

# Toepassing van internetstandaarden voor websites van bedrijven

Een statistische analyse van Internet.nl-scores

2026





Centraal Bureau  
voor de Statistiek

**adres** CBS Den Haag  
Henri Faasdreef 312  
2492 JP Den Haag  
Postbus 24500  
2490 HA Den Haag  
T +31 70 337 38 00

**datum** 29-4-2026

# Inhoudsopgave

<b>Over deze publicatie</b>	<b>5</b>
<b>1. Inleiding</b>	<b>6</b>
<b>2. Methodebeschrijving</b>	<b>7</b>
2.1. Enquête 'ICT-gebruik bij bedrijven'	7
2.2. Internet.nl-scans	7
2.2.1. Type scans	7
2.2.2. Scandata	8
2.3. Populatie en berekening uitkomsten	8
2.4. Percentage bedrijven met een website en hun domeinextensies	9
2.4.1. Bedrijven met een website	9
2.4.2. Verdeling websites over de verschillende domeinextensies	10
<b>3. Resultaten websitescans</b>	<b>12</b>
3.1. Resultaten eindscores van de websitescan	12
3.2. Resultaten websitescan per categorie	14
3.2.1. Categorie IPv6	15
3.2.2. Categorie DNSSEC	17
3.2.3. Categorie HTTPS	19
3.2.4. Categorie Beveiligingsopties	22
3.2.5. Categorie Autorisatie voor Routing (RPKI)	24
3.3. Verdelingen van de eindscores van de websitescans	26
3.4. Welke bedrijven hebben de hoogste en laagste eindscore voor de websitescan?	27
<b>4. Resultaten e-mailscans</b>	<b>34</b>
4.1. Resultaten eindscores van de e-mailscan	34
4.2. Resultaten e-mailscan per categorie	36
4.2.1. Categorie IPv6	37
4.2.2. Categorie DNSSEC	39
4.2.3. Categorie Authenticiteit	41
4.2.4. Categorie Beveiligd e-mailtransport (STARTTLS en DANE)	44
4.2.5. Categorie Autorisatie voor Routing (RPKI)	46
4.3. Verdelingen van de eindscores van de e-mailscan	48
4.4. Welke bedrijven hebben de hoogste en laagste eindscore voor de e-mailscan?	49
<b>5. Conclusie</b>	<b>56</b>
<b>Referenties</b>	<b>57</b>
<b>Bijlagen</b>	<b>58</b>
<b>A. Indelingen en gebruikte termen</b>	<b>58</b>
A.1. Overzicht indelingen	58
A.2. Overzicht subtesten websitecan	59

A.3. Overzicht subtesten e-mailscan . . . . .	62
A.4. Overzicht termen . . . . .	66
<b>B. Alle websitescanuitslagen</b>	<b>67</b>
B.1. Eindscore en categoriescores voor alle jaren . . . . .	67
B.2. Websitescanuitslagen voor categorie IPv6 . . . . .	79
B.3. Websitescanuitslagen voor categorie DNSSEC . . . . .	89
B.4. Websitescanuitslagen voor categorie HTTPS . . . . .	93
B.5. Websitescanuitslagen voor categorie Beveiligingsopties . . . . .	134
B.6. Websitescanuitslagen voor categorie RPKI . . . . .	144
B.7. Verdeling eindscores websitescan . . . . .	152
<b>C. Alle e-mailscanuitslagen</b>	<b>155</b>
C.1. E-mailscanuitslagen voor categorie IPv6 . . . . .	155
C.2. E-mailscanuitslagen voor categorie DNSSEC . . . . .	163
C.3. E-mailscanuitslagen voor categorie Authenticiteit . . . . .	171
C.4. E-mailscanuitslagen voor categorie Beveiligd e-mailtransport (STARTTLS en DANE) . . . . .	181
C.5. E-mailscanuitslagen voor categorie RPKI . . . . .	216
C.6. Verdeling eindscores e-mailscan . . . . .	228

## Over deze publicatie

In 2020 is het CBS op verzoek van het ministerie van Economische Zaken samen met Platform Internetstandaarden een onderzoek begonnen naar het gebruik van internetstandaarden bij websites van bedrijven in Nederland.

Het doel van dit onderzoek is om in kaart te brengen in welke mate bedrijven (veilige) internetstandaarden voor hun website gebruiken. In dit rapport worden de resultaten van 2026 gepresenteerd.

# 1. Inleiding

In 2020 is het CBS op verzoek van het ministerie van Economische Zaken samen met Platform Internetstandaarden een onderzoek begonnen naar het gebruik van internetstandaarden op websites van bedrijven in Nederland. Het doel van dit onderzoek is om in kaart te brengen in welke mate bedrijven (veilige) internetstandaarden gebruiken per bedrijfsgrootteklasse en bedrijfstak.

Het toepassen van internetstandaarden verhoogt de veiligheid, betrouwbaarheid en toegankelijkheid van het internet. In dit onderzoek wordt de testtool [Internet.nl](#) van Platform Internetstandaarden gebruikt om websites en e-mailserver van bedrijven te toetsen. Met deze tool kan een website of e-mailserver getoetst worden op bijna veertig internetstandaarden. Op basis van deze testen wordt door Internet.nl een eindscore toegekend als percentage tussen 0 en 100 procent. Een website of e-mailserver met een eindscore van 100 procent voldoet aan alle eisen om de desbetreffende dienst veilig, betrouwbaar en toegankelijk te maken.

De websites die in dit onderzoek gescand worden, komen uit de CBS-enquête 'ICT-gebruik bij bedrijven' [[CBS, 2025b](#)]<sup>1</sup>. In deze enquête wordt gevraagd of een bedrijf een eigen website heeft, en zo ja, wat de domeinnaam is met de meeste bezoekers. De testtool Internet.nl wordt vervolgens gebruikt om zowel een website- als een e-mailscan uit te voeren op de opgegeven domeinnamen. Doordat de websites via een representatieve steekproef verkregen zijn, kan per bedrijfsgrootteklasse en bedrijfstak bepaald worden in welke mate veilige internetstandaarden worden toegepast op de websites en e-mailserver van bedrijven.

De resultaten van eerdere scans zijn gepubliceerd in vier eerdere longreads [[CBS, 2022b, 2023b, 2024b, 2025c](#)]. In het rapport dat nu verschijnt, zijn nieuwe website- en e-mailscanresultaten toegevoegd. Deze scans zijn uitgevoerd in januari 2026 op websites verkregen uit de ICT-enquête van 2025. Een overzicht van alle scandata wordt gegeven in Tabel 2.1. Merk op dat de cijfers in dit rapport (licht) kunnen verschillen van de cijfers in eerdere publicaties. Dit komt doordat de analysemethode met terugwerkende kracht is verbeterd vanaf 2020. In Bijlage B en Bijlage C zijn de verbeterde cijfers voor alle jaren verzameld<sup>2</sup>. Ook is de titel van het rapport licht aangepast. Hoewel in het rapport van vorig jaar scanresultaten uit 2025 zijn gepresenteerd, was de naam 'Toepassing van internetstandaarden voor websites van bedrijven, 2024' gebruikt. Omdat het huidige rapport scanresultaten voor 2026 bevat, is ervoor gekozen om het jaartal '2026' in de titel te gebruiken. Het rapport met het jaartal '2025' in de titel bestaat hierdoor niet.

Het rapport is als volgt opgebouwd. In Hoofdstuk 2 wordt de methode beschreven die gebruikt is om de scans uit te voeren en te analyseren. De resultaten van de websitescans en e-mailscans worden achtereenvolgens in Hoofdstuk 3 en Hoofdstuk 4 besproken. In Hoofdstuk 5 worden de conclusies van dit onderzoek gegeven. Een overzicht van de gebruikte indelingen en een uitleg van de gebruikte termen is te vinden in Bijlage A. De resultaten van alle onderliggende website- en e-mailtesten zijn te vinden in Bijlage B en Bijlage C.

<sup>1</sup>Zie ook [[CBS, 2020, 2021, 2022a, 2023a, 2024a](#)].

<sup>2</sup>Om de verbeterde cijfers voor alle jaargangen van de websitescan te bekijken, kan bij elk figuur in Bijlage B op de knop 'Toon data' worden geklikt.

## 2. Methodebeschrijving

### 2.1. Enquête 'ICT-gebruik bij bedrijven'

De gebruikte domeinnamen komen uit het CBS-onderzoek 'ICT-gebruik bij bedrijven' (oftewel, de ICT-enquête). In de ICT-enquête onderzoekt het CBS het gebruik van informatie- en communicatietechnologie (ICT) bij bedrijven in Nederland [CBS, 2026]. De ICT enquête wordt jaarlijks gehouden onder een steekproef van ongeveer 50 000 Nederlandse bedrijven uit de bedrijfstakken C-N en Q volgens de Standaard Bedrijfsindeling 2008 (SBI 2008) (zie Tabel A.1 en Tabel A.2). De resultaten worden gepubliceerd op [Statline](#).

In de ICT-enquête wordt gevraagd of een bedrijf een website heeft. Aan bedrijven die aangeven een website te hebben, wordt in de ICT-enquête om de URL (Uniform Resource Locator, oftewel de domeinnaam) van de website gevraagd. Als een bedrijf meerdere websites heeft, wordt de URL van de website met de meeste bezoekers gevraagd (de hoofdwebsite). De websites die op deze manier verkregen zijn, worden gescand met de testtool [Internet.nl](#) van Platform Internetstandaarden.

### 2.2. Internet.nl-scans

#### 2.2.1. Type scans

Met de testtool Internet.nl worden twee typen scans uitgevoerd: een scan naar het gebruik van internetstandaarden op de website (de 'websitescan') en de bijbehorende e-mailserver (de 'e-mailscan')<sup>1</sup> van een bedrijf.

De testen van de websitescan zijn onder te verdelen in vijf categorieën (zie Paragraaf 3.2):

- **IPv6**: Bereikbaarheid via een modern internetadres;
- **DNSSEC**: Gebruik van een ondertekende domeinnaam;
- **HTTPS**: Gebruik van een beveiligde verbinding;
- **Beveiligingsopties**: Gebruik van ingestelde applicatie-beveiligingsopties;
- **RPKI**: Autorisatie voor routing.

De testen van de e-mailscan zijn ook op te delen in vijf categorieën (zie Paragraaf 4.2):

- **IPv6**: Bereikbaarheid via een modern internetadres;
- **DNSSEC**: Gebruik van een ondertekende domeinnaam;
- **Authenticiteit**: Authenticatie als protectie tegen phishing via e-mail;
- **Beveiligd e-mailtransport (STARTTLS en DANE)**: Beveiligde e-mailserververbinding;
- **RPKI**: Autorisatie voor routing.

---

<sup>1</sup>Er wordt aangenomen dat het bedrijf hetzelfde e-maildomein gebruikt als het opgegeven websitedomein uit de ICT-enquête.

Elke categorie bestaat uit een aantal subtesten. Deze subtesten worden in dit rapport beschouwd als geslaagd als ze door Internet.nl met 'passed' of 'good' worden aangeduid. Op basis van de onderliggende subtesten bepaalt Internet.nl of een bedrijf slaagt voor de gehele categorie of niet. Paragraaf A.2 en Paragraaf A.3 bevat per categorie een overzicht van alle subtesten. Omdat niet alle getoonde subtesten meewegen in de beslissing of een bedrijf slaagt voor de gehele categorie, wordt hierin ook vermeld wanneer een subtest verplicht is en wanneer niet. Een verplichte subtest telt mee voor de gehele categorie; een niet-verplichte subtest niet. Door Internet.nl wordt tot slot op basis van alle verplichte subtesten per domeinnaam een eindscore tussen de 0 en 100 procent berekend. Een website of e-mailserver met een eindscore van 100 procent voldoet aan alle eisen om de desbetreffende dienst veilig, betrouwbaar en toegankelijk te maken.

## 2.2.2. Scandata

Dit rapport bevat scans die zijn uitgevoerd van 2020 t/m 2026 (zie Tabel 2.1). De scan van 2020 is uitgevoerd op de URL's die in hetzelfde jaar van de ICT-enquête zijn verkregen. De overige scans zijn uitgevoerd op de URL's uit de ICT-enquête van een jaar eerder.

Tabel 2.1.: Details van de Internet.nl-scans

Label	Scandatum	Enquêtejaar	Websitescan	E-mailscan
2020	2020-10-22	2020	Ja	Nee
2021	2022-03-31	2021	Ja	Nee
2022	2022-12-24	2022	Ja	Nee
2023	2023-04-03	2022	Ja	Ja
2024	2024-04-03	2023	Ja	Ja
2025	2025-01-20	2024	Ja	Ja
2026	2026-01-15	2025	Ja	Ja

## 2.3. Populatie en berekening uitkomsten

De populatie in dit rapport bestaat uit alle bedrijven met een website in de bedrijfstakken C-N en Q volgens de Standaard Bedrijfsindeling 2008 (SBI 2008) (zie Tabel A.1). Doordat de websites via een statistisch representatieve steekproef verkregen zijn, kunnen uitkomsten per bedrijfsgrootteklasse en bedrijfstak voor de hele populatie worden berekend. Hiertoe zijn de scanresultaten in dit rapport opgehoogd met de weegfactoren uit de ICT-enquête [CBS, 2026]. Merk op dat in dit rapport ook uitkomsten voor de ICT-sector worden gepresenteerd. Dit is een samentelling van verschillende bedrijfstakken (zie Tabel A.2).

In sommige gevallen heeft een bedrijf aangegeven wel een website te hebben, maar is de opgegeven domeinnaam niet bruikbaar, omdat het niet verwijst naar een bestaande website. In 2026 is dit voor ongeveer 10 procent van de bedrijven met een website het geval. Voor deze bedrijven is gebruikgemaakt van donorimputatie, waarbij de resultaten zijn overgenomen van een vergelijkbaar bedrijf uit dezelfde bedrijfstak en bedrijfsgrootteklasse [Israëls et al., 2011].

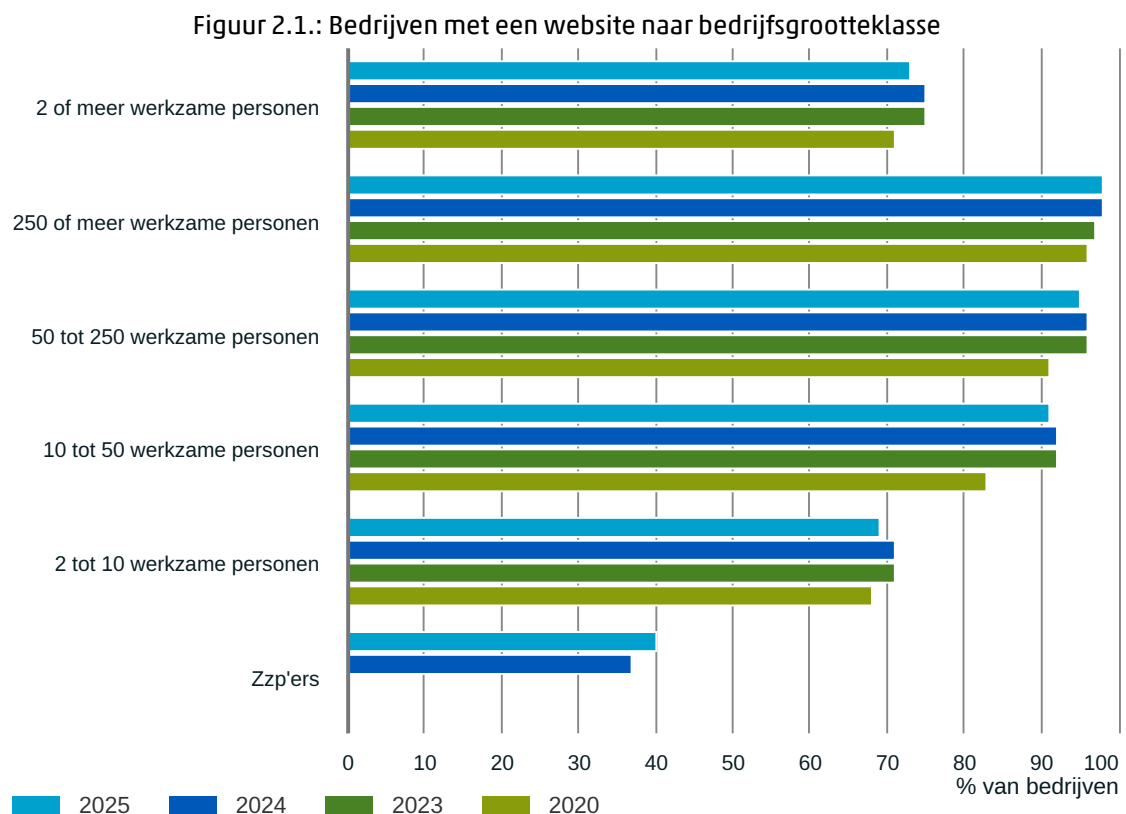
Sinds 2023 worden in dit onderzoek ook zzp'ers (zelfstandigen zonder personeel) meegenomen. Een zzp'er is gedefinieerd als een persoon die voor eigen rekening of risico arbeid verricht in een eigen bedrijf of praktijk (zelfstandig ondernemer) en geen personeel in dienst heeft. Voor 2024 is er geen data beschikbaar voor zzp'ers. Dit komt doordat de websitegerelateerde vragen in de ICT-enquête van 2023 niet aan zzp'ers zijn gesteld. Bij de verdelingen over de bedrijfstakken is er

dan ook voor gekozen om de zzp'ers niet mee te nemen. De getoonde resultaten naar bedrijfstak hebben daarom alleen betrekking op bedrijven met 2 of meer werkzame personen.

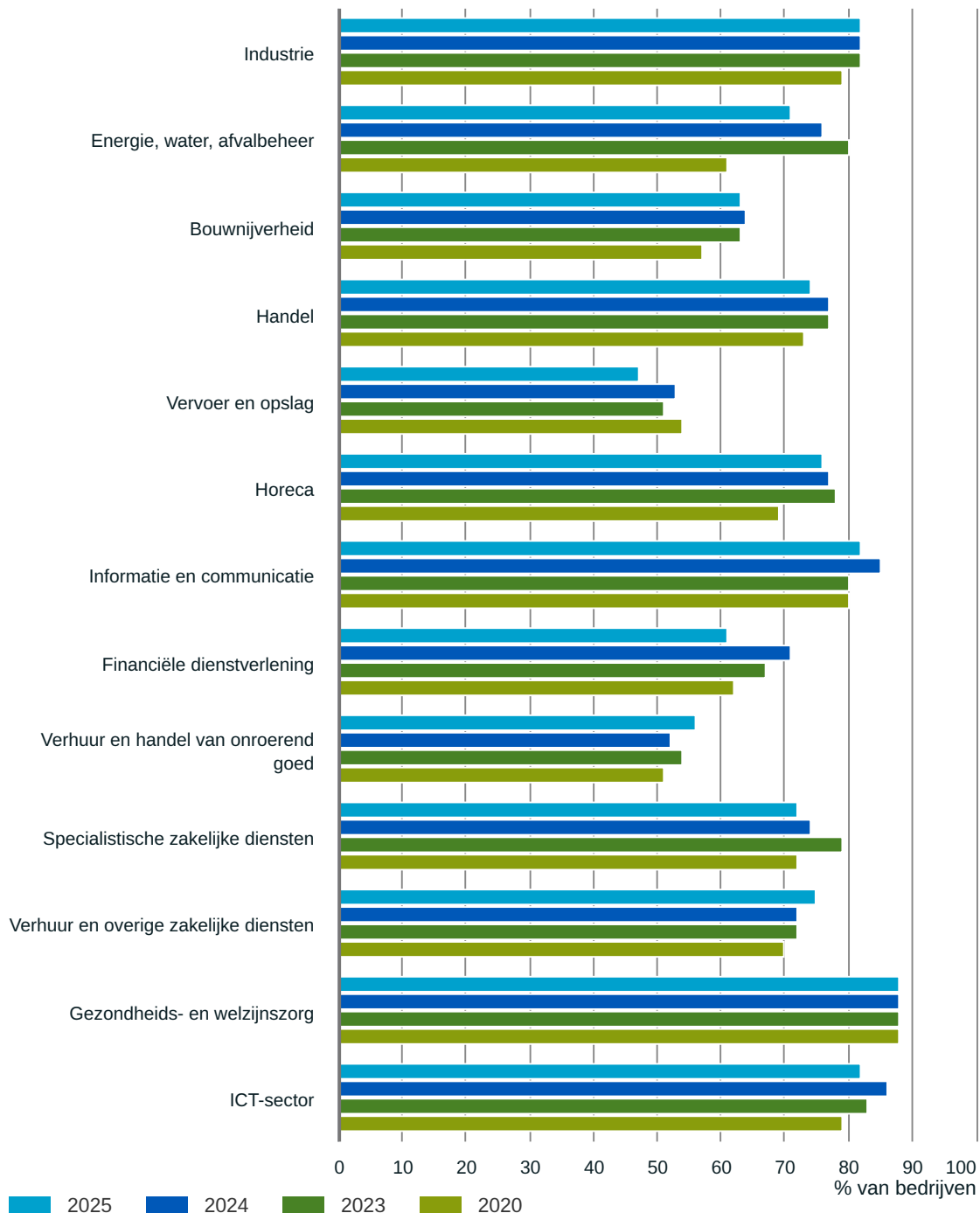
## 2.4. Percentage bedrijven met een website en hun domeinextensies

### 2.4.1. Bedrijven met een website

De resultaten van de ICT-enquête laten zien dat 73 procent van de bedrijven (2 of meer werkzame personen) in 2025 aangeeft een website te hebben (zie Figuur 2.1) [CBS, 2025b]. Dit is een kleine daling van 2 procentpunt ten opzichte van het jaar daarvoor. Grote bedrijven geven vaker aan een eigen website te hebben dan kleine bedrijven. Van de grote bedrijven (250 of meer werkzame personen) heeft 98 procent in 2025 een website, tegenover 69 procent van de kleine bedrijven (2 tot 10 werkzame personen). Figuur 2.2 laat zien dat bedrijven in de bedrijfstak 'Gezondheids- en welzijnszorg' in 2025 het vaakst een website hebben (88 procent). In de bedrijfstak 'Vervoer en opslag' hebben bedrijven juist het minst vaak een website (47 procent).



