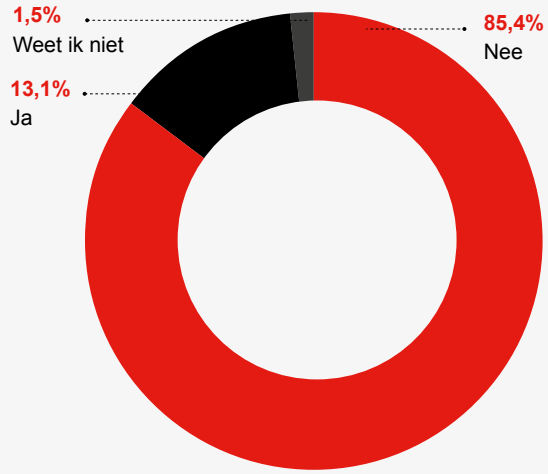

**Conclusie:**

Niet alleen digitale beveiliging is belangrijk. Bij 25,8% van de respondenten kunnen ongewenste gasten naar binnen lopen. Ondanks dat veel organisaties alleen bevoegden binnen laten in de serverruimte is ook algehele fysieke beveiliging een belangrijk punt om cybersecurity te bewaken. Ook kan hiermee (onbedoelde) schade aan de serverruimte en/of de gehele organisatie worden voorkomen.

## Heeft elke medewerker een persoonlijk account (dus niet alleen een groeps-account zoals receptie of magazijn)?

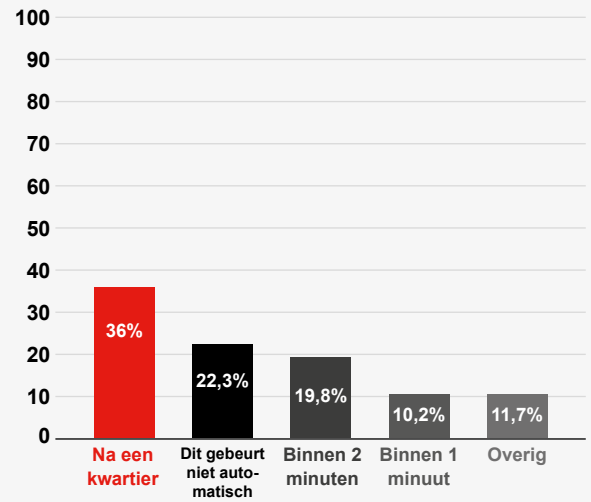



## Mogen wachtwoorden tussen medewerkers gedeeld worden?



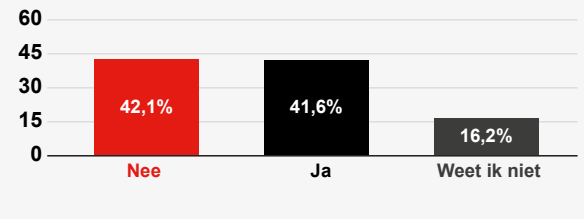

**Conclusie:**
Bij ruim 85% van de respondenten is er een beleid dat er geen wachtwoorden mogen worden gedeeld. Anno 2022 is het ook uit den boze om wachtwoorden onderling te delen.

## Na hoeveel minuten wordt jouw scherm, op kantoor of tijdens het thuiswerken, vergrendeld?




**Conclusie:**
Iedere medewerker zou moeten aanleren zijn of haar device te vergrendelen als de werkplek wordt verlaten. Het advies is om hier streng op toe te zien en elkaar hierop aan te spreken.

## Zijn accounts van medewerkers met hogere rechten afgeschermd door middel van aanvullende maatregelen?




**Conclusie:**
Bij ruim 40% van de respondenten is de organisatie nog onvolwassen in het beheer van accounts met meer rechten. Deze accounts hebben vaak toegang tot bedrijfskritische applicaties en data en hebben daarom meerdere verdedigingslagen nodig.

## Over ACA IT-Solutions

ACA IT-Solutions is gespecialiseerd in dienstverlening en advisering op het gebied van IT en cybersecurity. Daarbij hechten wij veel waarde aan de kracht van samenwerking. Wij staan namelijk graag aan de zijde van de ondernemer om samen te kijken naar de best passende oplossing voor de organisatie en die is steeds anders: anders ten opzichte van andere organisaties en anders in de loop der tijd.

ACA IT-Solutions is, met ruim 30 jaar ervaring, een betrouwbare IT-partner voor veel verschillende typen organisaties voor het MKB, grootbedrijf en instanties. De werkzaamheden bestaan o.a. uit het leveren van advies, ontwerp, installatie, ondersteuning, beheer en trainingen op ICT-gebied. Meer informatie: **aca-it.nl**

### Cyber-assessment

In de vraagstelling en onderzoeksaanpak van dit marktonderzoek en de hierop volgende OSINT-scan komen elementen terug uit de cybersecurity assessments die ACA IT-Solutions uitvoert voor opdrachtgevers. Meer informatie over deze assessments en onze werkwijze is terug te vinden op **aca-it.nl/scan**

### Vragen of contact

Voor vragen over de onderzoeksopzet, de resultaten en/of advies over dit marktonderzoek kan contact opgenomen worden met:

ACA IT-Solutions
Beukenlaan 40-50
5651 CD Eindhoven
040-8800100
**info@aca-it.nl**