Figuur 2.2.: Bedrijven met een website naar bedrijfstak (2 of meer werkzame personen)



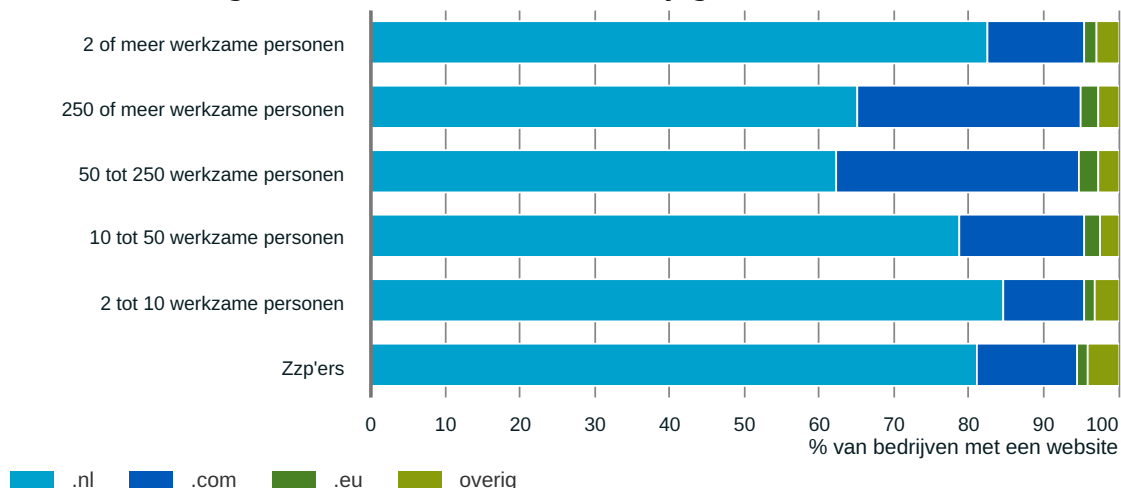
### 2.4.2. Verdeling websites over de verschillende domeinextensies

In Figuur 2.3 en Figuur 2.4 wordt per bedrijfsgrootteklasse en bedrijfstak de verdeling van de domeinextensies van de (hoofd)websites van bedrijven getoond over de meeste voorkomende extensies. De verdeling per bedrijfsgrootteklasse in Figuur 2.3 toont aan dat .nl de meest voorkomende domeinextensie is: 82,6 procent van de bedrijven met een website (2 of meer werkzame personen) heeft in 2025 .nl als domeinextensie van de hoofdwebsite. Waar .nl daarnaast vaker voorkomt bij kleinere bedrijven, is te zien dat .com vaker voorkomt bij grotere bedrijven. De domeinextensie .eu heeft tot slot nog een klein aandeel. Naast deze

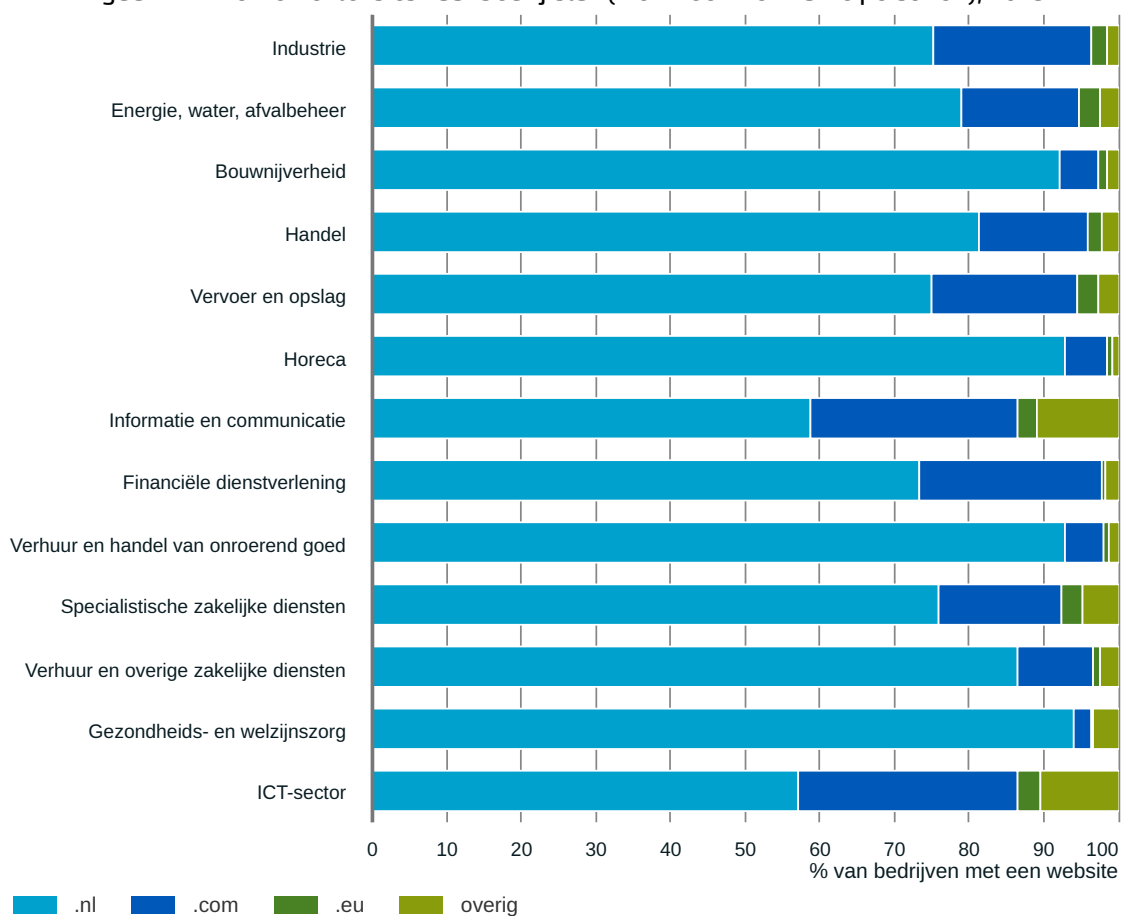
domeinextensies zijn er nog meer dan 100 verschillende domeinextensies die bij elkaar niet meer dan 3 procent van het totaal uitmaken. Deze worden met de categorie 'overig' aangeduid.

Figuur 2.4 toont de verdeling van de domeinnaamextensies per bedrijfstak (2 of meer werkzame personen). Het gebruik van de domeinextensie .nl varieert in 2025 in de meeste bedrijfstakken tussen de 57,2 en 94,2 procent. De bedrijfstak 'Gezondheids- en welzijnszorg' gebruikt .nl het vaakst (94,2 procent), de ICT-sector juist het minst vaak (57,2 procent).

Figuur 2.3.: Domeinextensies naar bedrijfsgrootteklasse, 2025



Figuur 2.4.: Domeinextensies naar bedrijfstak (2 of meer werkzame personen), 2025



## 3. Resultaten websitescans

Met de websitescan van Internet.nl wordt getest of websites van bedrijven aan moderne internetstandaarden voldoen. In dit hoofdstuk worden de resultaten van de websitescan besproken om zo per bedrijfsgroottesklasse en bedrijfstak in kaart te brengen welk percentage bedrijven de juiste internetstandaarden toepast. De resultaten van de e-mailscan worden in het volgende hoofdstuk besproken.

De websitescan van Internet.nl bevat vijf categorieën:

- **IPv6**: Bereikbaarheid via een modern internetadres;
- **DNSSEC**: Gebruik van een ondertekende domeinnaam;
- **HTTPS**: Gebruik van een beveiligde verbinding;
- **Beveiligingsopties**: Gebruik van ingestelde applicatie-beveiligingsopties;
- **RPKI**: Autorisatie voor routing.<sup>1</sup>

In Paragraaf 3.1 wordt eerst gekeken naar de gemiddelde eindscores.<sup>2</sup> In Paragraaf 3.2 worden de categorieën daarna in meer detail beschreven en wordt er los ingezoomd op de resultaten per categorie. Paragraaf 3.3 en Paragraaf 3.4 tonen resultaten over de verdelingen van de eindscores. Paragraaf A.2 bevat een overzicht van alle subtesten per categorie met een korte uitleg en Tabel A.13 bevat een lijst met technische termen. De resultaten van alle onderliggende testen worden getoond in Bijlage B. In Bijlage B worden tevens de resultaten voor alle voorgaande jaren getoond.

### 3.1. Resultaten eindscores van de websitescan

In Figuur 3.1 en Figuur 3.2 worden per bedrijfsgroottesklasse en bedrijfstak de eindscores van websites van bedrijven in Nederland getoond. De gemiddelde eindscore voor alle bedrijfsgroottesklassen is per jaar ongeveer gelijk en neemt elk jaar toe. Zo is de gemiddelde Internet.nl-eindscore gestegen voor alle bedrijven met een website (2 of meer werkzame personen) van 60,4 procent in 2020 naar 74,7 procent in 2026. Voor grote bedrijven met een website (250 of meer werkzame personen) was de Internet.nl-eindscore in 2020 nog 59,2 procent, terwijl dat in 2026 tot 76,1 procent is toegenomen. Deze toename van de eindscore is in dezelfde mate te zien voor de andere bedrijfsgroottesklassen. Opvallend is dat de groei tussen 2025 en 2026 relatief groter is dan in voorgaande jaren met 6,7 procentpunt voor alle bedrijven met een website en 5,9 procentpunt voor zzp'ers met een website.

In de Cybersecuritymonitor 2024 wordt geconstateerd dat kleine bedrijven vaak minder maatregelen treffen om hun ICT-systemen te beveiligen dan grote bedrijven [CBS, 2025a]. Bij het toepassen van internetstandaarden valt het echter op dat kleine bedrijven het even goed, zo niet beter, doen dan middelgrote bedrijven (50 tot 250 werkzame personen). Een verklaring zou kunnen zijn dat kleine bedrijven vaker ICT-specialisten inhuren om hun website te maken en dat

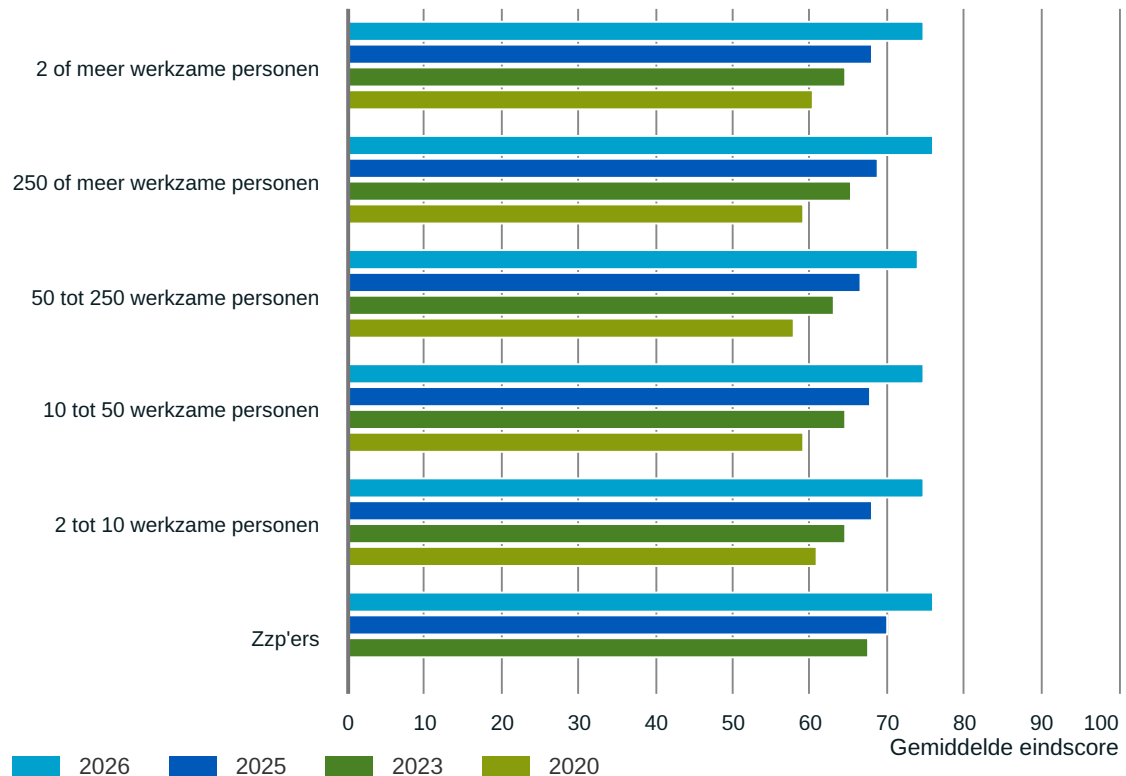
<sup>1</sup>Deze categorie is pas in 2022 toegevoegd.

<sup>2</sup>Merk op dat de resultaten voor zzp'ers voor 2024 ontbreken. Dit komt omdat in de ICT-enquête van 2023 niet aan zzp'ers is gevraagd of zij een website hebben.

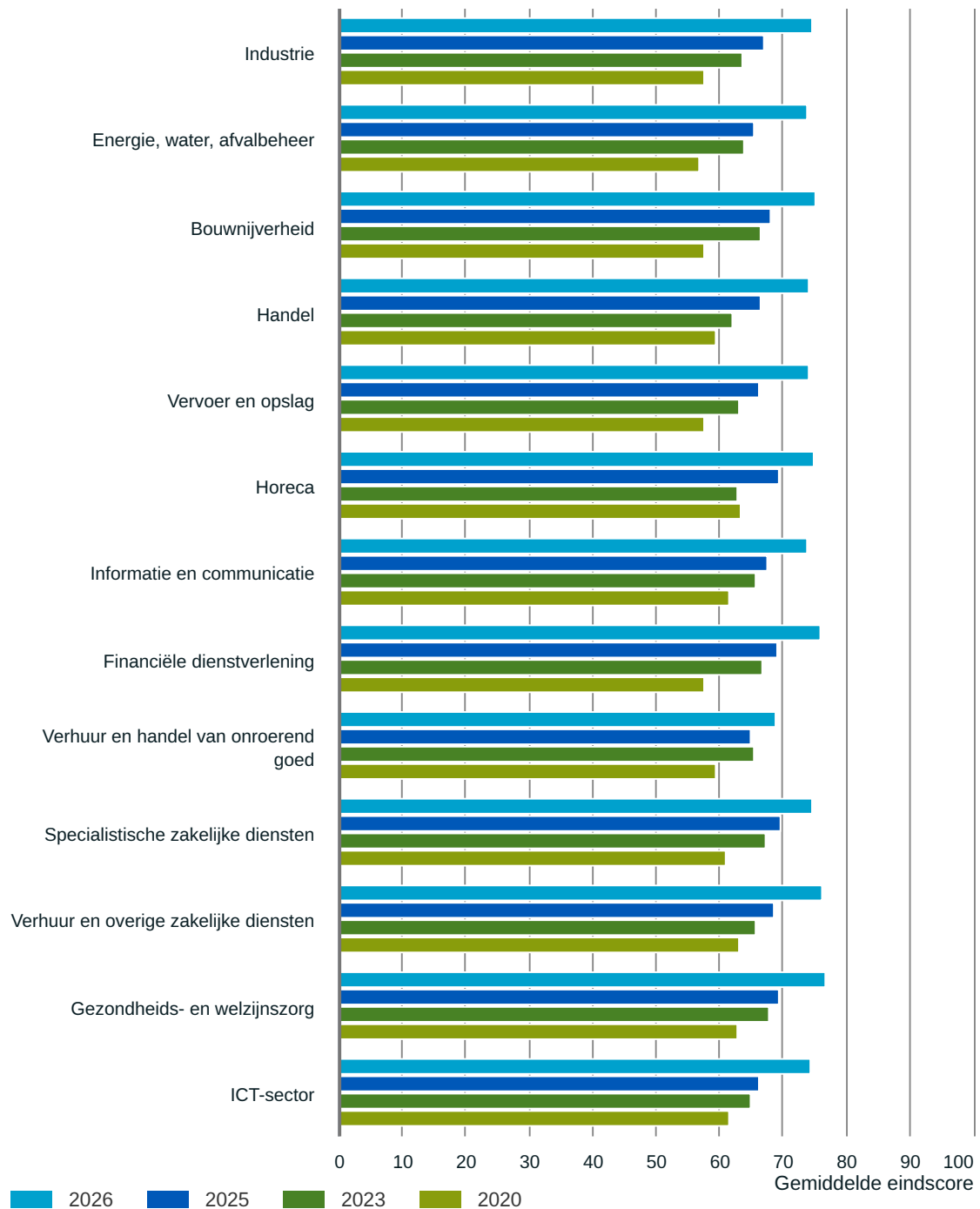
hierbij nieuwere standaarden worden gebruikt. Middelgrote bedrijven hebben mogelijk vaker een website die al wat langer geleden ontwikkeld is. Bij onderhoudswerkzaamheden zijn deze internetstandaarden later ook niet toegepast.

Figuur 3.2 toont de gemiddelde eindscore per bedrijfstak. In 2026 varieert de gemiddelde eindscore van 68,8 procent voor de bedrijfstak 'Verhuur en handel van onroerend goed' tot 76,6 procent voor de bedrijfstak 'Gezondheids- en welzijnszorg'. Daarnaast is te zien dat de totale eindscore voor alle bedrijfstakken tussen 2020 en 2026 gestegen is. Tussen 2025 en 2026 is een relatief grote groei te zien tussen de 4,0 en 8,4 procentpunt voor de verschillende bedrijfstakken.

Figuur 3.1.: Gemiddelde eindscore op Internet.nl voor de websitescan naar bedrijfsgrootteklasse



Figuur 3.2.: Gemiddelde eindscore op Internet.nl voor de websitescan naar bedrijfstak (2 of meer werkzame personen)

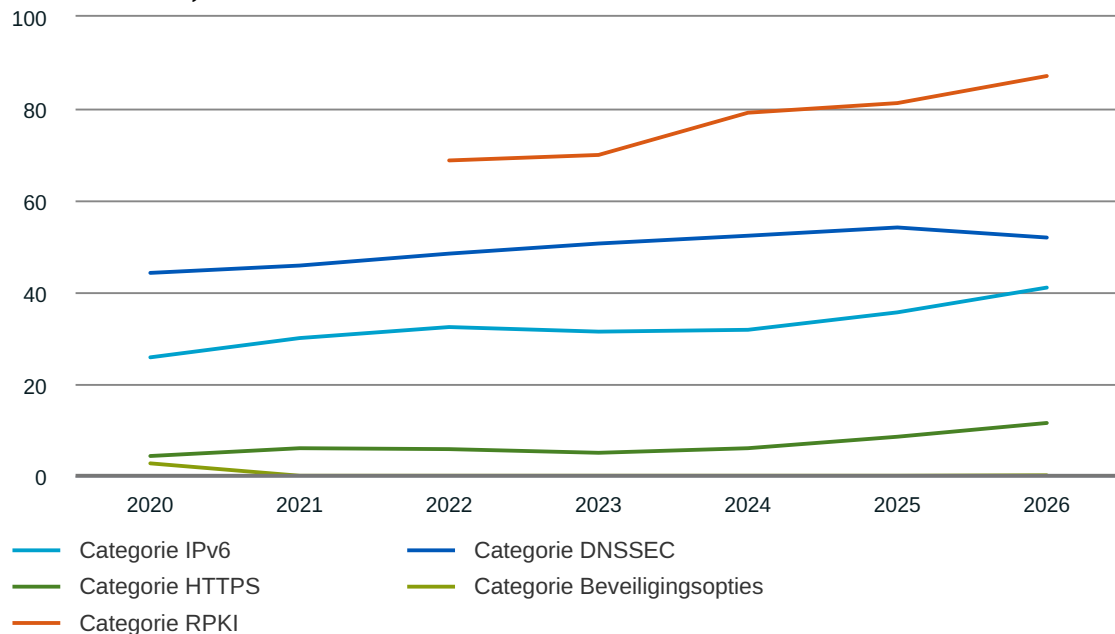


### 3.2. Resultaten websitescan per categorie

Figuur 3.3 toont het percentage van bedrijven met een website dat slaagt voor elk van de vijf categorieën. Het is te zien dat bedrijven in 2026 het vaakst slagen voor de categorie RPKI (87,1 procent). Voor de categorieën DNSSEC en IPv6 slaagt respectievelijk 51,9 en 41,0 procent. Er is een kleine daling te zien voor de categorie DNSSEC ten opzichte van 2025, terwijl bij alle andere categorieën een stijging te zien is. Slechts een klein deel slaagt voor de categorieën HTTPS (11,5

procent) en Beveiligingsopties (0,1 procent). Belangrijk hierbij te vermelden is dat een bedrijf enkel voor een categorie slaagt als deze aan alle verplichte subtesten voldoet.<sup>3</sup>

Figuur 3.3.: Bedrijven die slagen voor de websitescan naar categorie (2 of meer werkzame personen)



In de rest van deze paragraaf wordt voor elk van de vijf categorieën het percentage van geslaagde bedrijven per bedrijfsgrootteklasse en bedrijfstak besproken (zie Figuur 4.4 t/m Figuur 4.13). Hoewel de eindscores niet veel lijken te variëren per bedrijfsgrootteklasse en bedrijfstak, zijn hier wel aanzienlijke verschillen per categorie te zien. Deze verschillen worden hieronder besproken. Daarnaast wordt naar een aantal belangrijke subtesten verwezen. De uitkomsten van alle onderliggende testen voor alle jaren worden in Figuur B.13 t/m Figuur B.82 gegeven.

### 3.2.1. Categorie IPv6

De categorie IPv6 bevat testen die controleren in hoeverre een website bereikbaar is via een Internet Protocol (IP)-adres van het type IPv6. Elk apparaat dat verbinding maakt met het internet (zoals computers, printers etc.) heeft een uniek adres, oftewel een IP-adres. Dit IP-adres is een reeks tekens dat het apparaat herkenbaar maakt voor andere apparaten. Vroeger werden vooral IP-adressen van het type IP versie 4 (IPv4) gebruikt, maar omdat deze inmiddels opraken, worden er tegenwoordig ook steeds meer gebruikgemaakt van IP-adressen van het type 'IP versie 6' (IPv6). Één van de grote voordelen van het type IPv6 is dat deze adressen langer zijn en uit meer verschillende tekens kan bestaan. Hierdoor zijn er veel meer unieke adressen beschikbaar.

Figuur 3.4 laat zien dat kleine bedrijven met een website (2 tot 10 werkzame personen) in 2026 vaker slagen voor de categorie IPv6 dan grote bedrijven: respectievelijk 42,8 en 32,3 procent. Voor zzp'ers met een website is te zien dat zij nog beter scoren: 47,7 procent slaagt in 2026 voor de categorie IPv6. In elke bedrijfsgrootteklasse is een stijging te zien tussen 2025 en 2026. Dat kleine bedrijven vaker voor de categorie IPv6 slagen dan grote bedrijven komt wellicht doordat kleine bedrijven hun website vaker hosten bij externe providers met moderne

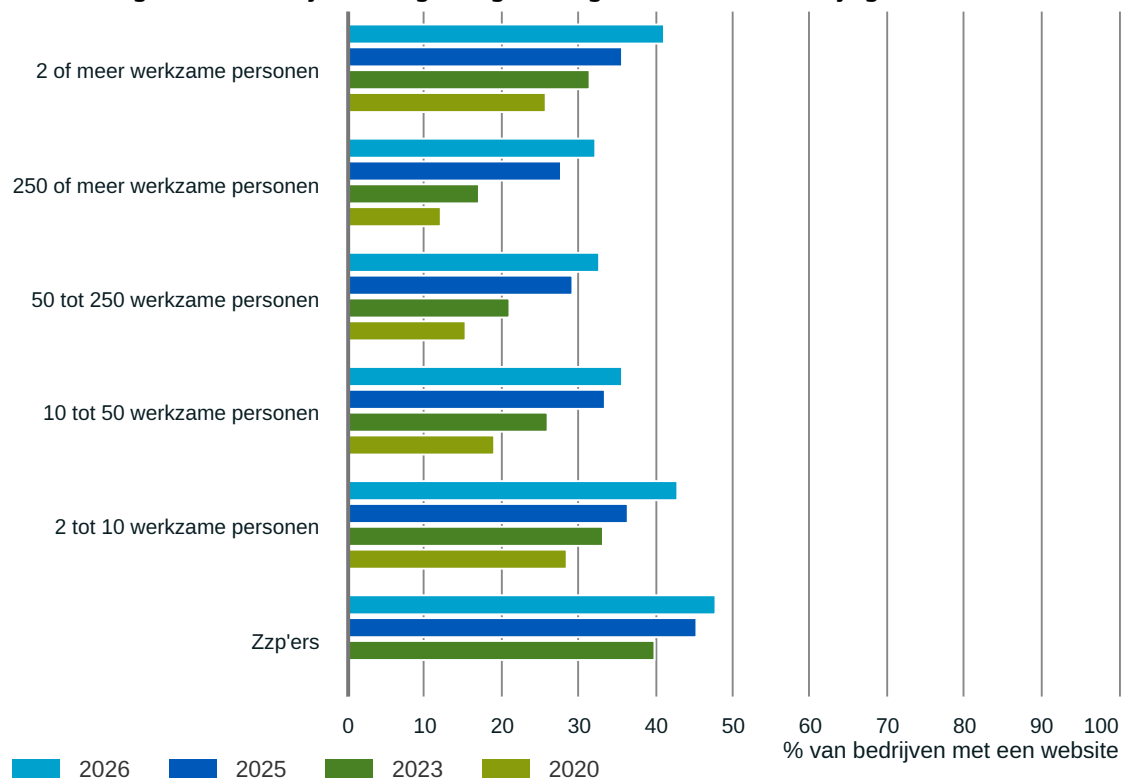
<sup>3</sup>Voor de categorie Beveiligingsopties is geen enkele vraag verplicht. Een bedrijf slaagt enkel voor deze categorie als aan alle subtesten voldaan is.

netwerkinstellingen. Grote bedrijven draaien hun website mogelijk vaker op eigen servers die minder up-to-date zijn. Het ontbreken van ondersteuning van IPv6 brengt niet direct een veiligheidsrisico met zich mee, dus voor veel grote bedrijven is er ook minder aanleiding om hun servers aan te passen om IPv6 te gaan ondersteunen.

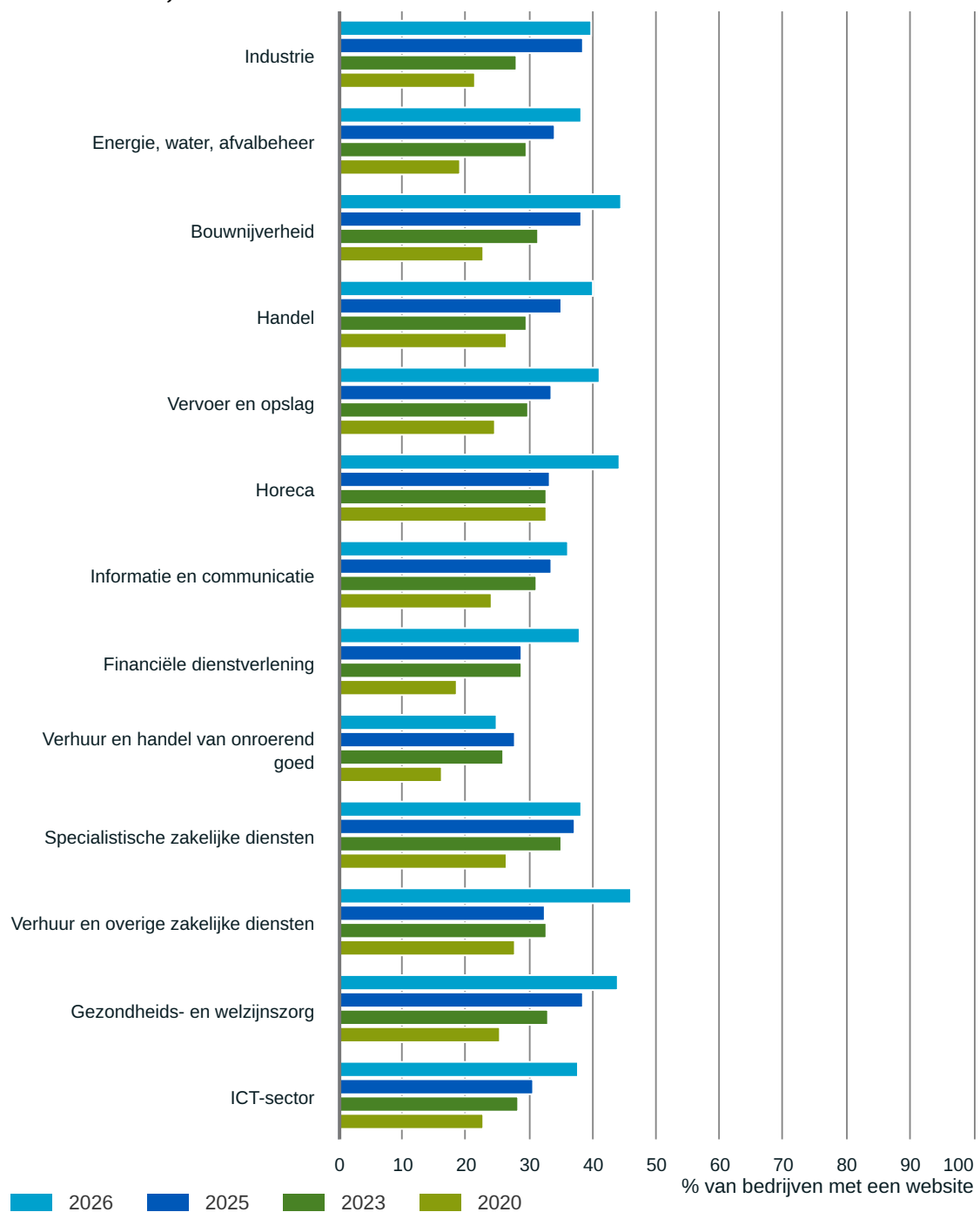
De uitsplitsing van de categorie IPv6 naar bedrijfstak getoond in Figuur 3.5 laat zien dat de bedrijfstakken 'Verhuur en overige zakelijke diensten', 'Bouwnijverheid', 'Horeca' en 'Gezondheids- en welzijnzorg' de ondersteuning van IPv6 het beste op orde hebben. Vergeleken met 2020 zijn de scores echter in alle bedrijfstakken gestegen. Vooral de resultaten van de bedrijfstakken 'Verhuur en overige zakelijke diensten', 'Horeca' en 'Financiële dienstverlening' zijn aanzienlijk gestegen tussen 2025 en 2026.

De categorie IPv6 is gebaseerd op vijf onderliggende subtesten. Het grootste gedeelte van de bedrijven met een website (ongeveer 85 procent) slaagt voor de subtesten over IPv6-adoptie bij nameservers (Figuur B.13 t/m Figuur B.16), terwijl aan de subtesten over IPv6-adoptie bij webservern en de vergelijking tussen IPv4 en IPv6 door een stuk minder bedrijven (ongeveer 40 procent) wordt voldaan (Figuur B.17 t/m Figuur B.22)

Figuur 3.4.: Bedrijven met geslaagde categorie 'IPv6' naar bedrijfsgrootteklasse



Figuur 3.5.: Bedrijven met geslaagde categorie 'IPv6' naar bedrijfstak (2 of meer werkzame personen)



### 3.2.2. Categorie DNSSEC

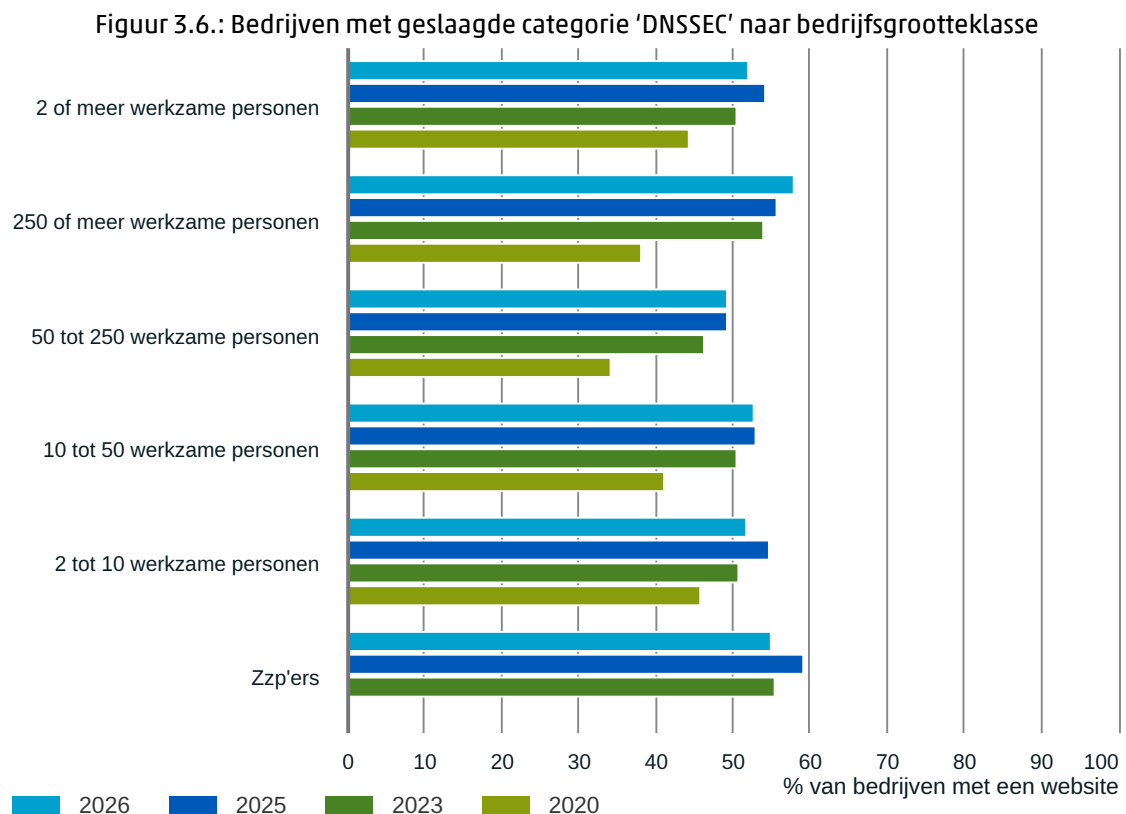
De categorie DNSSEC geeft aan in hoeverre een website beveiligd is met Domain Name System Security Extensions (DNSSEC). DNSSEC is een beveiligingssysteem voor het Domain Name System (DNS), het internettelefoonboek dat zorgt voor de vertaling van domeinnamen naar IP adressen. Met alleen DNS is de vertaling van een domeinnaam namelijk niet beveiligd. Een kwaadwillende zou een gebruiker alsnog kunnen omleiden naar een vals IP adres, waar vervolgens vertrouwelijke gegevens of zelfs geld ontfutseld zou kunnen worden door middel van phishing

en pharming<sup>4</sup>. Met DNSSEC wordt bij de vertaling van domeinnaam naar IP adres daarom altijd een digitale handtekening toegevoegd die automatisch kan worden gecontroleerd.

Figuur 3.6 laat zien dat 51,9 procent van de bedrijven met een website in 2026 een geldige handtekening heeft. Ten opzichte van 2020 zijn de resultaten in alle bedrijfsgroottes verbeterd, maar ten opzichte van 2025 is er in verschillende grootteklassen een daling te zien. Alleen het percentage van grote bedrijven dat slaagt is gestegen ten opzichte van 2025. Zo slaagt 57,9 procent van de grote bedrijven met een website in 2026 voor de categorie DNSSEC, tegenover 55,8 procent in 2025. Kleine bedrijven met een website scoren in 2026 nu 51,8 procent, terwijl dat in 2025 nog 54,6 procent was.

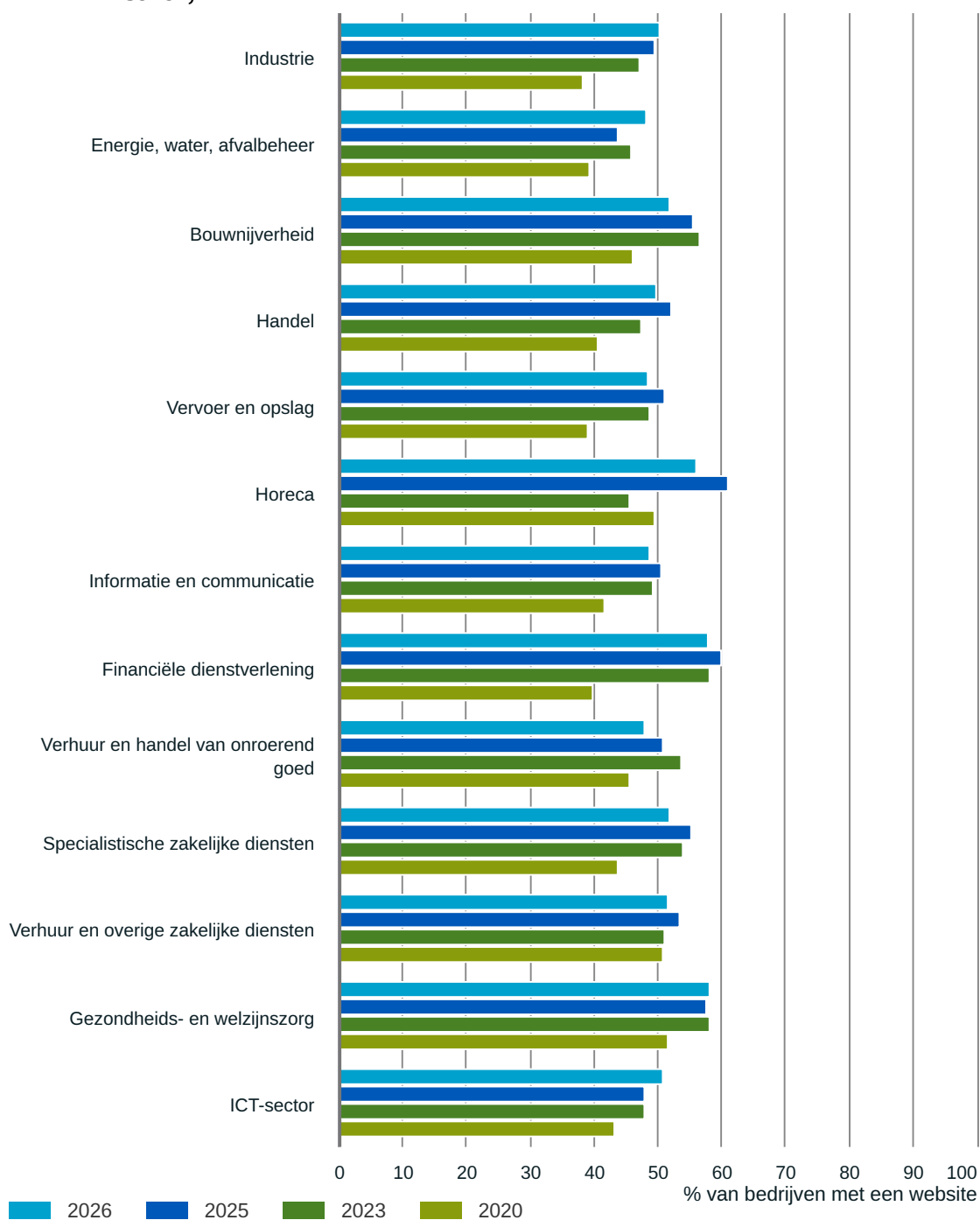
Figuur 3.7 laat zien dat bedrijven in de bedrijfstak 'Gezondheids- en welzijnzorg' in 2026 het vaakst slagen (58,2 procent), gevolgd door bedrijven in de bedrijfstak 'Financiële dienstverlening' (57,8 procent). Bedrijven uit de bedrijfstak 'Verhuur en handel van onroerend goed' slagen in 2026 het minst vaak (48,0 procent). Of er een stijging of daling te zien is ten opzichte van 2025, varieert tussen de verschillende bedrijfstakken.

De categorie DNSSEC is gebaseerd op maar twee onderliggende testen: DNSSEC aanwezig (Figuur B.23) en DNSSEC geldig (Figuur B.25). Het is dan ook te zien dat de scoreverdeling van de categorie DNSSEC bijna identiek is aan de resultaten voor deze onderliggende testen.



<sup>4</sup>Bij pharming probeert een crimineel gegevens van gebruikers te verkrijgen door ze naar een nepversie van een echte website te leiden. Bij phishing probeert een crimineel op een meer directe manier gegevens van een gebruiker te verkrijgen door personen te benaderen met e-mails die lijken op bijvoorbeeld de e-mail van een bank met een verzoek om inloggegevens te geven.

Figuur 3.7.: Bedrijven met geslaagde categorie 'DNSSEC' naar bedrijfstak (2 of meer werkzame personen)



### 3.2.3. Categorie HTTPS

De categorie HTTPS geeft aan of een website bereikbaar is via een beveiligde verbinding. Met Hypertext Transfer Protocol Secure (HTTPS) worden alle gegevens die op een website ingevoerd en verstuurd worden, versleuteld. Vertrouwelijke informatie, zoals wachtwoorden, creditcard- of bankgegevens, of andere (persoons)gegevens, kunnen hierdoor niet zomaar onderschept of afgeluisterd worden. Deze categorie is gebaseerd op maar liefst 21 subtesten die verschillende aspecten van beveiligde verbinding controleren, waaronder HTTP, TLS, certificatie en DANE.

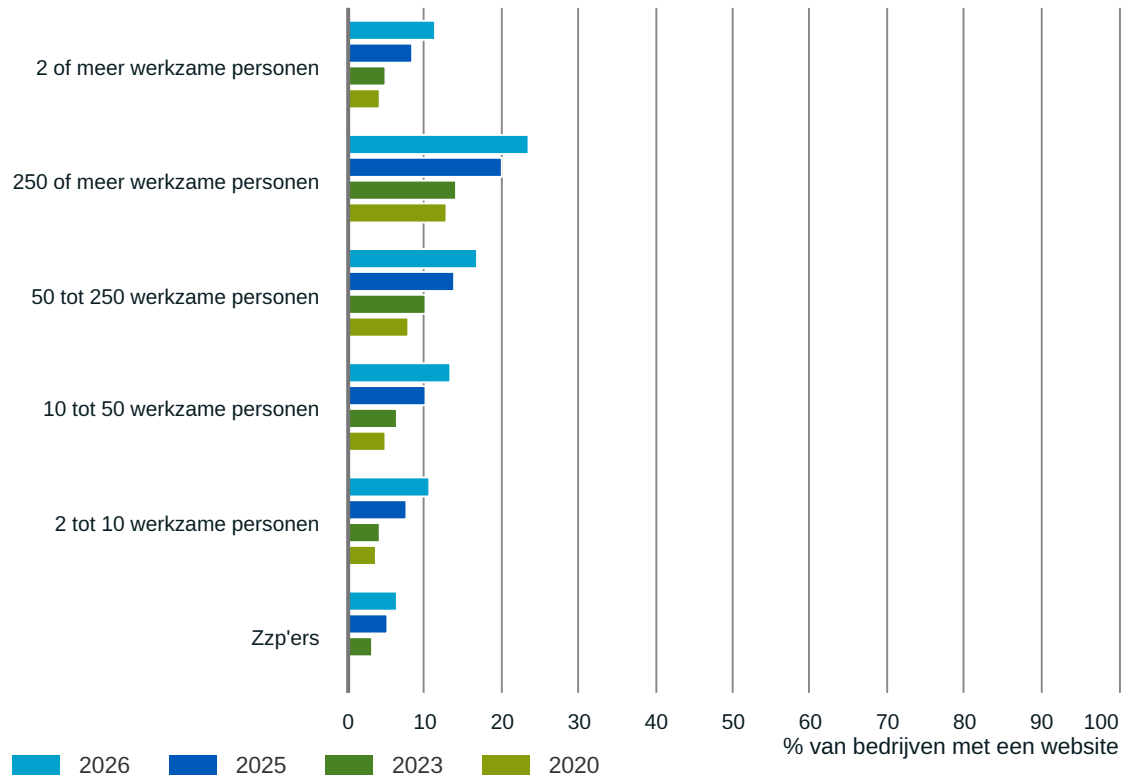
Ditmaal is in Figuur 3.8 te zien dat grote bedrijven aanzienlijk beter scoren voor de categorie HTTPS dan kleine bedrijven. Opvallend is wel dat het slagingspercentage voor deze categorie vrij laag is. Slechts 11,5 procent van alle bedrijven met een website heeft in 2026 een positieve uitslag voor de categorie HTTPS. Dit lage slagingspercentage wordt veroorzaakt door het groot aantal subtesten dat gebruikt wordt om de categorie HTTPS te doen slagen. Als één van de verplichte subtesten niet slaagt, zal hiermee ook de totale categorie HTTPS niet slagen. Ondanks dat niet veel bedrijven slagen voor de gehele categorie HTTPS, is in Figuur B.27 wel te zien dat 95,1 procent van alle bedrijven met een website HTTPS beschikbaar heeft. Figuur B.28 toont dat dit redelijk gelijkmatig over de bedrijfstakken verdeeld is. De resultaten van alle andere subtesten zijn te vinden in Paragraaf B.4.

Figuur 3.9 toont aan dat de bedrijfstak 'Gezondheids- en welzijnszorg' in 2026 het beste scoort voor de categorie HTTPS (18,6 procent). Deze bedrijfstak heeft ten opzichte van 2025 bijna een verdubbeling van het slagingspercentage voor deze categorie. Voor bijna alle andere bedrijfstakken is ook een groei te zien, behalve voor de bedrijfstakken 'Vervoer en opslag' en 'Verhuur en handel van onroerend goed'.

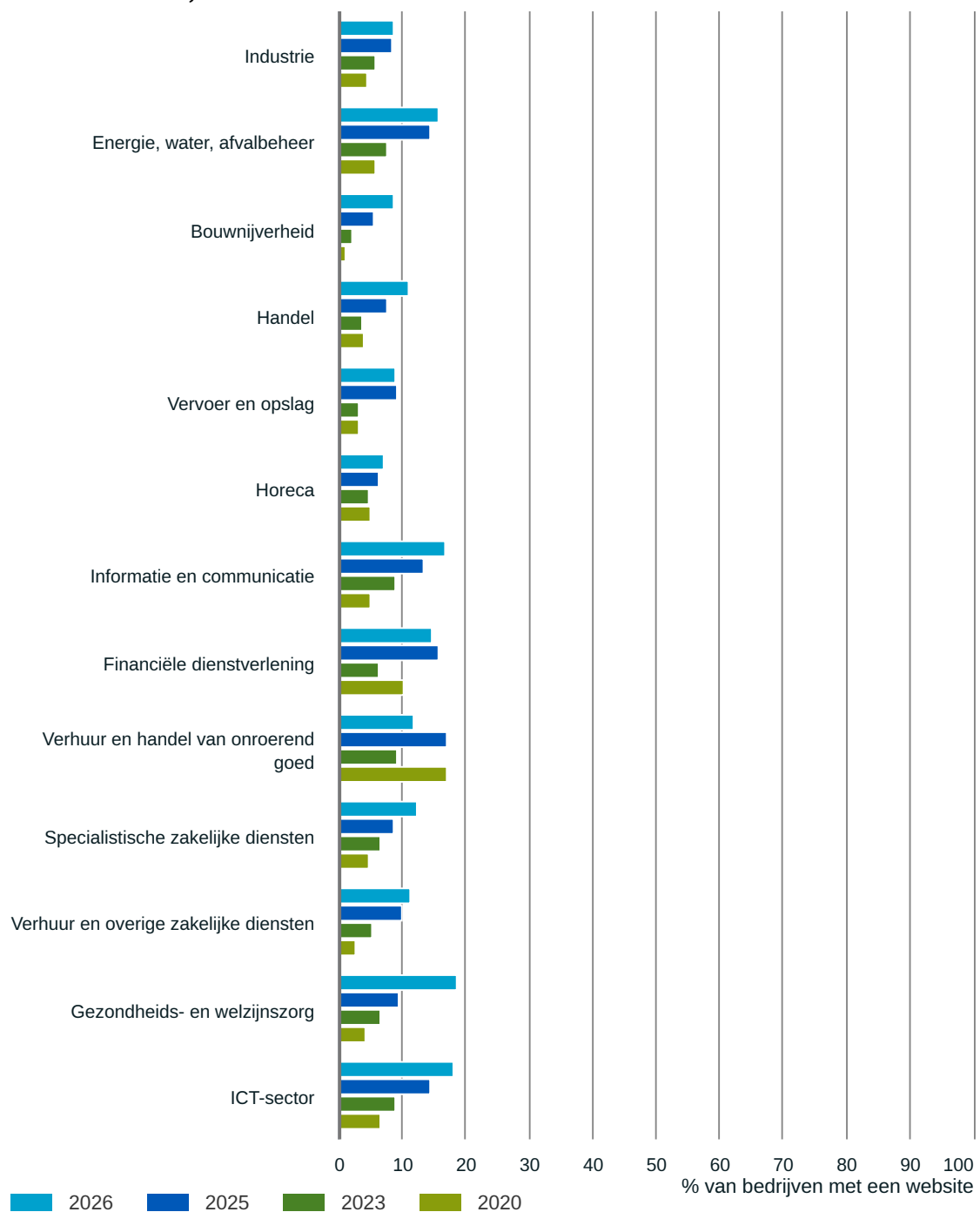
Één van de testen binnen de categorie HTTPS waar bedrijven slecht op scoren, is het gebruik van HSTS, zoals in Figuur B.33 te zien is. HSTS staat voor HTTP Strict-Transport-Security, en laat browsers weten dat een website alleen met HTTPS benaderd moet worden. Dit betekent dat alle toekomstige verzoeken met HTTP automatisch moeten worden omgezet in verzoeken met HTTPS. Door de lage score op deze subtest, valt ook de score op de totale categorie HTTPS laag uit. Van alle bedrijven met een website slaagt in 2026 maar 19,6 procent voor deze test.

Voor het overgrote gedeelte van de subtesten binnen de subcategorieën HTTP, TLS en certificatie is te zien dat meer dan 70 procent van de bedrijven slaagt, waarbij een aantal subtesten zelfs door meer dan 95 procent wordt behaald (zie Paragraaf B.4). De in 2026 nieuw geïntroduceerde subtest over een geldig CAA-record voor het domein, waarvan de uitkomst te zien is in Figuur B.63, wordt door nog maar weinig bedrijven behaald. Deze subtest en de subtesten over DANE en OCSP stapling worden niet meegenomen bij het berekenen van de categorie- en eindscores. Deze subtesten hebben ook de laagste slagingspercentages.

Figuur 3.8.: Bedrijven met geslaagde categorie 'HTTPS' naar bedrijfsgrootteklasse



Figuur 3.9.: Bedrijven met geslaagde categorie 'HTTPS' naar bedrijfstak (2 of meer werkzame personen)



### 3.2.4. Categorie Beveiligingsopties

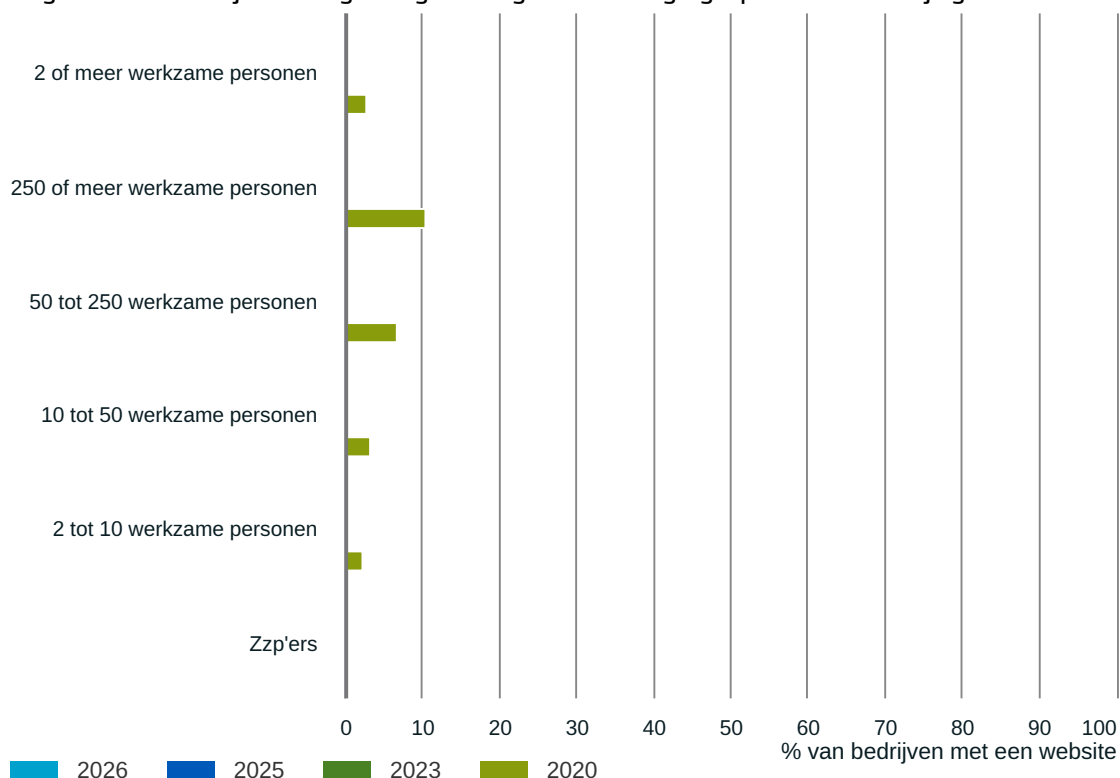
Met de categorie Beveiligingsopties wordt bepaald of een website de juiste 'security headers' heeft ingesteld om bezoekers te beschermen tegen cyberaanvallen. Met een security header kan een website bepalen hoe een browser waarmee de website bezocht wordt zich moet gedragen. Zo kan de security header Content-Security-Policy (CSP) bepalen welke bronnen (zoals scripts, afbeeldingen etc.) geladen mogen worden. Op deze manier worden bezoekers beschermd tegen aanvallen met bijvoorbeeld cross-site scripting (XSS) of framing. Deze categorie bestaat uit vijf

subtesten die niet worden meegenomen bij het berekenen van de overkoepelende eindscore, maar die in dit geval wel meetellen voor de uitslag van deze specifieke categorie.

Figuur 3.10 toont aan dat in 2020 nog ruim 10 procent van de grote bedrijven met een website voor deze categorie slaagde. Van alle bedrijven met een website slaagde 2,7 procent in 2020. Vanaf 2021 slagen echter nauwelijks bedrijven voor deze categorie (0,1 procent in 2026), waardoor de groene, licht- en donkerblauwe staafjes niet meer zichtbaar zijn. Dat weinig bedrijven vanaf 2021 slagen, komt door twee onderliggende subtesten, namelijk de subtest 'Content-Security-Policy' (Figuur B.73) en 'security.txt' (Figuur B.77). De eerste van deze twee testen telt sinds 21 maart 2021 mee ook voor de uitslag van de hele categorie. Blijkbaar zijn er nauwelijks bedrijven die de subtest 'Content-Security-Policy' volgens de laatste eisen voor hun website uitvoeren, waardoor ook de hele categorie Beveiligingsopties nauwelijks succesvolle resultaten oplevert.

De andere onderliggende subtesten van deze categorie vertonen nog wel een positieve trend over de jaren heen. Zo slagen door de jaren heen steeds meer bedrijven met een website voor de subtest 'X-Frame-Options' (Figuur B.69). Voor alle bedrijven met een website is een stijging te zien van 11,9 procent in 2020 naar 16,4 procent in 2026. Grote bedrijven slagen daarbij vaker voor deze test dan kleine bedrijven. Van de grote bedrijven met een website slaagt 27,3 procent in 2026, tegenover 15,6 procent van de kleine bedrijven met een website. Een vergelijkbare uitkomst is te zien bij de subtest 'X-Content-Type-Options' (Figuur B.71)

Figuur 3.10.: Bedrijven met geslaagde categorie 'Beveiligingsopties' naar bedrijfsgrootteklasse



Figuur 3.11.: Bedrijven met geslaagde categorie 'Beveiligingsopties' naar bedrijfstak (2 of meer werkzame personen)

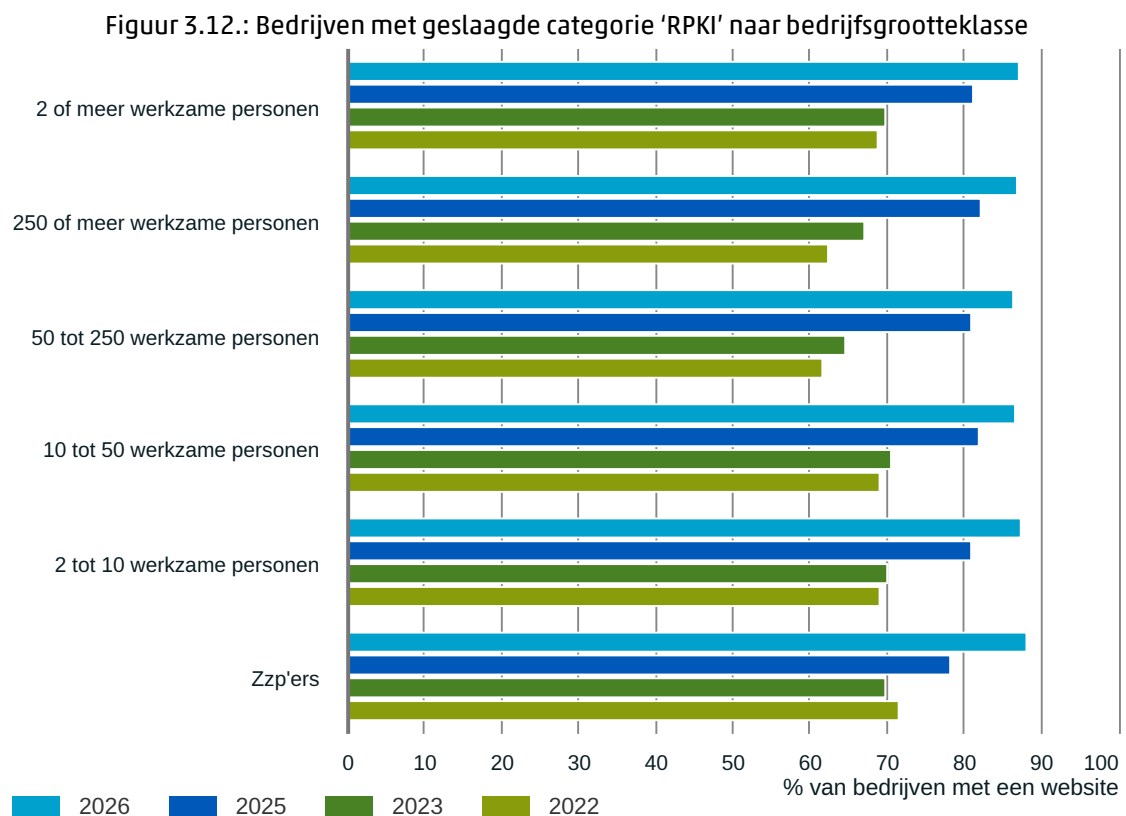


### 3.2.5. Categorie Autorisatie voor Routing (RPKI)

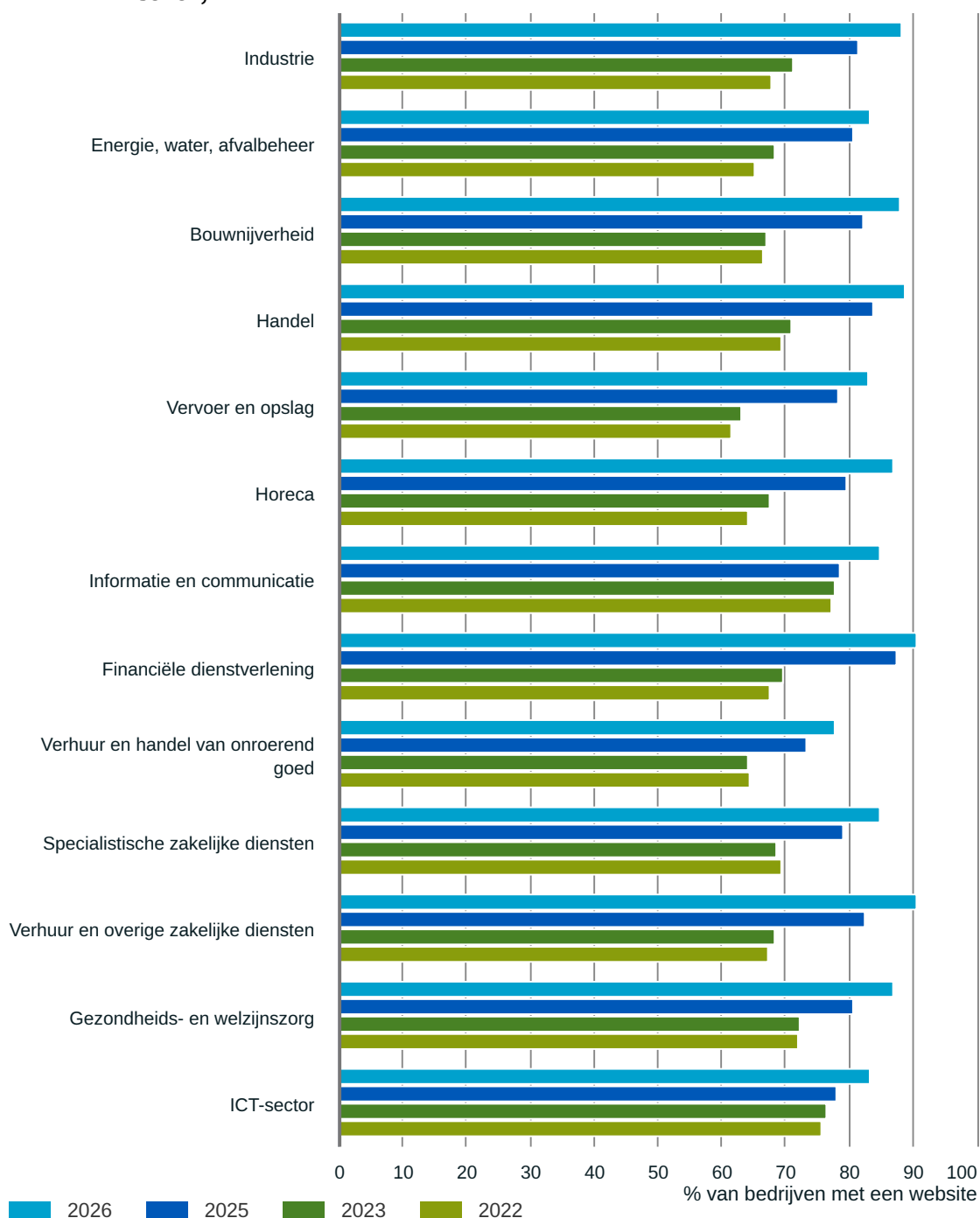
Resource Public Key Infrastructure (RPKI) is een techniek die kan worden gezien als een aanvulling op het eerdergenoemde DNSSEC. Hoewel DNSSEC zorgt voor de juiste vertaling van domeinnamen naar IP-adressen, zorgt RPKI er ook daadwerkelijk voor dat het verkeer naar die IP-adressen op de juiste plek belandt. Met RPKI kan dus worden voorkomen dat internetverkeer wordt omgeleid naar de systemen van een ongeautoriseerd netwerk. Deze categorie is pas in 2022 aan de webitescan toegevoegd.

Figuur 3.12 laat een stijging zien in de uitkomsten ten opzichte van 2025 voor alle grootteklassen. Van alle bedrijven met een website slaagt 87,1 procent in 2026, tegenover 81,2 procent in 2025. Er zijn geen grote verschillen tussen de verschillende grootteklassen. Figuur 3.13 toont aan dat de bedrijfstakken 'Financiële dienstverlening' en 'Verhuur en overige zakelijke diensten' met 90,5 procent het hoogste scores. Geen enkele bedrijfstak heeft een slagingspercentage onder de 77,7 procent.

Als alleen naar de subtest 'Geldigheid van route-aankondiging voor webserver' gekeken wordt (Figuur B.85), dan is te zien dat 87,2 procent van de bedrijven met een website een geldige RPKI op de website heeft in 2026. Voor de subtest 'Geldigheid van route-aankondiging voor nameserver van domein' (Figuur B.81) is te zien dat 92,1 procent van de bedrijven met een website slaagt.



Figuur 3.13.: Bedrijven met geslaagde categorie 'RPKI' naar bedrijfstak (2 of meer werkzame personen)



### 3.3. Verdelingen van de eindscores van de websitescans

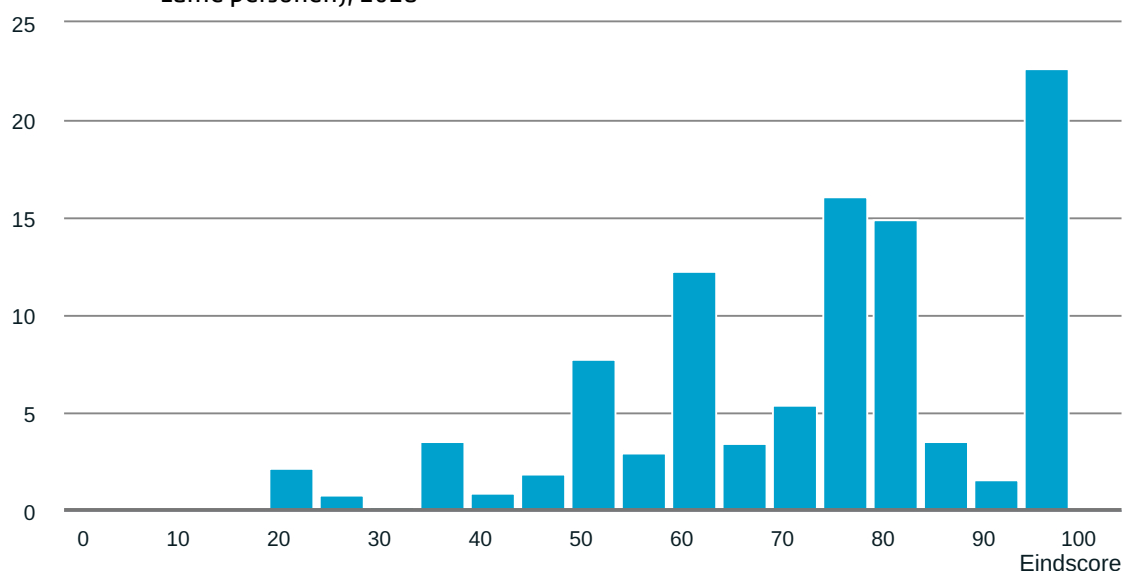
Hoewel de gemiddelde eindscore van alle bedrijven met een website (2 of meer werkzame personen) in 2026 rond de 75 procent ligt, is hierboven al geconstateerd dat de uitslag voor de verschillende categorieën wel per bedrijfsgrootteklasse en bedrijfstak varieert. In deze paragraaf wordt gekeken naar de spreiding van de eindscores voor alle bedrijven.

De verdeling van de eindscore voor alle bedrijven met een website is voor 2026 te zien in

Figuur 3.14. De verdeling vertoont pieken rond de 60, 75 en 95 procent. In Tabel 3.1 zijn daarnaast drie kwartielen weergegeven. De verdelingen voor de overige jaren worden getoond in Paragraaf B.7. In Tabel 3.1 geeft het eerste kwartiel (Q1) aan dat 25 procent van de bedrijven een eindscore lager dan 62 procent behaalt. Het tweede kwartiel (Q2, de mediaan) geeft aan dat de helft van alle bedrijven een score hoger dan 78 procent behaalt. Het derde kwartiel (Q3) geeft ten slotte aan dat 25 procent van de bedrijven een score hoger dan 86 procent behaalt. Voor alle kwartielen geldt dat er een stijging te zien is ten opzichte van 2025. Kortom, de hele verdeling is naar rechts verplaatst, wat wijst op een stijging in eindscore over de gehele linie.

In een voorgaand rapport werd aangetoond dat de pieken in de verdeling redelijk overeenkomen met het aantal categorieën waarvoor een website slaagt [CBS, 2022b]. De spreiding rondom een piek wordt veroorzaakt door spreiding van het aantal geslaagde onderliggende subtesten. De scorebepaling is echter dynamisch en past zich aan de veiligheidseisen aan. Hierdoor is te zien dat de verdeling van de scores over de jaren verandert. Meer bedrijven schuiven richting de 100 procent score op, waardoor de piek rond de 100 procent is toegenomen.

Figuur 3.14.: Verdeling eindscores websitescan voor bedrijven met een website (2 of meer werkzame personen), 2026



Tabel 3.1.: Percentielen eindscores websitescan voor bedrijven met een website (2 of meer werkzame personen)

Percentiel	2020	2021	2022	2023	2024	2025	2026
25	43	47	49	48	49	50	62
50 (mediaan)	64	68	68	70	70	71	78
75	76	79	79	79	79	81	86

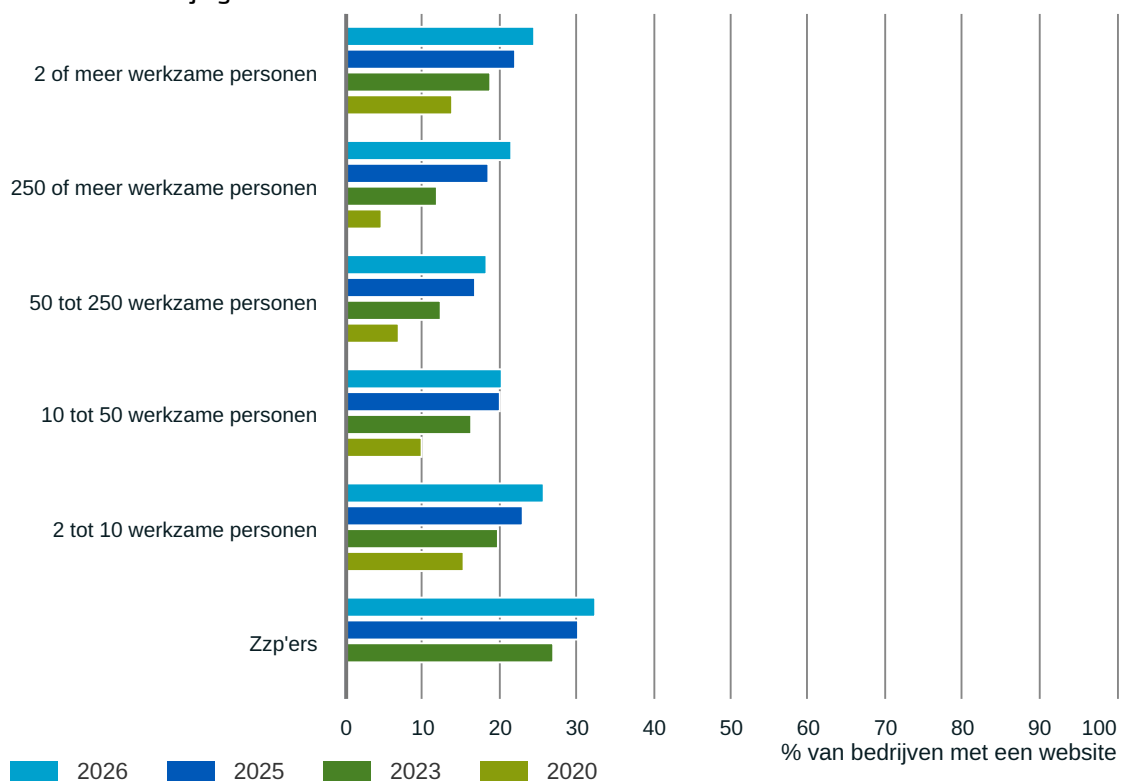
### 3.4. Welke bedrijven hebben de hoogste en laagste eindscore voor de websitescan?

In Figuur 3.15 en Figuur 3.16 worden de bedrijven met de hoogste scores voor de websitescan weergegeven per bedrijfsgrootteklasse en bedrijfstak. Als gekeken wordt naar het percentage van bedrijven dat een eindscore van 90 procent of meer haalt, dan is een duidelijke trend te zien.

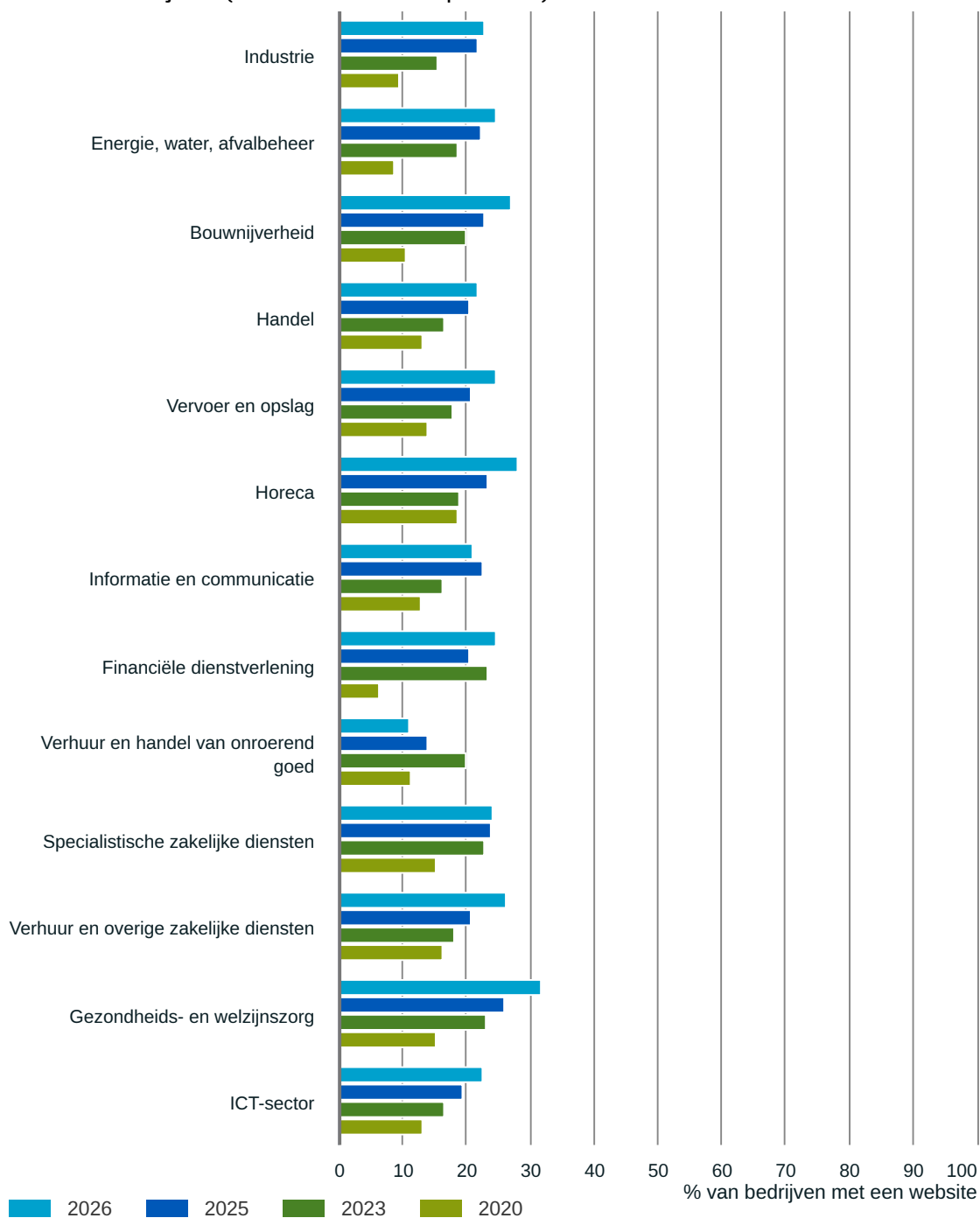
Kleine bedrijven met een website halen relatief vaker een eindscore van 90 procent of meer dan grote bedrijven. Zzp'ers behalen relatief gezien nog vaker hoge scores. Daarnaast kan geconcludeerd worden dat het aantal bedrijven met een website dat een eindscore van 90 procent haalt in 2026 is toegenomen. In 2020 haalde maar 13,8 procent van de bedrijven een score van 90 of meer, terwijl dat in 2026 ondertussen al 24,5 procent is.

De verdeling van bedrijven met een eindscore van 90 procent of meer in Figuur 3.16 laat zien dat de bedrijfstak 'Gezondheids- en welzijnzorg' in 2026 de best scorende bedrijfstak is. Mogelijk spelen de bestaande normen voor informatiebeveiliging in de zorg, zoals de NEN 7510, hierin een rol. In 2026 heeft 31,6 procent van de bedrijven in de bedrijfstak 'Gezondheids- en welzijnzorg' een website met een eindscore van 90 procent of meer.

Figuur 3.15.: Bedrijven met een eindscore van 90 procent of hoger voor de websitescan naar bedrijfsgrootteklasse



Figuur 3.16.: Bedrijven met een eindscore van 90 procent of hoger voor de websitescan naar bedrijfstak (2 of meer werkzame personen)

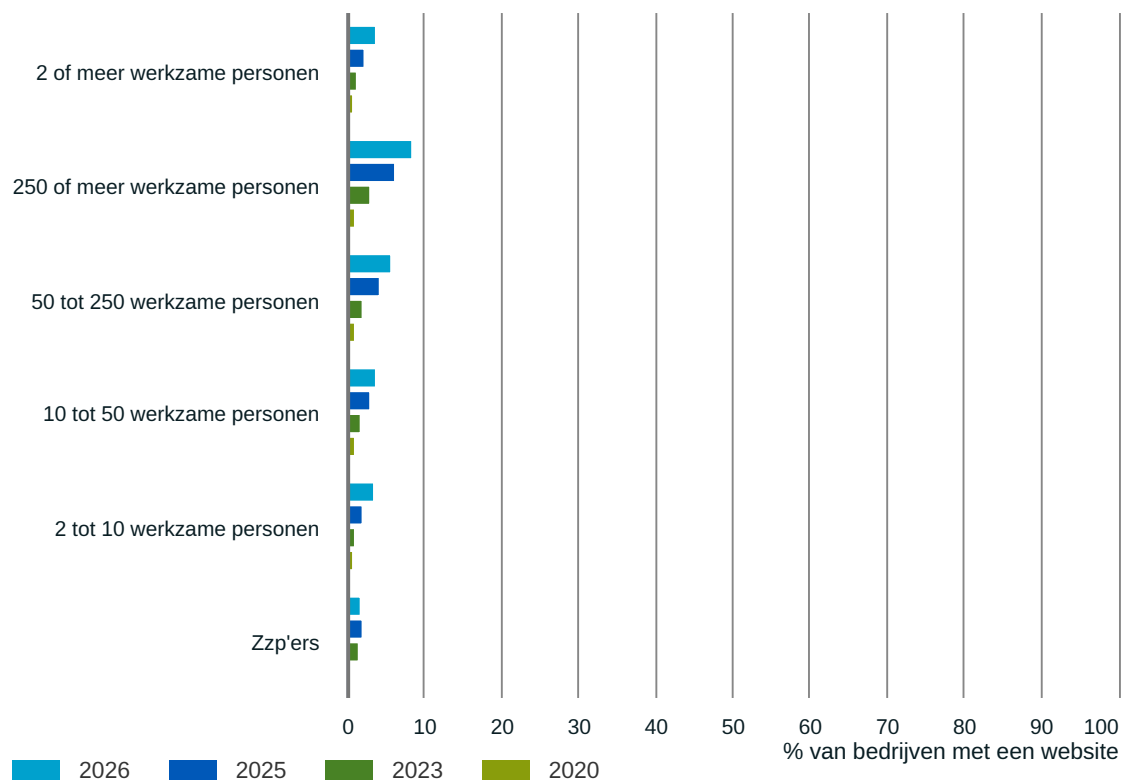


In Figuur 3.17 wordt gekeken naar het percentage van bedrijven met een website dat een eindscore van 100 procent haalt. Waar in Figuur 3.15 duidelijk te zien was dat grote bedrijven relatief minder vaak een score van 90 procent of meer halen ten opzichte van kleine bedrijven, is in Figuur 3.17 te zien dat deze trend voor bedrijven met een eindscore van 100 procent precies andersom is. Van de grote bedrijven met een website haalt in 2026 8,5 procent een score van 100 procent. Dus hoewel kleine bedrijven vaker goed scoren (met een score van 90 procent of meer), is te concluderen dat als grote bedrijven boven de 90 procent scoren, ze relatief vaker ook direct een 100 procent score halen. Een verklaring zou wellicht kunnen zijn dat grote bedrijven hun website op hun eigen server hosten, terwijl kleine bedrijven hun website vaker hosten bij een

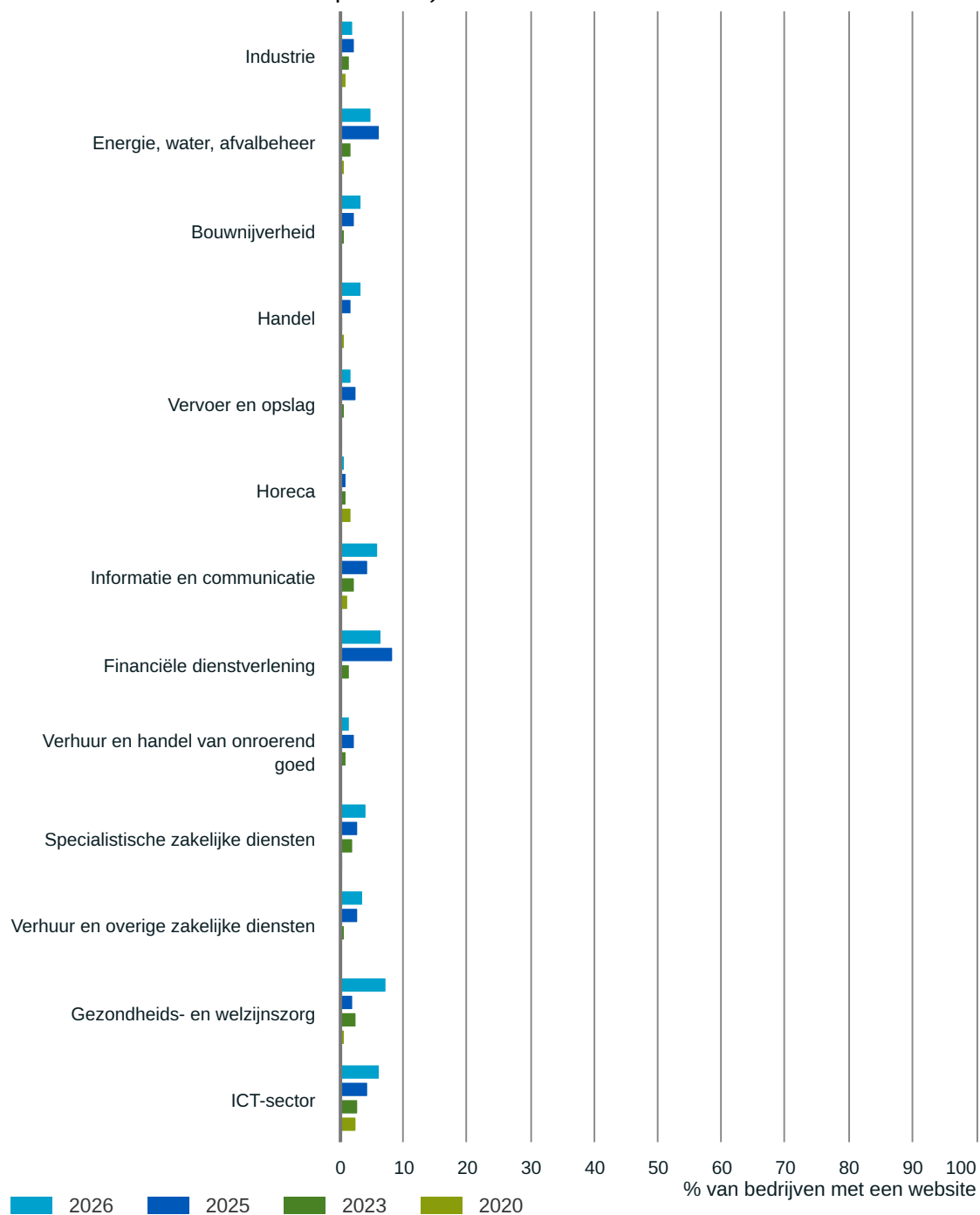
externe serviceprovider. Van een aantal internetstandaarden is bekend dat bedrijven deze - vanwege afhankelijkheden van de netwerkinstellingen van de server - in dat geval niet helemaal in eigen hand hebben.

Figuur 3.18 laat de verdeling over de bedrijfstakken zien van de bedrijven met een website die een eindscore van 100 procent halen. Net als bij de score van 90 procent of meer, is de bedrijfstak 'Gezondheids- en welzijnszorg' de best scorende bedrijfstak. Opvallend is dat de best scorende bedrijfstak uit 2025, de 'Financiële dienstverlening', in 2026 procentueel gezien minder bedrijven heeft met een eindscore van 100 procent ten opzichte van 2025. Voor bijna alle andere bedrijfstakken is juist een stijging te zien.

Figuur 3.17.: Bedrijven met een eindscore van 100 procent voor de websitescan naar bedrijfsgrootteklasse



Figuur 3.18.: Bedrijven met een eindscore van 100 procent voor de websitescan naar bedrijfstak (2 of meer werkzame personen)

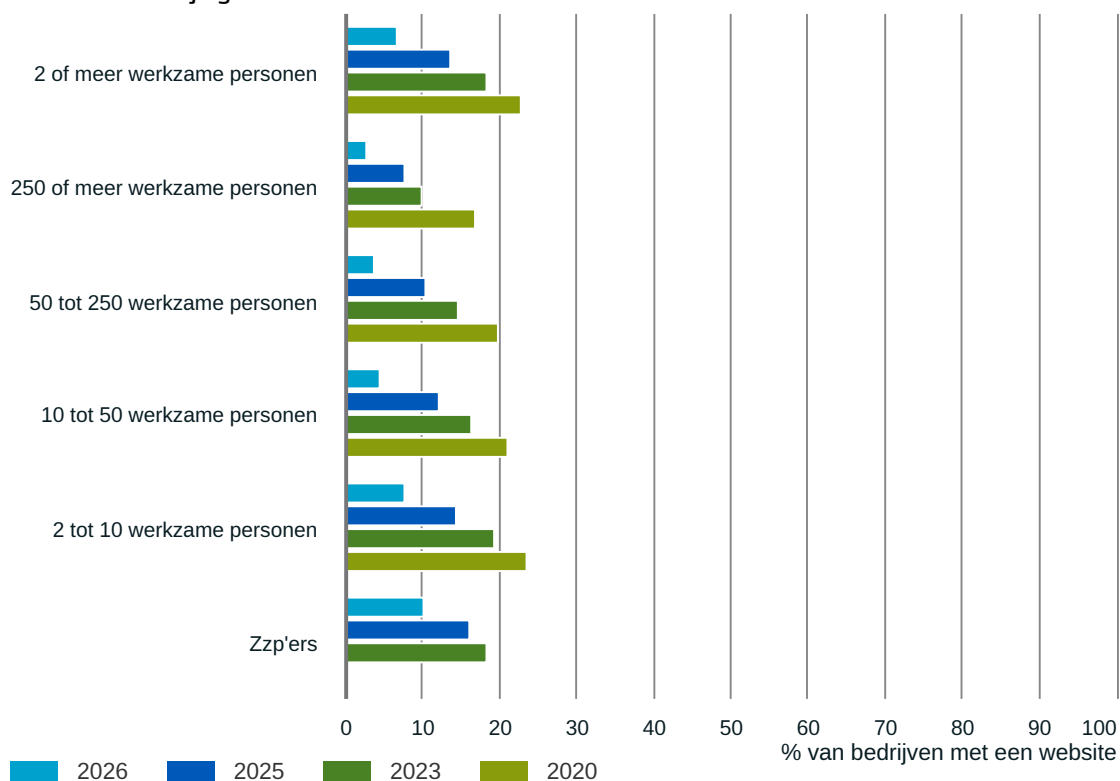


Tot nu toe is aangetoond dat kleine bedrijven relatief vaker een score van 90 procent of meer halen dan grote bedrijven. Eerder in Figuur 3.1 is ook geconstateerd dat de gemiddelde eindscore over alle bedrijfsgrootteklassen niet veel varieert, met gemiddelde eindscores voor alle bedrijfsgrootteklassen van rond de 75 procent. Dit impliceert dat kleine bedrijven ook vaker juist een lagere score halen, waardoor de gemiddelde eindscore voor grote en kleine bedrijven ongeveer gelijk is. In Figuur 3.19 is te zien dat dit inderdaad het geval is: kleine bedrijven halen relatief vaker een eindscore van 40 procent of minder dan grote bedrijven. In 2026 heeft 7,6 procent van de kleine bedrijven met een website een score onder de 40 procent, tegenover maar 2,7 procent van de grote bedrijven met een website. Hiermee kan geconcludeerd worden dat de

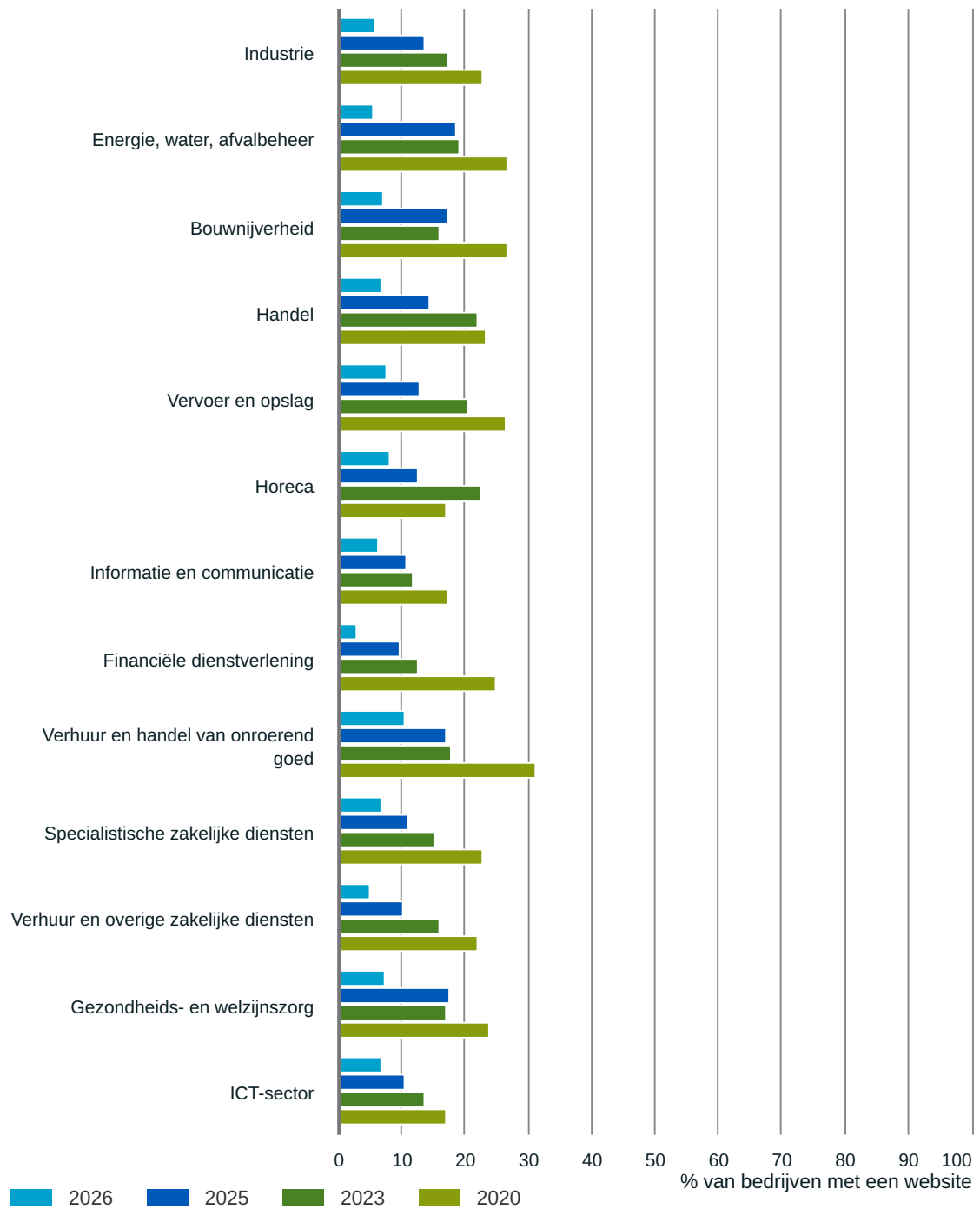
spreiding van de scores voor kleine bedrijven groter is dan voor grote bedrijven: kleine bedrijven hebben websites met zowel de laagste als de hoogste scores. In deze figuur is daarnaast te zien dat er ten opzichte van 2025 voor alle grootteklassen in 2026 een aanzienlijke daling is van het percentage bedrijven met een eindscore van 40 procent of minder.

In Figuur 3.20 is te zien dat het percentage van bedrijven met een eindscore van 40 procent of minder ook voor alle bedrijfstakken flink is gedaald. Bijvoorbeeld voor de bedrijfstak 'Financiële dienstverlening', waarvoor een daling te zien is van 9,8 procent in 2025 naar 2,8 procent in 2026. Daartegenover heeft de bedrijfstak 'Verhuur en handel van onroerend goed' procentueel de meeste bedrijven met een lage score: 10,6 procent van de bedrijven in deze bedrijfstak heeft een eindscore van 40 procent of minder. Dit is echter nog steeds een daling ten opzichte van 2025.

Figuur 3.19.: Bedrijven met een eindscore van 40 procent of minder voor de websitescan naar bedrijfstak



Figuur 3.20.: Bedrijven met een eindscore van 40 procent of lager voor de websitescan naar bedrijfstak (2 of meer werkzame personen)



## 4. Resultaten e-mailscans

In dit hoofdstuk worden de resultaten van de e-mailscan besproken. De e-mailscan van Internet.nl bevat vijf categorieën:

- **IPv6**: Bereikbaarheid via een modern internetadres;
- **DNSSEC**: Gebruik van een ondertekende domeinnaam;
- **Authenticiteit**: Protectie tegen e-mailphishing;
- **Beveiligd e-mailtransport (STARTTLS en DANE)**: Beveiligd e-mailtransport;
- **RPKI**: Autorisatie voor routing.<sup>1</sup>

In Paragraaf 4.1 worden eerst de gemiddelde eindscores besproken.<sup>2</sup> In Paragraaf 4.2 worden de categorieën daarna in meer detail beschreven en wordt er los ingezoomd op de resultaten per categorie. Paragraaf 4.3 en Paragraaf 4.4 tonen resultaten over de verdelingen van de eindscores. Paragraaf A.3 bevat een overzicht van alle subtesten per categorie met een korte uitleg en Tabel A.13 bevat een lijst met technische termen. De resultaten van de onderliggende testen worden getoond in Bijlage C.

### 4.1. Resultaten eindscores van de e-mailscan

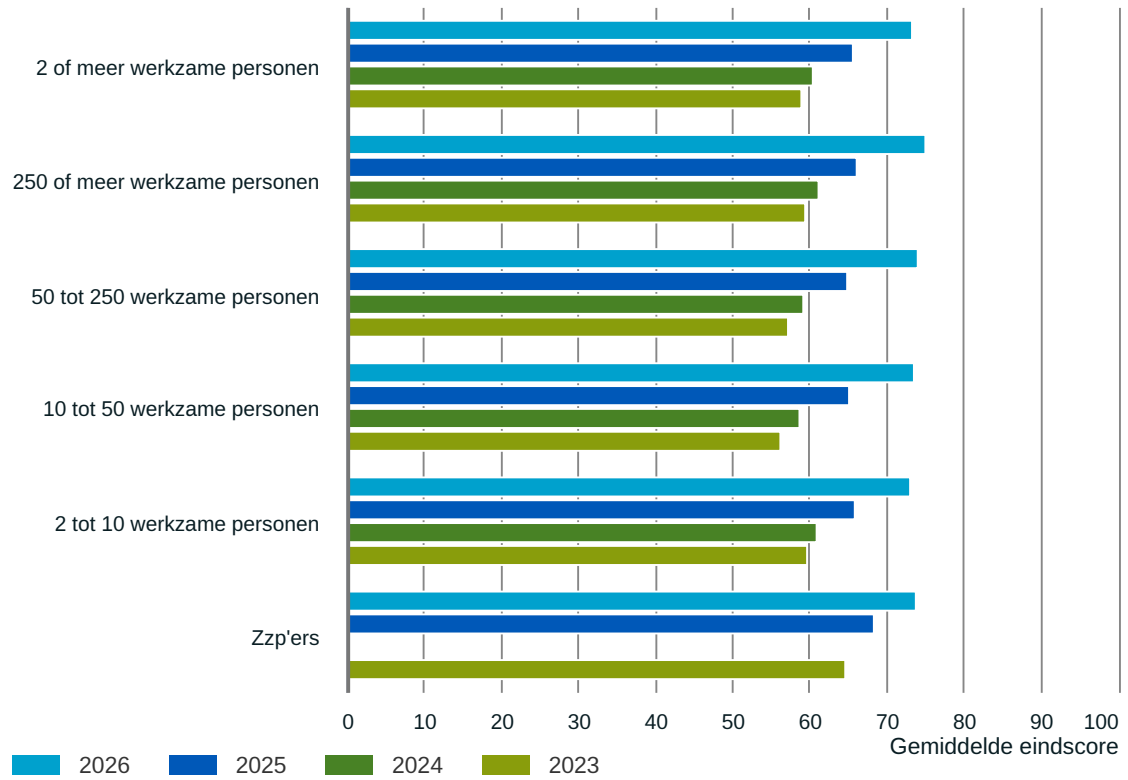
Figuur 4.1 en Figuur 4.2 tonen per bedrijfsgroottesklasse en bedrijfstak de verdeling van de gemiddelde eindscores. De gemiddelde eindscore voor alle bedrijven met een website (2 of meer werkzame personen) is gestegen van 65,7 procent in 2025 naar 73,2 procent in 2026. De verschillen tussen de bedrijfsgroottesklassen zijn daarentegen klein en blijven over de tijd heen constant. Voor de bedrijfstakken varieert de gemiddelde eindscore in 2026 van 68,4 procent voor de bedrijfstak 'Verhuur en handel van onroerend goed' tot 74,9 procent voor de bedrijfstak 'Horeca'. De grootste stijging was te zien voor de bedrijfstak 'Energie, water, afvalbeheer' met 9,7 procentpunt.

---

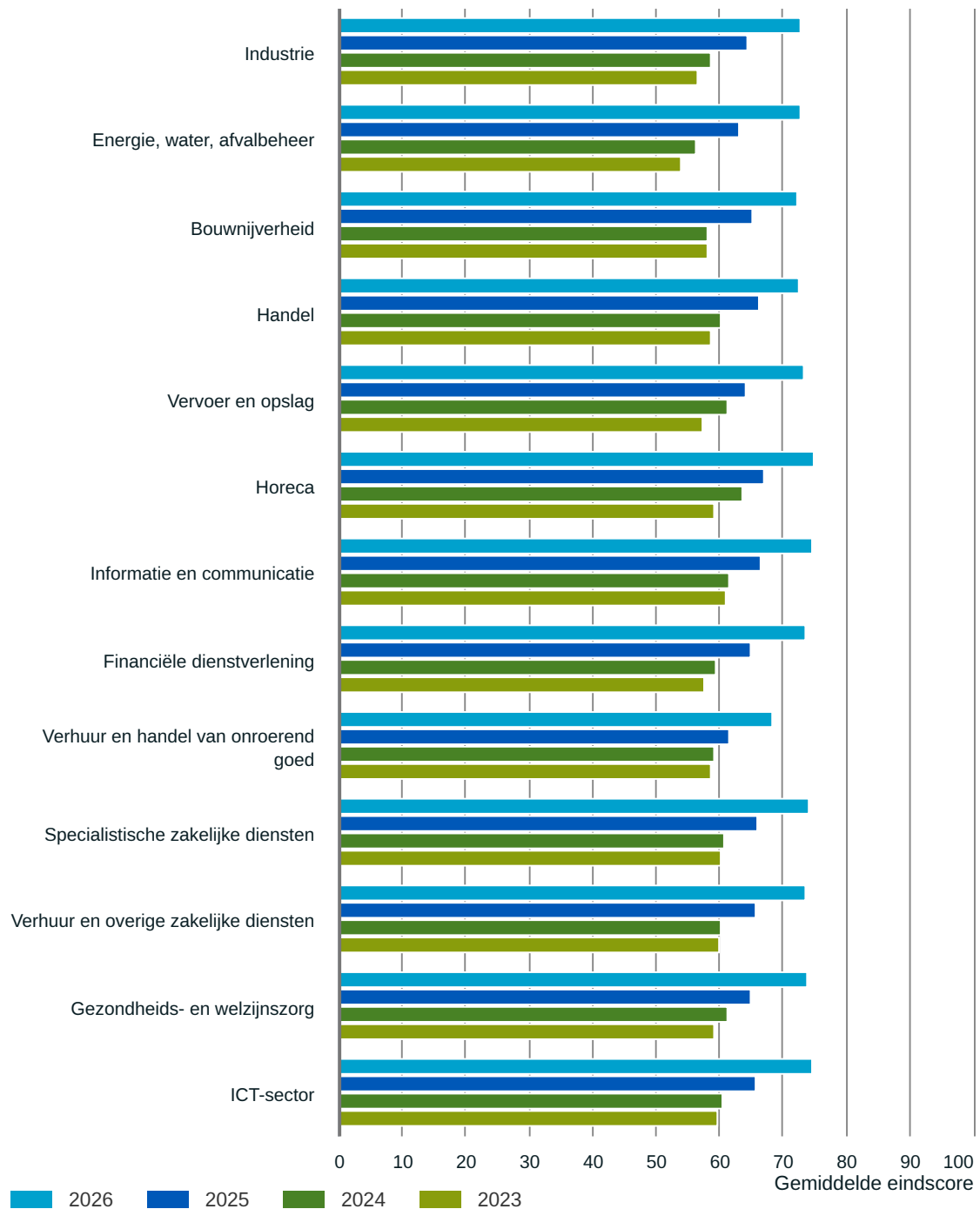
<sup>1</sup>Deze categorie is pas in 2022 toegevoegd.

<sup>2</sup>Merk op dat de resultaten voor zzp'ers voor 2024 ontbreken. Dit komt omdat in de ICT-enquête van 2023 niet aan zzp'ers is gevraagd of zij een website hebben.

Figuur 4.1.: Gemiddelde eindscore op Internet.nl voor de e-mailscan naar bedrijfsgrootteklasse



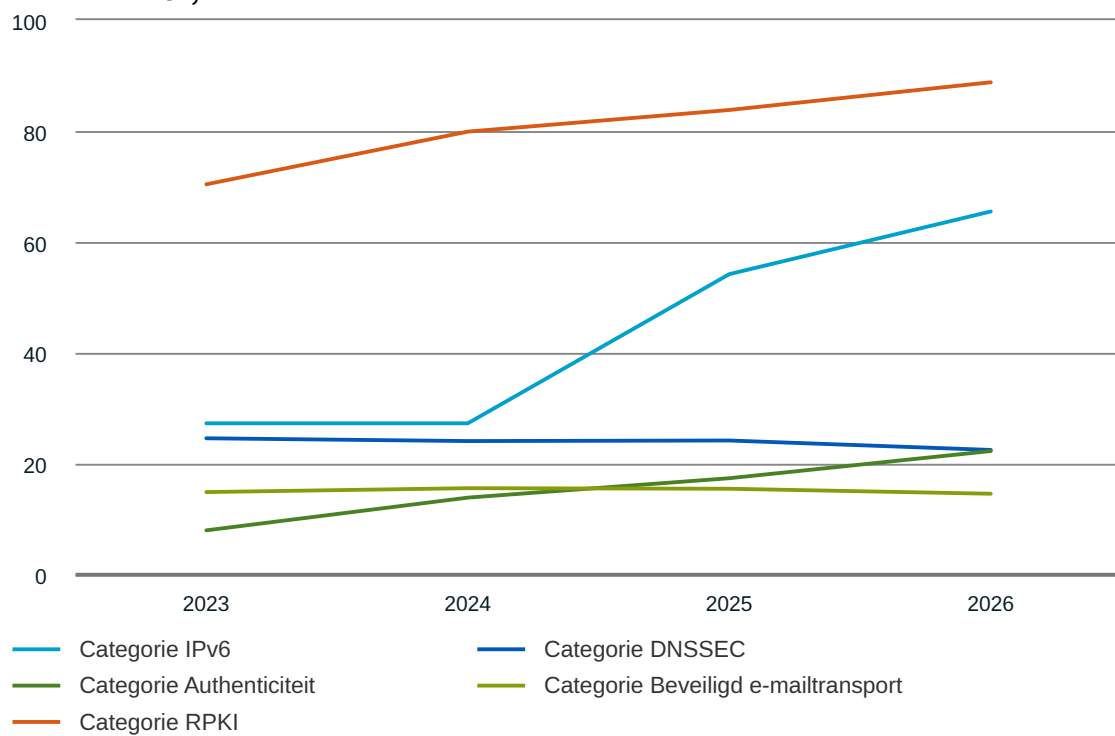
Figuur 4.2.: Gemiddelde eindscore op Internet.nl voor de e-mailscan naar bedrijfstak (2 of meer werkzame personen)



## 4.2. Resultaten e-mailscan per categorie

Figuur 4.3 toont het percentage van bedrijven met een website dat slaagt voor elk van de vijf categorieën. Het is te zien dat bedrijven in 2026 het vaakst slagen voor de categorieën RPKI (88,8 procent) en IPv6 (65,5 procent). Voor de categorie IPv6 is daarnaast een grote stijging van te zien van 38,2 procentpunt ten opzichte van 2024. Slechts een klein deel slaagt voor de categorieën Authenticiteit (22,3 procent), Beveiligd e-mailtransport (14,6 procent) en DNSSEC (22,5 procent). Voor de laatste twee categorieën is zelfs een kleine daling te zien ten opzichte van 2025.

Figuur 4.3.: Bedrijven die slagen voor de e-mailscan naar categorie (2 of meer werkzame personen)



In de rest van deze paragraaf wordt voor elk van de vijf categorieën het percentage van geslaagde bedrijven per bedrijfsgroottesklasse en bedrijfstak besproken (zie Figuur 4.4 t/m Figuur 4.13). Hoewel de eindscores niet veel variëren per bedrijfsgroottesklasse en bedrijfstak, zijn hier wel aanzienlijke verschillen per categorie te zien. Deze verschillen worden hieronder besproken en waar nodig naar de belangrijkste subtesten verwezen. De uitkomsten van alle onderliggende testten worden in Bijlage C gegeven.

#### 4.2.1. Categorie IPv6

De categorie IPv6 test in hoeverre een e-mailserver bereikbaar is via een IP-adres van het type IPv6 (zie ook Paragraaf 3.2.1). Hierin is duidelijk te zien dat de IPv6-adoptie voor e-mailservers sinds 2024 erg is toegenomen. Figuur 4.4 toont dat kleinere bedrijven tot en met vorig jaar beter scoorden dan grotere bedrijven. Opvallend is wel dat dit patroon voor 2026 minder duidelijk zichtbaar is. Voor grotere bedrijven is het percentage van bedrijven dat slaagt sterker gestegen dan voor kleinere bedrijven. In 2025 slaagden zzp'ers daarnaast het vaakst van alle bedrijfsgroottesklassen (59,1 procent), terwijl zij in 2026 juist het minst vaak slagen (59,3 procent).

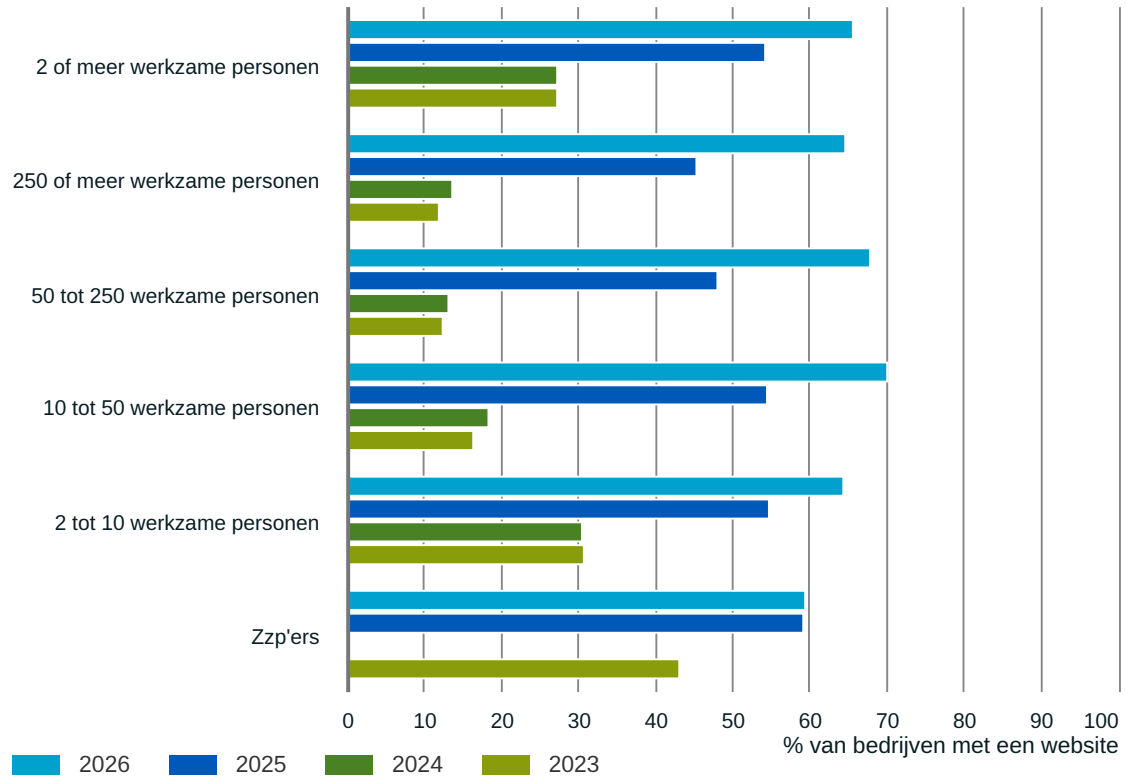
Figuur C.1 t/m Figuur C.8 laten zien dat dit voornamelijk komt door een verandering in de uitslag voor de subtesten 'IPv6-adressen voor mailservers' en 'IPv6-bereikbaarheid voor mailservers'. Het percentage van bedrijven dat slaagt is voor deze subtesten sterker gestegen voor grotere bedrijven dan voor kleinere bedrijven. Voor de subtesten 'IPv6-adressen voor nameservers' en 'IPv6-bereikbaarheid voor nameservers' slaagden grotere bedrijven in eerdere jaren al vaker dan kleinere bedrijven. Dit patroon is ook in 2026 weer terug te zien.

De resultaten naar bedrijfstak in Figuur 4.5 laten zien dat de bedrijfstak 'Informatie en communicatie' in 2026 de best scorende bedrijfstak is (73,4 procent). De bedrijfstak 'Verhuur en

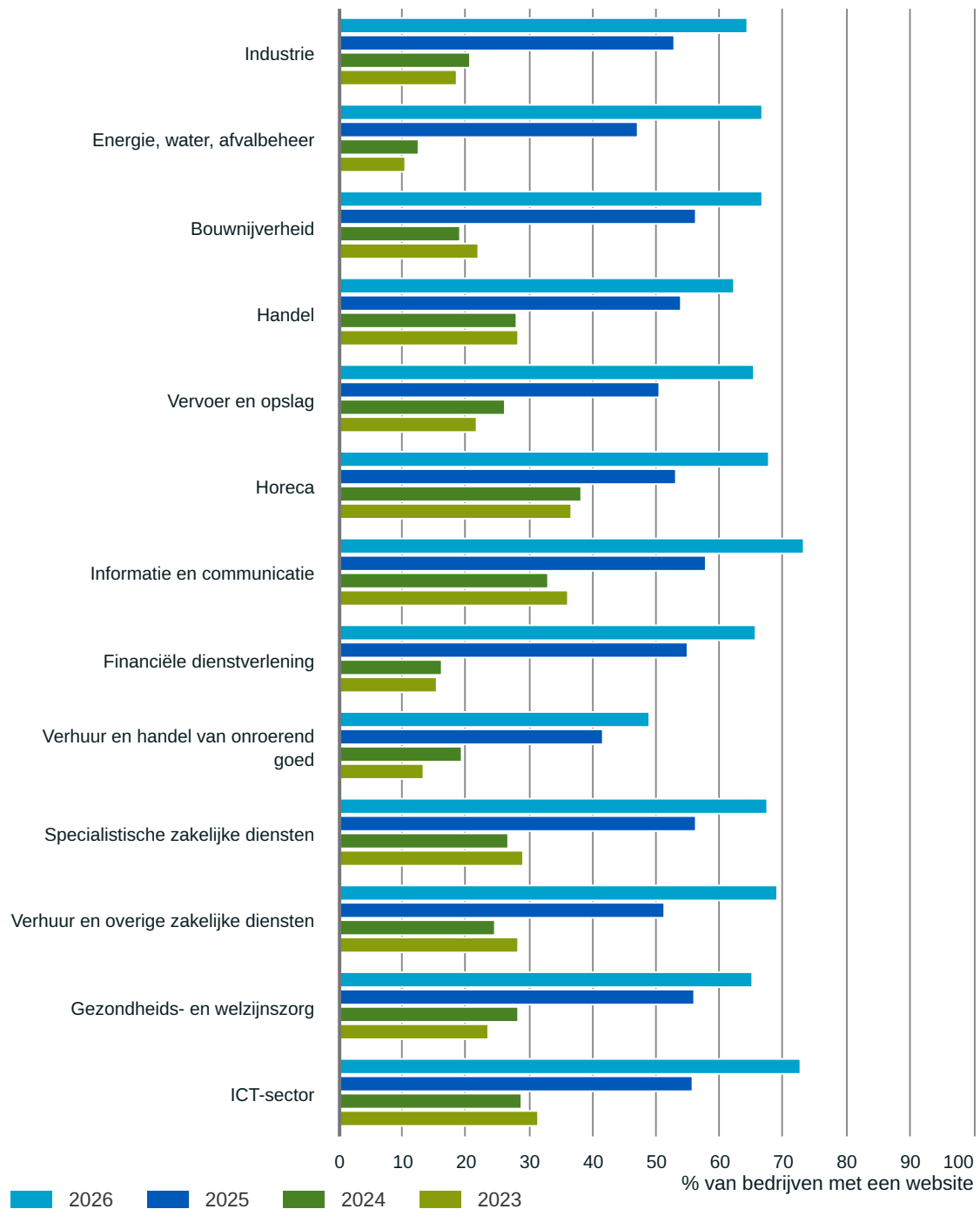
handel van onroerend goed' heeft met 49,0 procent de laagste eindscore. Toch worden in alle bedrijfstakken in 2026 aanzienlijk hogere eindscores behaald dan een jaar eerder.

Opvallend is dat de grote stijging in IPv6-adoptie die te zien is bij de e-mailscan niet in even grote mate terug te zien is bij de geteste websites (zie Figuur 3.4 en Figuur 3.5).

Figuur 4.4.: Bedrijven met geslaagde categorie 'IPv6' naar bedrijfsgrootteklasse



Figuur 4.5.: Bedrijven met geslaagde categorie 'IPv6' naar bedrijfstak (2 of meer werkzame personen)



#### 4.2.2. Categorie DNSSEC

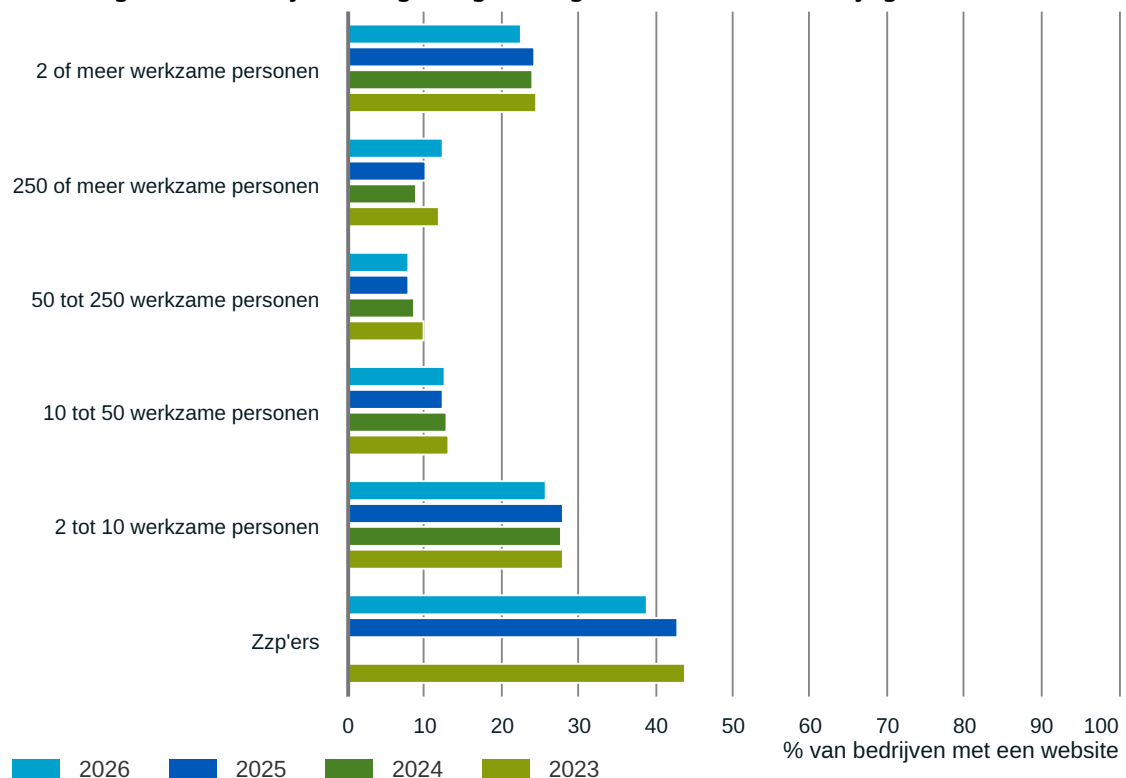
De categorie DNSSEC test of het e-maildomein met een geldige handtekening ondertekend is (zie Paragraaf 3.2.2). Figuur 4.6 laat zien dat zzp'ers met een website in 2026 met 38,8 procent het vaakst slagen voor deze categorie, gevolgd door kleine bedrijven (2 tot 10 werkzame personen) (25,7 procent). Middelgrote bedrijven (50 tot 250 werkzame personen) zitten daar behoorlijk onder: 8,0 procent van deze groep slaagt in 2026 voor de categorie DNSSEC. Vergeleken met vorig jaar is er een kleine daling te zien van het percentage van bedrijven met een website dat slaagt

voor deze categorie. Vooral het percentage voor kleine bedrijven is licht gedaald van 27,9 procent in 2025 naar 25,7 procent in 2026. Ook voor zzp'ers is er een kleine daling te zien van 42,7 procent in 2025 naar 38,8 procent in 2026. Voor de overige bedrijfsgrootteklassen is er wel sprake van een kleine stijging ten opzichte van 2025. Het patroon dat kleine bedrijven en zzp'ers een lagere score behalen in 2026 dan in 2025, terwijl de overige bedrijfsgrootteklassen juist een kleine stijging vertonen, is terug te zien in de resultaten van alle subtesten (zie Paragraaf C.2).

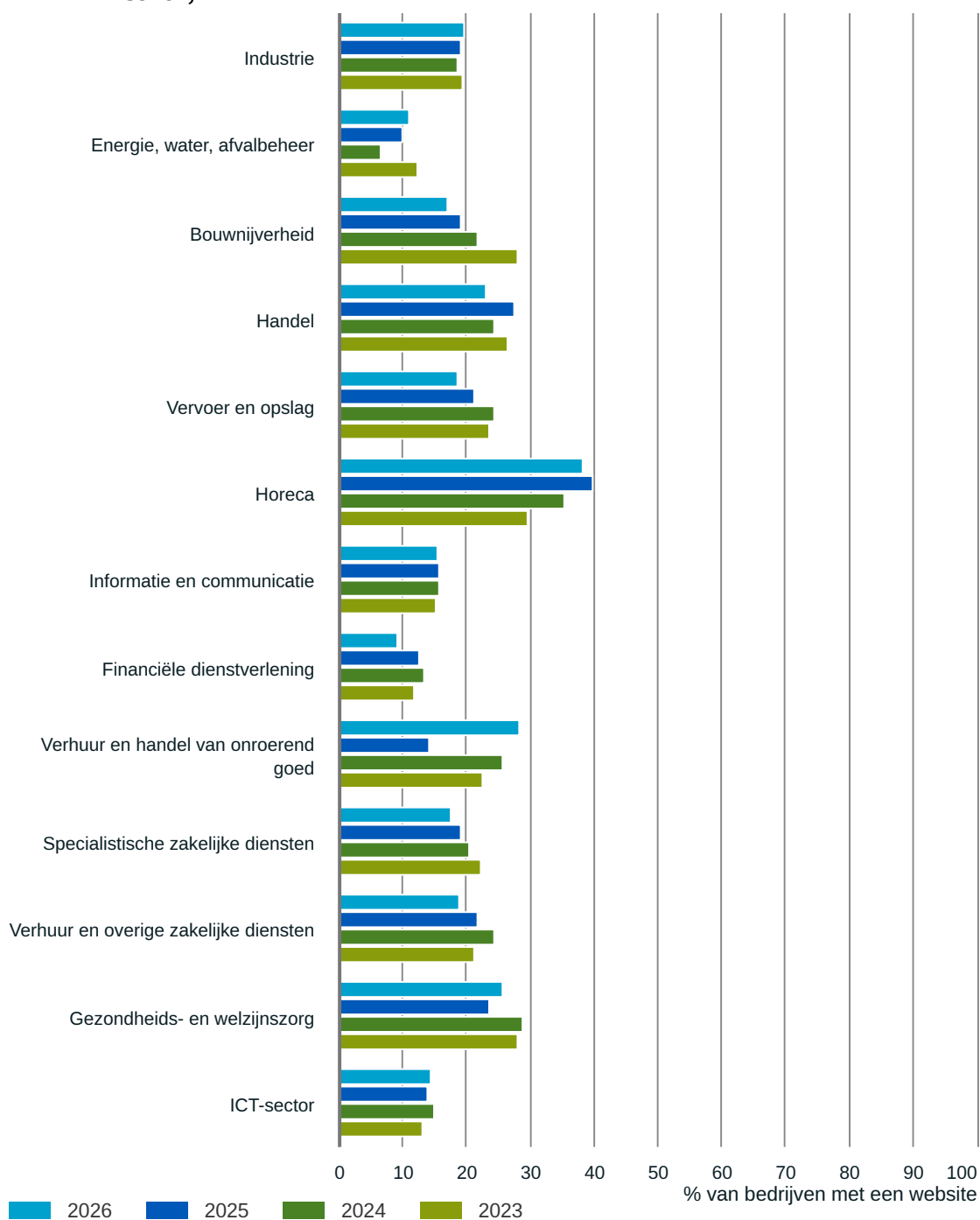
De uitsplitsingen naar bedrijfstak laten zien dat bedrijven uit de bedrijfstak 'Horeca' in 2026 het vaakst slagen voor deze categorie (38,3 procent) (zie Figuur 4.7). In de bedrijfstak 'Financiële dienstverlening' wordt het laagst gescoord: slechts 9,1 procent van de bedrijven in deze bedrijfstak slaagt voor de categorie DNSSEC. Opvallend is dat deze bedrijfstak voor dezelfde categorie in de websitescan juist hoog scoort vergeleken met andere bedrijfstakken (zie Paragraaf 3.2.2). Ook voor de verdeling naar grootteklasse zijn relatief veel verschillen te zien tussen de websitescan en de e-mailscan voor deze categorie. Als een bedrijf DNSSEC op orde heeft voor het webdomein, wil dat dus niet direct zeggen dat DNSSEC ook op orde is voor het e-maildomein (en vice versa).

De categorie DNSSEC wordt bepaald door vier onderliggende testen. Over het algemeen wordt voornamelijk laag gescoord op de aanwezigheid en geldigheid van DNSSEC voor het e-mailserverdomein. Van de verschillende bedrijfsgrootteklassen slagen zzp'ers het vaakst voor deze twee subtesten (44,0 procent) in 2026 (zie Figuur C.13 en Figuur C.15). Voor de aanwezigheid en geldigheid van DNSSEC voor het e-mailadresdomein wordt wat hoger gescoord. Zo slaagt 54,9 procent van de zzp'ers voor deze twee subtesten in 2026 (zie Figuur C.9 en Figuur C.11).

Figuur 4.6.: Bedrijven met geslaagde categorie 'DNSSEC' naar bedrijfsgrootteklasse



Figuur 4.7.: Bedrijven met geslaagde categorie 'DNSSEC' naar bedrijfstak (2 of meer werkzame personen)



### 4.2.3. Categorie Authenticiteit

Bij de categorie Authenticiteit wordt gekeken in hoeverre bedrijven de juiste authenticatiemechanismes toepassen, zoals DMARC (Domain-based Message Authentication, Reporting & Conformance), DKIM (DomainKeys Identified Mail) en SPF (Sender Policy Framework). Deze protocollen gaan phishing, spam, virussen en andere malware tegen door de authenticiteit van een e-mailbericht te waarborgen [SIDN, 2026]. Zo voorziet DKIM elk uitgaand bericht van een digitale handtekening. De publieke sleutel wordt via DNS gepubliceerd (zie ook Paragraaf 3.2.2),

zodat een ontvanger de digitale handtekening kan verifiëren. Op deze manier wordt voorkomen dat kwaadwillenden een bericht namens een ander kunnen verzenden of de inhoud van een bericht onderweg kunnen veranderen.

Voor de categorie Authenticiteit, getoond in Figuur 4.8, slaagt 22,3 procent van alle bedrijven met een website in 2026. Er is hierbij een groot verschil tussen de scores voor kleine en grote bedrijven. Zo slaagt slechts 19,6 procent van de kleine bedrijven, tegenover 59,4 procent van de grote bedrijven (250 of meer werkzame personen). Voor elk van de bedrijfsgrootteklassen is wel een stijging te zien ten opzichte van een jaar eerder. Dat grote bedrijven beter scoren op de categorie Authenticiteit is goed te begrijpen, omdat e-mailspoofing<sup>3</sup> van grote bedrijven aantrekkelijker is voor cybercriminelen. Ze kunnen zich bijvoorbeeld per mail voordoen als een bank om het slachtoffer te overtuigen geld over te maken. Bovendien kan het voor grote bedrijven meer imagoschade tot gevolg hebben. Voor deze bedrijven is er dus veel aan gelegen om zich hier zo goed mogelijk tegen te beschermen.

De slagingspercentages per bedrijfstak getoond in Figuur 4.9 laten daarnaast een interessante omkering zien. Zo scoort de bedrijfstak 'Financiële dienstverlening' voor de categorieën IPv6 en DNSSEC relatief slecht ten opzichte van de andere bedrijfstakken, terwijl het voor de categorie Authenticiteit met 44,9 procent de beste scorende bedrijfstak is. Voor alle bedrijfstakken is wel sprake van een stijging ten opzichte van een jaar eerder.

De onderliggende subtesten van de categorie Authenticiteit worden gegeven in Paragraaf C.3. Per subtest wordt een stuk beter gescoord dan voor de hele categorie. Figuur C.17 t/m Figuur C.20 laten zien hoeveel bedrijven DMARC toepassen. Met DMARC wordt er bepaald hoe om te gaan met inkomende berichten waarvoor DKIM of SPF geen geldige validatie oplevert [SIDN, 2026]. Deze kunnen bijvoorbeeld weggegooid worden of in quarantaine worden gezet. Voor 2026 is te zien dat 64,9 procent van de bedrijven met een website DMARC heeft (zie Figuur C.17). Daarentegen heeft slechts 22,8 procent DMARC met een voldoende strikt beleid (zie Figuur C.19). Deze subtest lijkt het meest bepalend voor de categoriescore, aangezien dit de verplichte subtest is waar het slechtst op wordt gescoord. Zo hebben grote bedrijven DMARC het best op orde: 57,0 procent heeft DMARC met een voldoende strikt beleid. Daarnaast is de grote groei voor de bedrijfstakken 'Financiële dienstverlening' en 'Energie, water en afvalbeheer' ook terug te zien in de DMARC-policy-subtest (zie Figuur C.20).

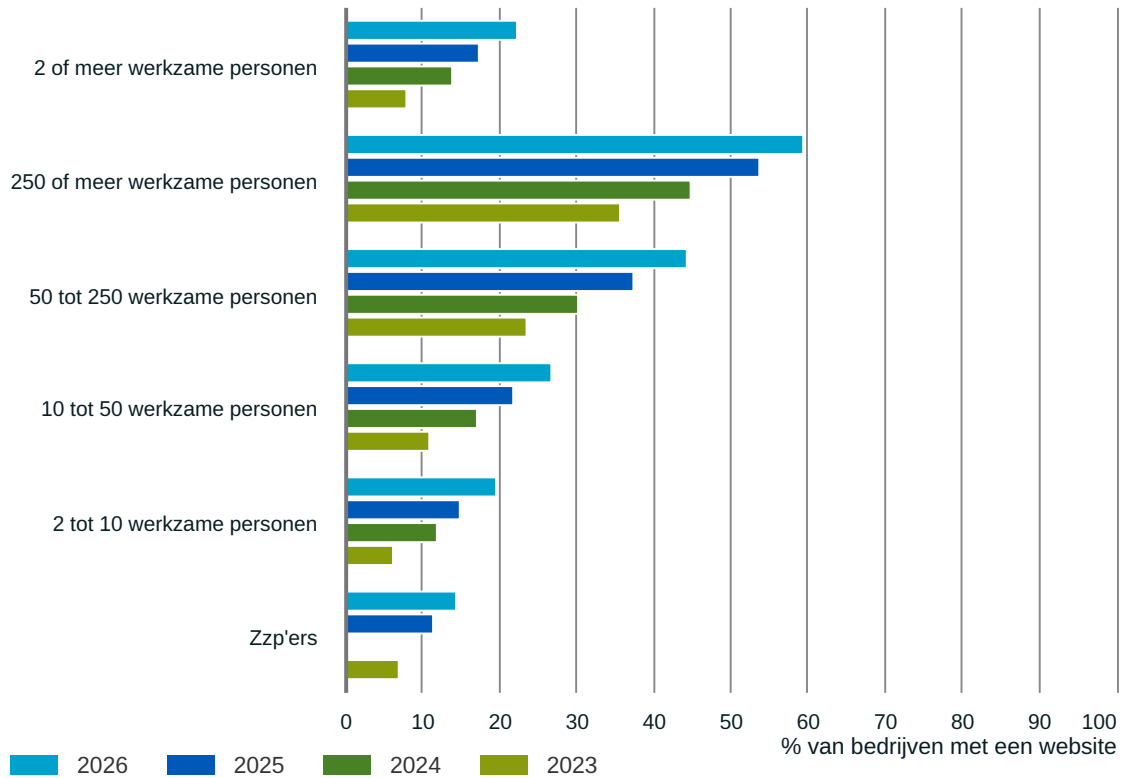
Ook DKIM wordt gebruikt om e-mails te authenticeren. Figuur C.21 laat zien dat 83,0 procent van de bedrijven met een website DKIM heeft in 2026. De verschillen tussen grote en kleine bedrijven zijn klein: Figuur C.22 laat zien dat de bedrijfstak 'Financiële dienstverlening' voorloopt met het gebruik van DKIM, alhoewel de verschillen per bedrijfstak niet groot zijn.

Tot slot laten Figuur C.23 en Figuur C.24 zien welke bedrijven SPF gebruiken. SPF voorkomt dat servers e-mailberichten accepteren van ongeautoriseerde servers [SIDN, 2026]. Hiervoor wordt een lijst van geldige adressen via het DNS gebruikt. Van de bedrijven met een website heeft 90,7 procent SPF in 2026 (zie Figuur C.23). De verschillen tussen de bedrijfsgrootteklassen zijn weer niet groot. Van de kleine bedrijven slaagt 89,1 procent voor deze test, terwijl dat voor de grote bedrijven 97,8 procent is. Figuur C.24 laat zien dat de bedrijfstak 'Financiële dienstverlening' het meest van SPF gebruikmaakt (97,1 procent). Figuur C.25 geeft aan welk deel van de bedrijven SPF ook met een voldoende strikt beleid gebruiken. Het is te zien dat 84,5 procent van de bedrijven met een website in 2026 hieraan voldoet.

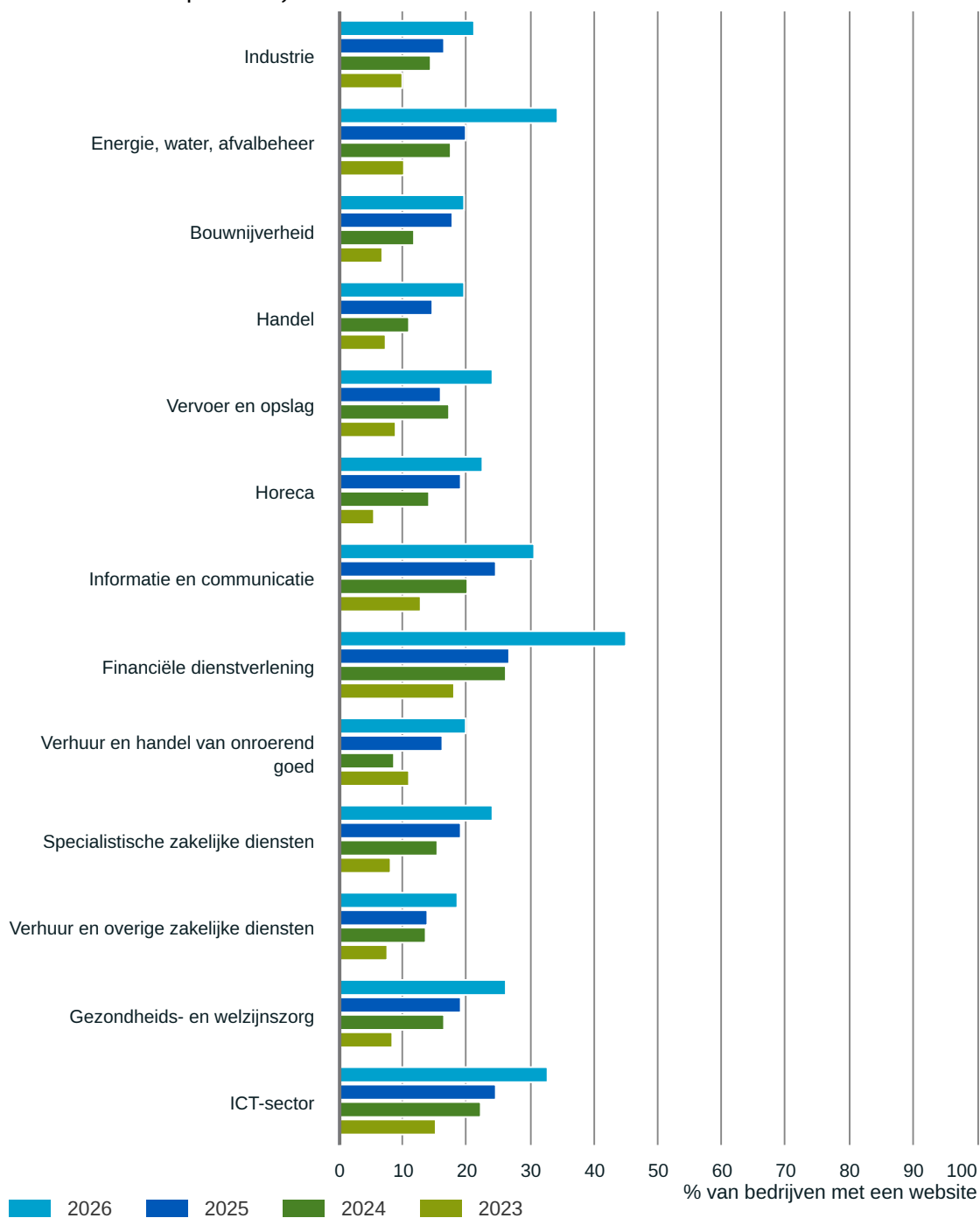
---

<sup>3</sup>E-mailspoofing is een techniek gebruikt voor spammail en phishing-aanvallen om de e-mail van de verzender te vervalsen, zodat het lijkt alsof de mail door een ander bedrijf verstuurd is.

Figuur 4.8.: Bedrijven met geslaagde categorie 'Authenticiteit' naar bedrijfsgrootteklasse



Figuur 4.9.: Bedrijven met geslaagde categorie 'Authenticiteit' naar bedrijfstak (2 of meer werkbare personen)



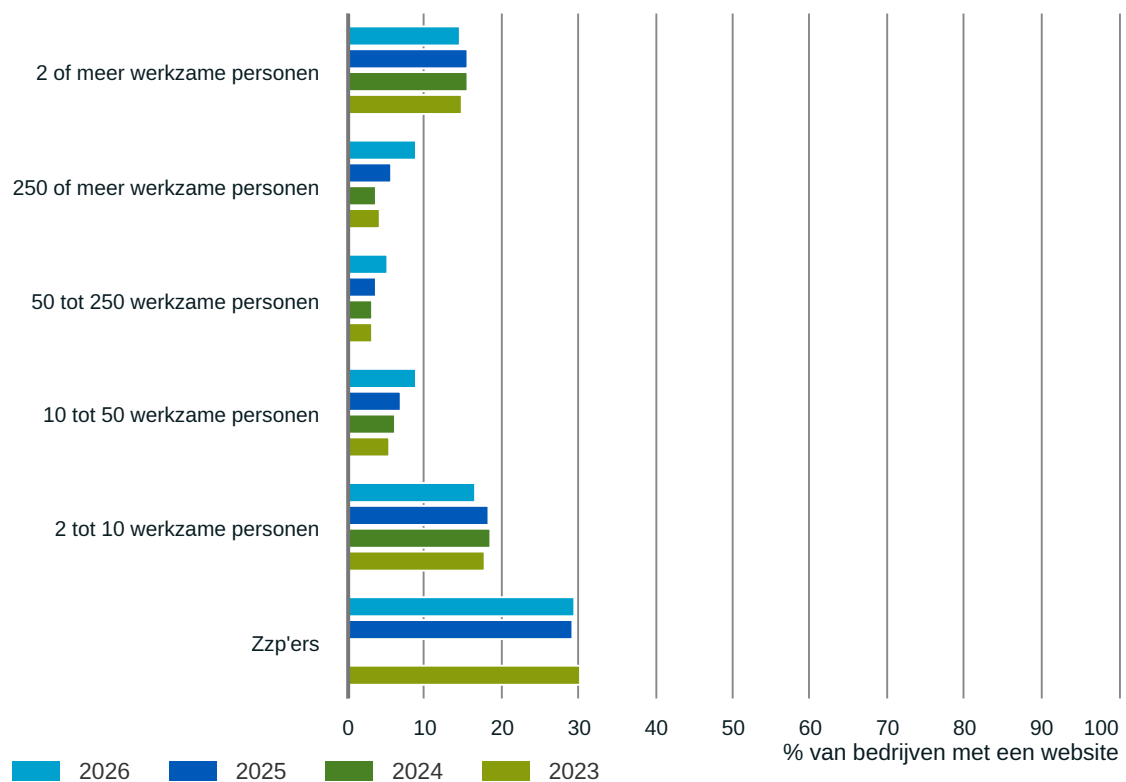
#### 4.2.4. Categorie Beveiligd e-mailtransport (STARTTLS en DANE)

Bij de categorie Beveiligd e-mailtransport wordt gekeken in hoeverre de e-mailserver een beveiligde connectie maakt met de e-mailserver van een andere partij. Zo voorkomt STARTTLS dat aanvallers mogelijk e-mails kunnen onderscheppen door het gebruik van TLS-encryptie tijdens het transport af te dwingen [SIDN, 2026]. Met DANE (DNS-based Authentication of Named Entities) wordt daarnaast bescherming geboden tegen aanvallers die proberen STARTTLS te omzeilen door het e-mailverkeer te manipuleren.

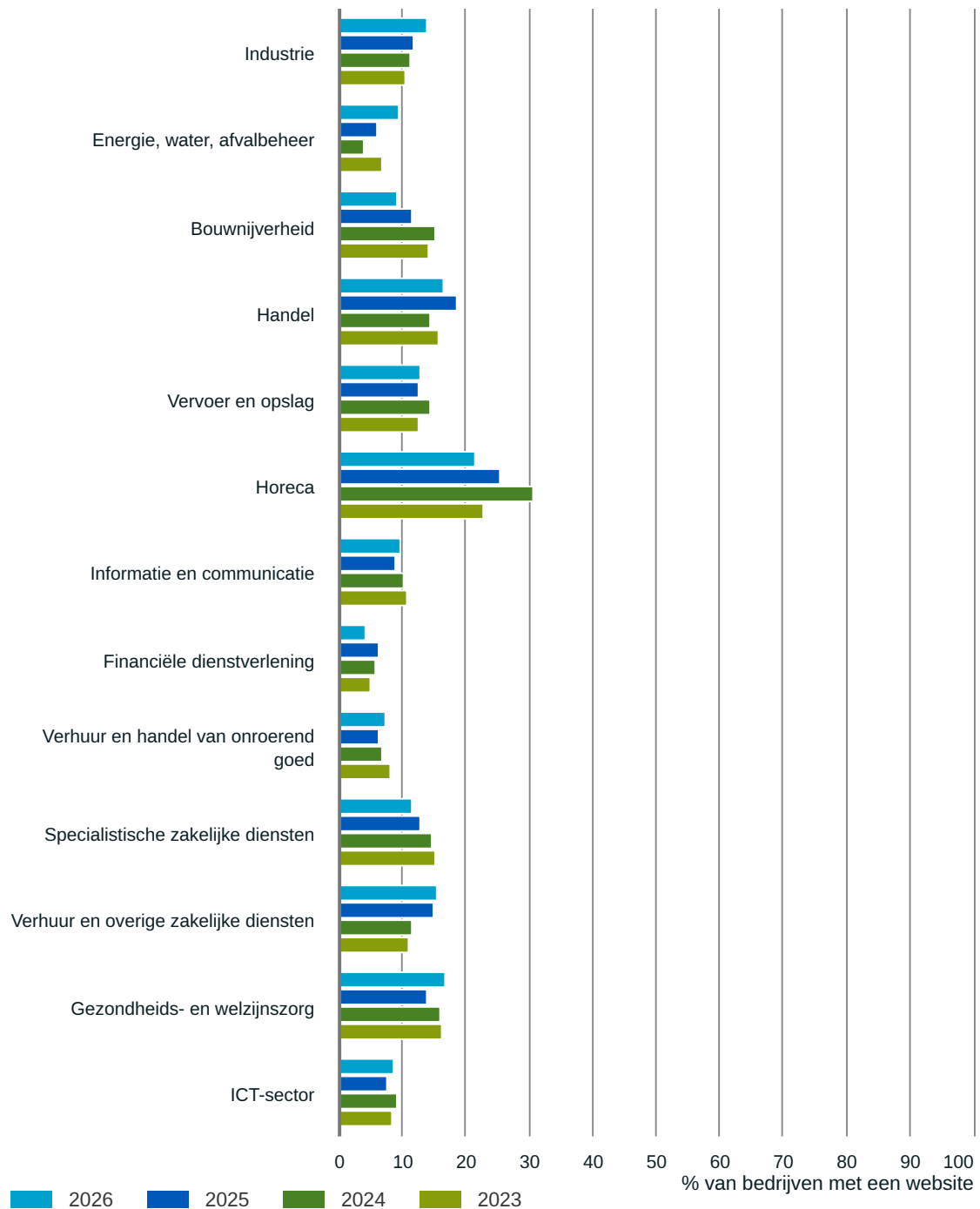
Figuur 4.10 en Figuur 4.11 tonen per bedrijfsgrootteklasse en bedrijfstak het percentage bedrijven dat slaagt voor deze categorie. Van alle bedrijven met een website slaagt 14,6 procent in 2026. Dit is een kleine daling ten opzichte van een jaar eerder (15,5 procent). Vooral het percentage voor kleine bedrijven is licht gedaald van 18,2 procent in 2025 naar 16,5 procent in 2026. Voor de overige bedrijfsgrootteklassen is er wel sprake van een kleine stijging ten opzichte van 2025. Vergeleken met de andere bedrijfsgrootteklassen scoren zzp'ers het best met een slagingspercentage van 29,5 procent voor deze categorie. Van de middelgrote bedrijven slaagt slechts 5,2 procent.

De onderliggende subtesten van deze categorie worden in Paragraaf C.4 gegeven. De lage scores worden voornamelijk veroorzaakt door de testen op DANE ('DANE aanwezig', 'DANE geldig' en 'DANE-ervangingschema'). Figuur C.57 laat bijvoorbeeld zien dat maar 15,2 procent van de bedrijven slaagt voor de test 'DANE aanwezig'. Voor bedrijven met 50 tot 250 werkzame personen is dit zelfs slechts 5,7 procent. Voor de andere subtesten wordt een stuk beter gescoord (zie Figuur C.27 t/m Figuur C.56).

Figuur 4.10.: Bedrijven met geslaagde categorie 'Beveiligd e-mailtransport' naar bedrijfsgrootteklasse



Figuur 4.11.: Bedrijven met geslaagde categorie 'Beveiligd e-mailtransport' naar bedrijfstak (2 of meer werkzame personen)

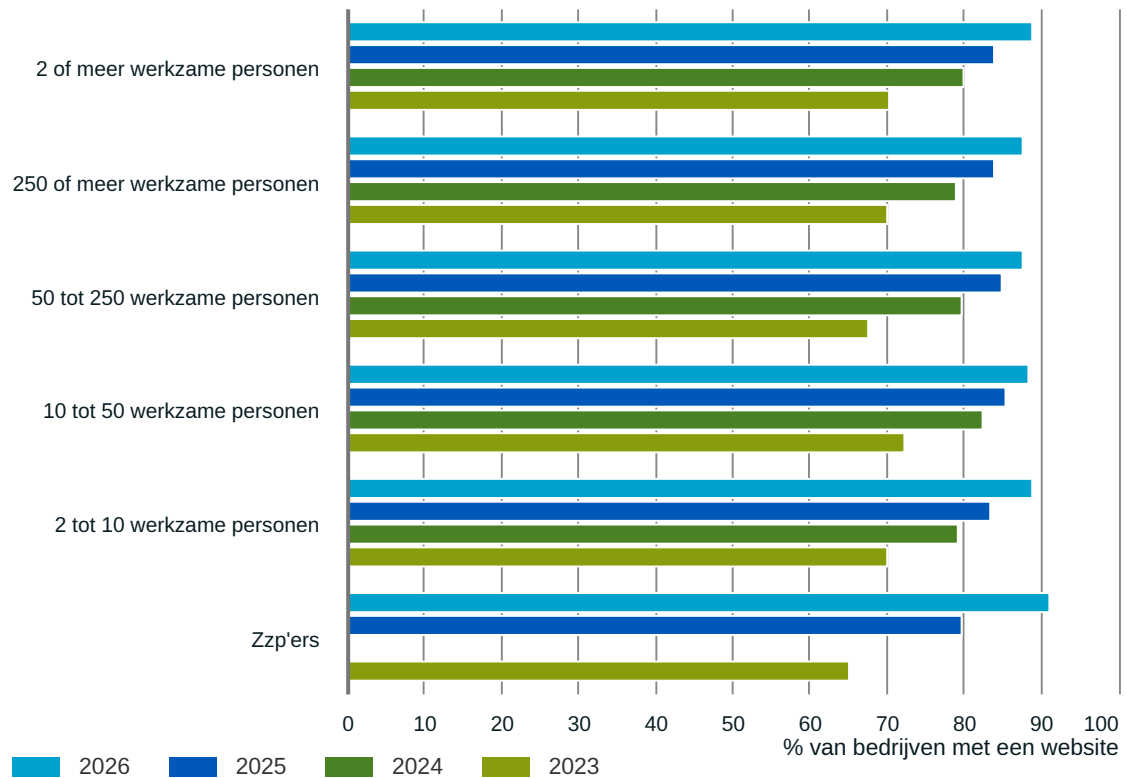


#### 4.2.5. Categorie Autorisatie voor Routing (RPKI)

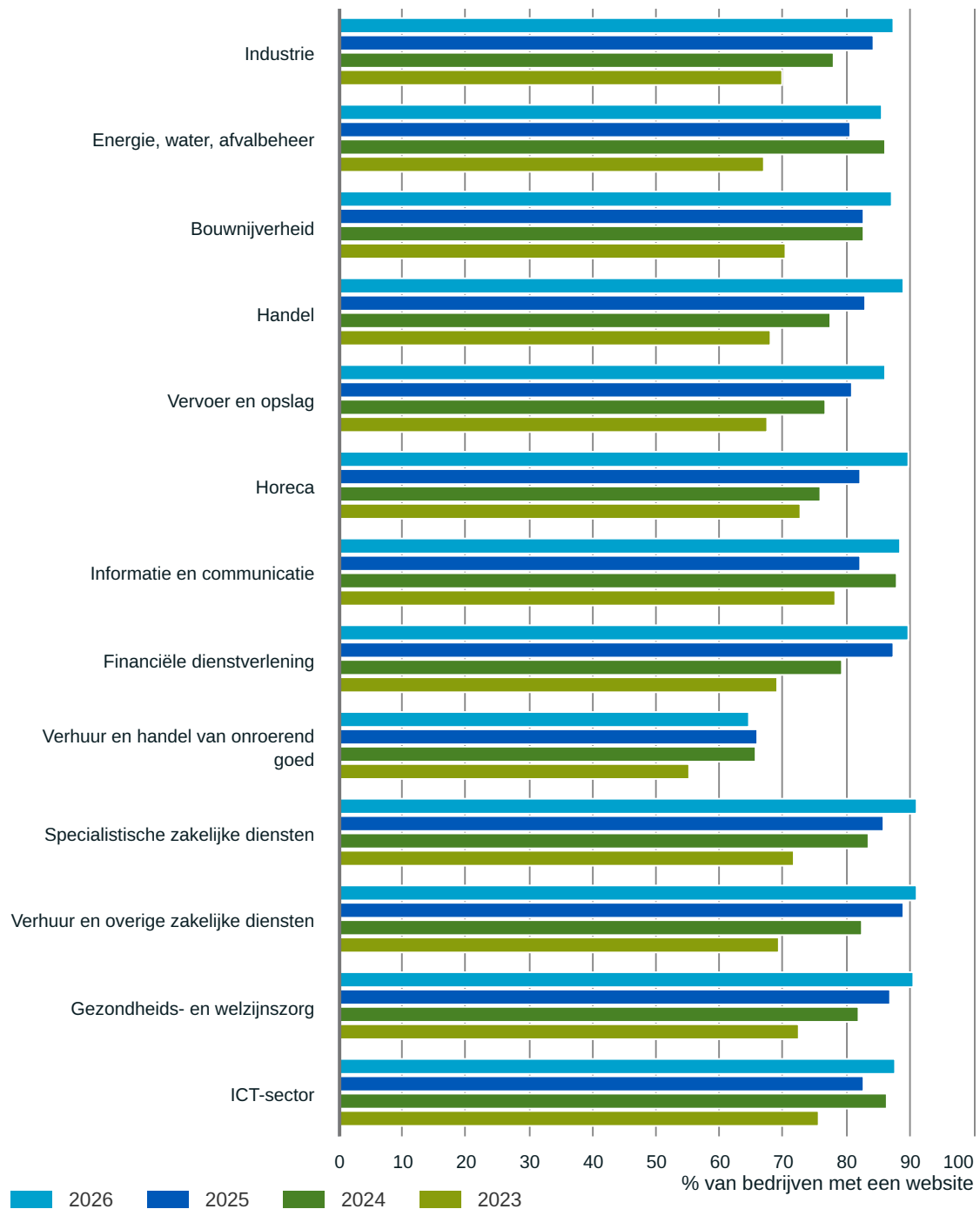
Als laatste wordt naar de categorie RPKI gekeken in Figuur 4.12 en Figuur 4.13. In deze categorie wordt onderzocht of een website een route-aankondiging heeft die kan worden gematcht aan de gepubliceerde route-autorisatie (RPKI) (zie ook Paragraaf 3.2.5). Net als bij de websitescan wordt er op deze categorie duidelijk het best gescoord. Van alle bedrijven met een website slaagt 88,8 procent in 2026. Tussen de verschillende bedrijfsgrootteklassen en bedrijfstakken zijn weinig verschillen te zien: bijna overal is een stijging te zien in de afgelopen jaren. Alleen de bedrijfstak

'Verhuur en handel van onroerend goed' heeft met 64,6 procent een aanzienlijk lagere score dan de andere bedrijfstakken. Ook in de voorgaande jaren scoort deze bedrijfstak afwijkend op de categorie RPKI. Tot slot zijn ook tussen de verschillende subtesten weinig verschillen te zien in de resultaten.

Figuur 4.12.: Bedrijven met geslaagde categorie 'RPKI' naar bedrijfsgrootteklasse



Figuur 4.13.: Bedrijven met geslaagde categorie 'RPKI' naar bedrijfstak (2 of meer werkzame personen)



### 4.3. Verdelingen van de eindscores van de e-mailscan

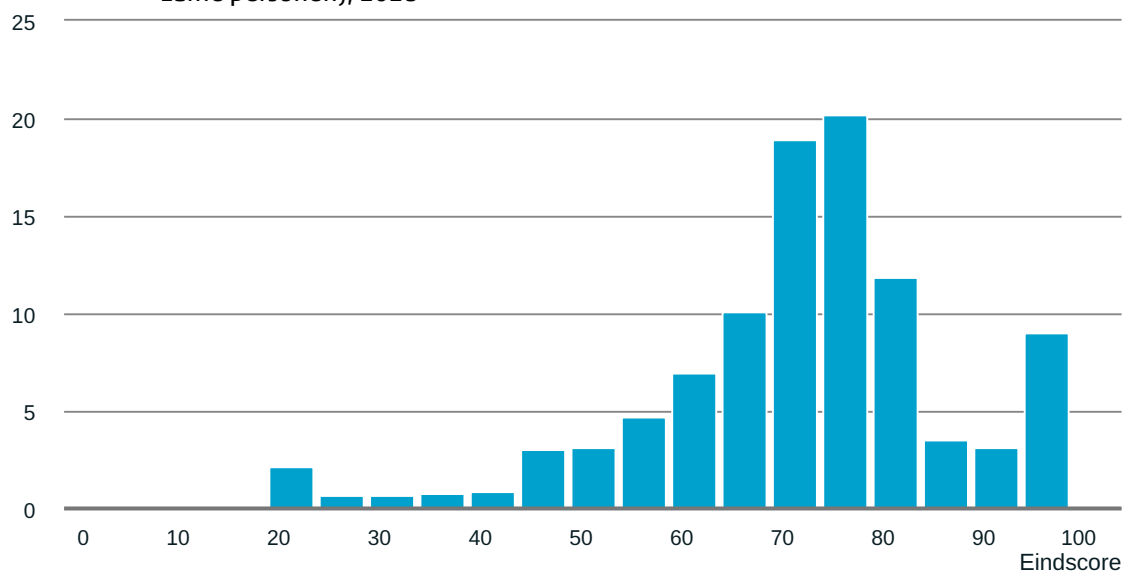
In 2026 ligt de gemiddelde eindscore rond de 73 procent voor alle bedrijven met een website (2 of meer werkzame personen). In deze paragraaf wordt gekeken naar de spreiding van deze eindscores.

De verdeling van de eindscores van de e-mailscan in januari 2026 wordt in Figuur 4.14 getoond voor alle bedrijven met een website. In Tabel 4.1 zijn daarnaast de drie kwartielen weergegeven.

De verdeling van de overige jaren wordt in Paragraaf C.6 gegeven.

Voor 2026 is er een duidelijke piek te zien rond de gemiddelde eindscore van 73 procent. Een tweede piek is te zien voor bedrijven met een hoge eindscore tussen de 95 en 100 procent. Over de jaren zijn de kwartielen aanzienlijk omhooggeschoven. Waar in 2024 nog 25 procent van de gehele populatie een eindscore had onder de 50 procent, heeft in 2026 25 procent van de gehele populatie een eindscore onder de 67 procent. Kortom, er zijn in 2026 minder bedrijven met een lage eindscore. Evenzo zijn de overige kwartielen, en daarmee de gehele distributie, verschoven naar hogere eindscores.

Figuur 4.14.: Verdeling eindscores e-mailscan voor bedrijven met een website (2 of meer werkzame personen), 2026



Tabel 4.1.: Percentielen eindscores e-mailscan voor bedrijven met een website (2 of meer werkzame personen)

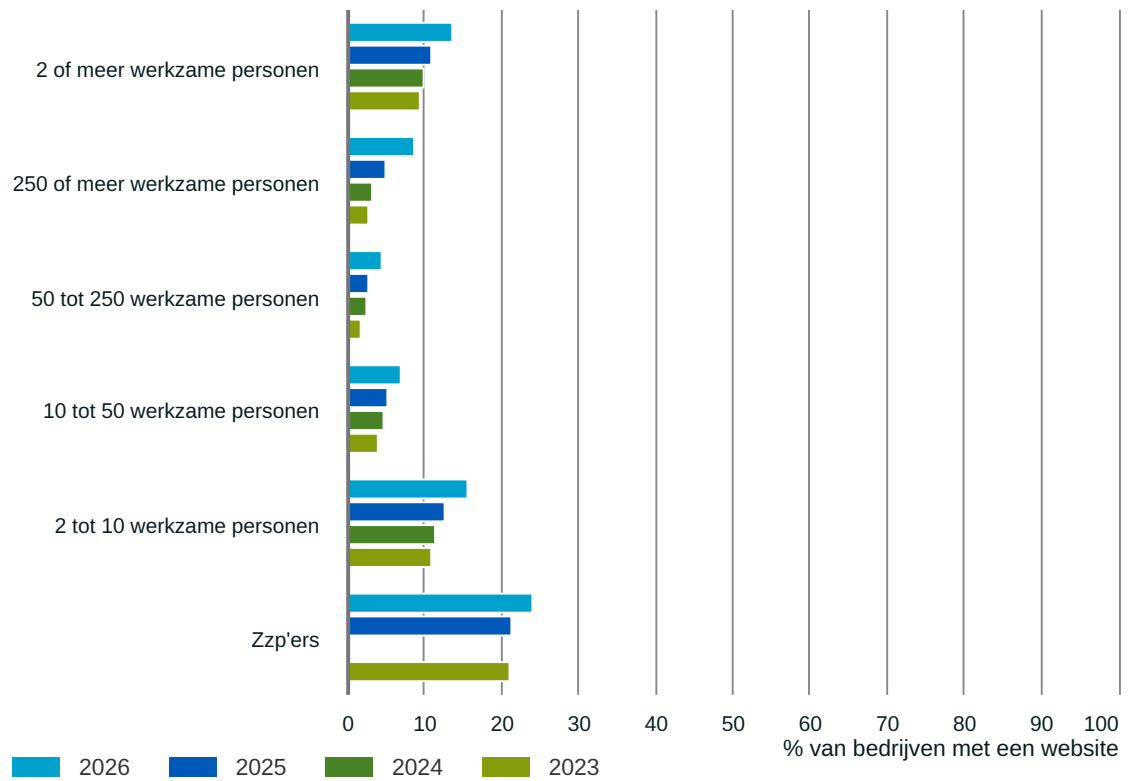
Percentiel	2023	2024	2025	2026
25	50	50	55	67
50 (mediaan)	55	61	67	74
75	67	69	75	82

#### 4.4. Welke bedrijven hebben de hoogste en laagste eindscore voor de e-mailscan?

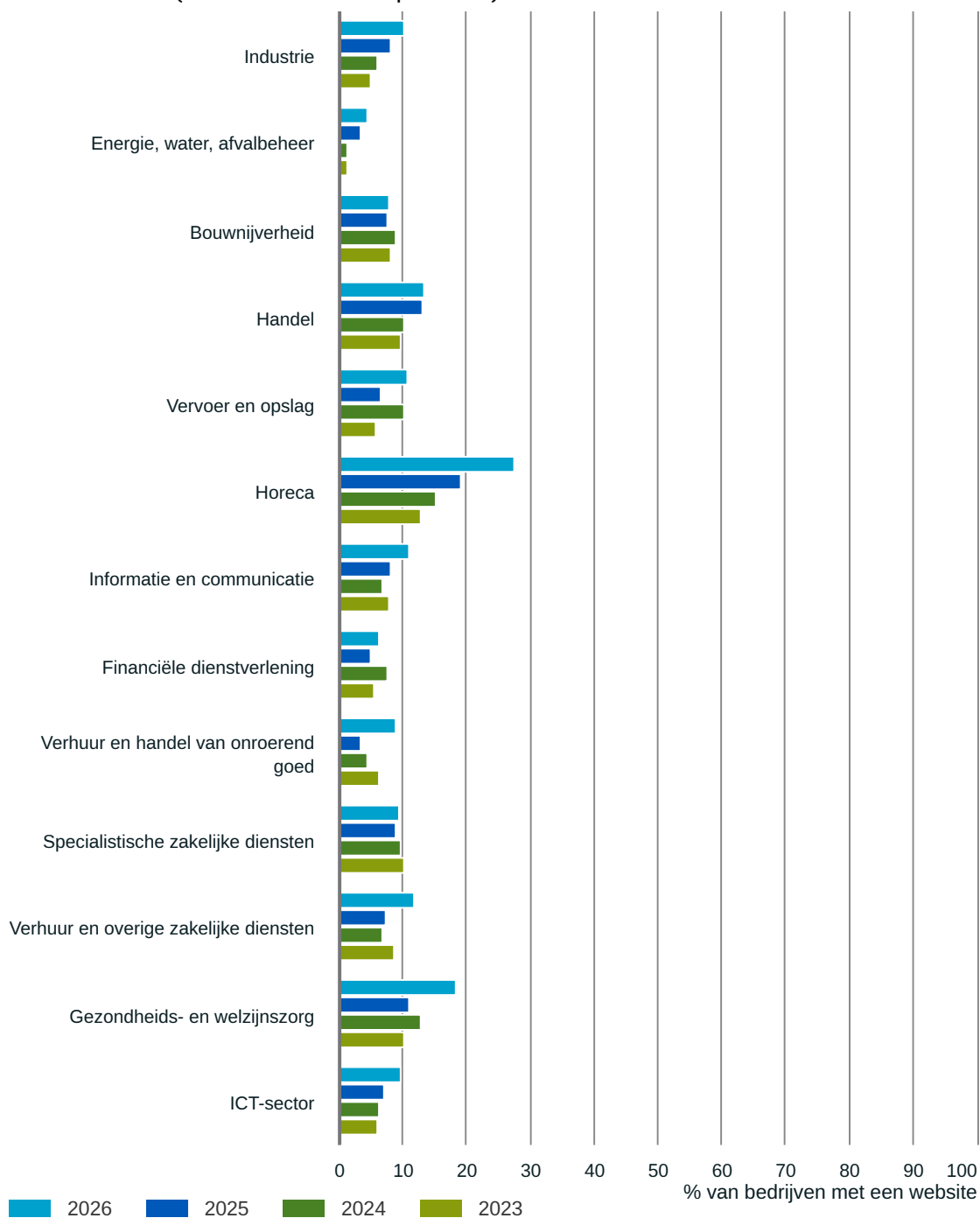
In Figuur 4.15 en Figuur 4.16 worden de bedrijven met de hoogste eindscores voor de e-mailscan per bedrijfsgrootteklasse en bedrijfstak weergegeven. Net als bij de websitescan is weer te zien dat kleine bedrijven vaker een eindscore van 90 procent of hoger halen dan grotere bedrijven. Bijna 24 procent van de zzp'ers haalt in 2026 bijvoorbeeld een eindscore van 90 procent of meer, terwijl dat voor bedrijven met 250 of meer werkzame personen slechts 8,6 procent is. Hoewel voor alle bedrijfsgrootteklassen een stijging te zien is ten opzichte van vorig jaar, is voor bedrijven met 250 of meer werkzame personen met 3,7 procentpunt ten opzichte van 2025 wel de grootste stijging te zien. De verdeling over de bedrijfstakken laat zien dat bedrijven in de bedrijfstak

'Horeca' het vaakst een eindscore van 90 of hoger behalen (27,6 procent). In deze bedrijfstak is ook de grootste stijging te zien ten opzichte van vorig jaar (8,5 procentpunt).

Figuur 4.15.: Bedrijven met een eindscore van 90 procent of hoger voor de e-mailscan naar bedrijfs-grootteklasse

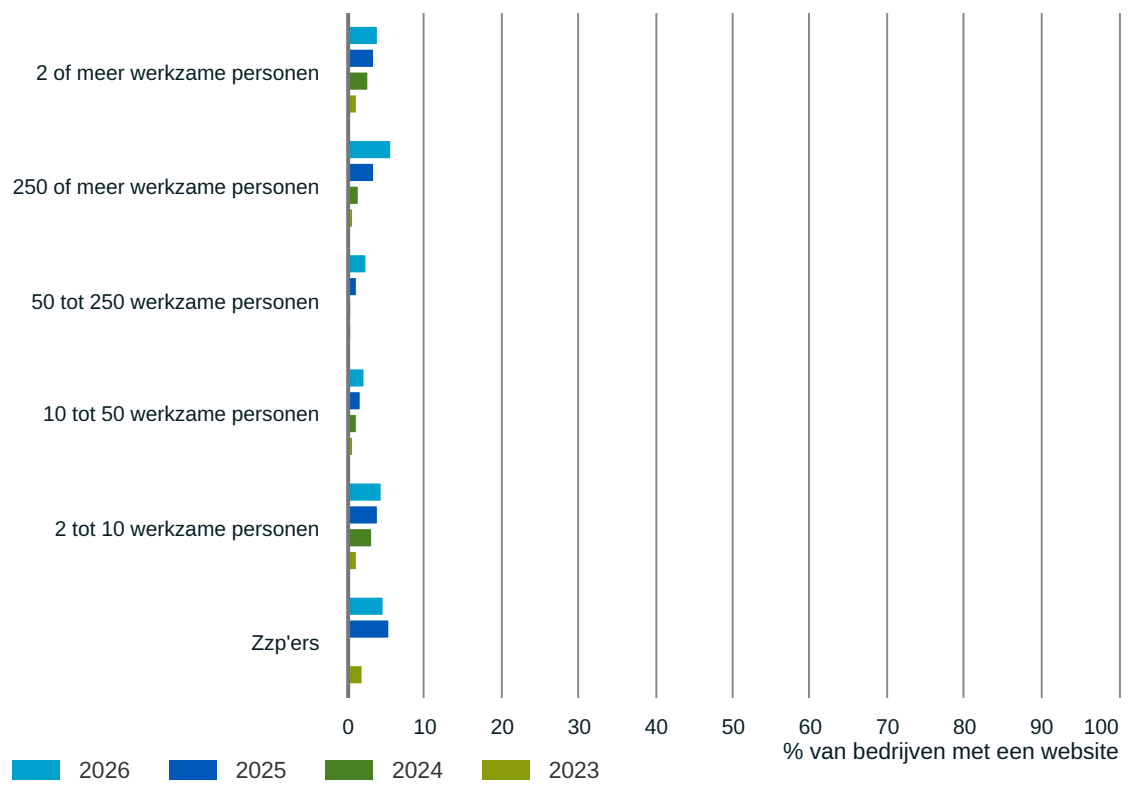


Figuur 4.16.: Bedrijven met een eindscore van 90 procent of hogervoor de e-mailscan naar bedrijfstak (2 of meer werkzame personen)



In Figuur 4.17 en Figuur 4.18 wordt gekeken naar het percentage van bedrijven dat een eindscore van 100 procent haalt. Hoewel voor alle bedrijfsgroottes een kleine stijging te zien is ten opzichte van vorig jaar, halen nog maar weinig bedrijven een 100 procent score. In totaal behaalt 4,0 procent van de bedrijven met een website in 2026 een eindscore van 100 procent. Waar vorig jaar de zzp'ers het met 5,5 procent het best deden van alle bedrijfsgroottes, scoren de grote bedrijven nu met 5,7 procent het best. Van alle bedrijfstakken wordt in de bedrijfstak 'Horeca' het vaakst een 100 procent score behaald (11,3 procent).

Figuur 4.17.: Bedrijven met een eindscore van 100 procent voor de e-mailscan naar bedrijfsgrootteklasse

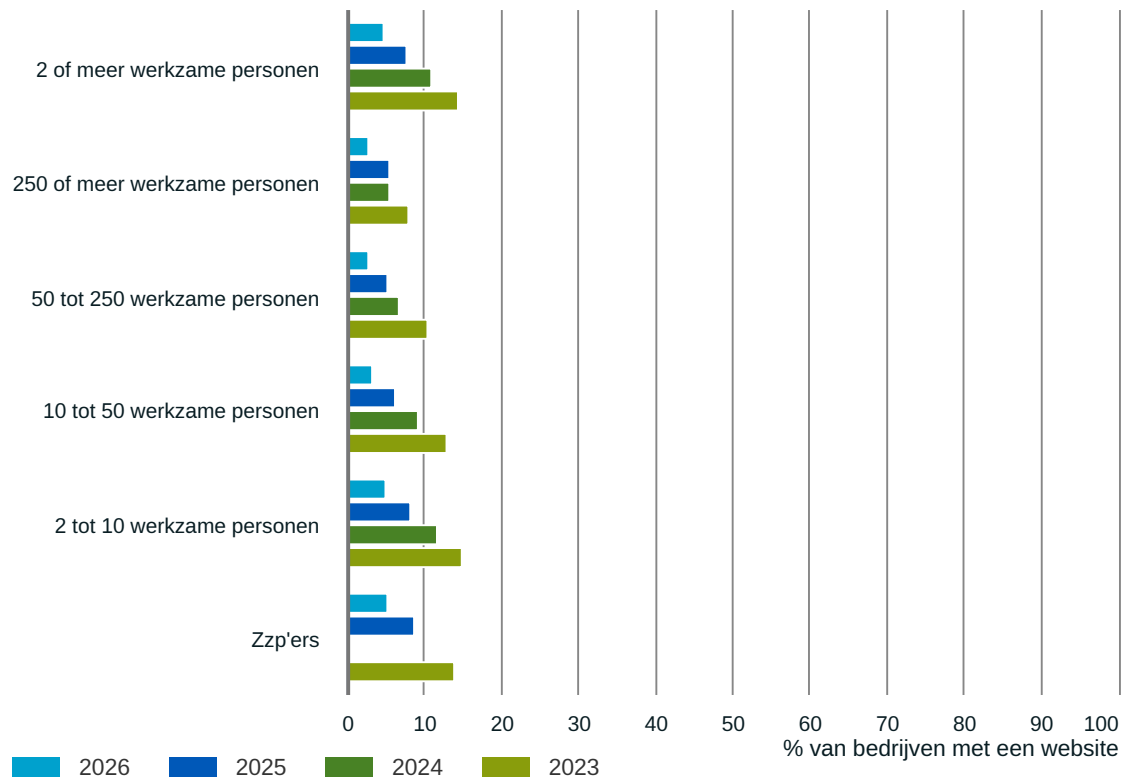


Figuur 4.18.: Bedrijven met een eindscore van 100 procent voor de e-mailscan naar bedrijfstak (2 of meer werkzame personen)

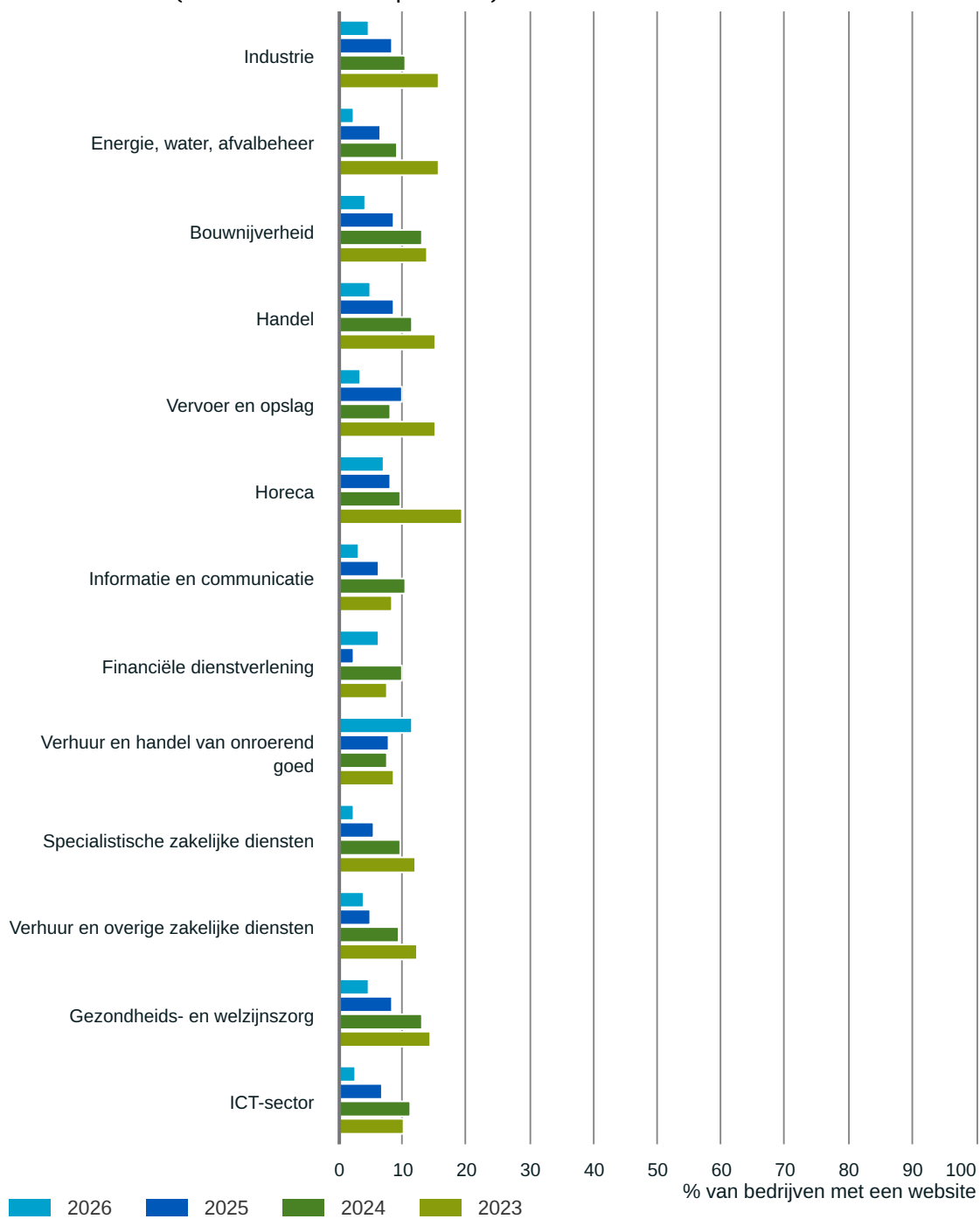


Tot slot wordt in Figuur 4.19 en Figuur 4.20 gekeken naar de bedrijven die juist laag scoren op de e-mailscan (40 procent of minder). Bijna 5 procent van de bedrijven met een website haalt in 2026 een eindscore van 40 procent of minder. Over het algemeen komt een eindscore van 40 procent of minder iets vaker voor bij kleinere bedrijven dan bij grotere bedrijven. Wel is het percentage voor alle bedrijfsgrootteklassen gedaald ten opzichte van vorig jaar. Een eindscore van 40 procent of minder wordt in 2026 het vaakst behaald in de bedrijfstak 'Verhuur en handel van onroerend goed' (11,4 procent).

Figuur 4.19.: Bedrijven met een eindscore van 40 procent of lager voor de e-mailscan naar bedrijfs-grootteklasse



Figuur 4.20.: Bedrijven met een eindscore van 40 procent of lager voor de e-mailscan naar bedrijfstak (2 of meer werkzame personen)



## 5. Conclusie

In dit rapport is de toepassing van internetstandaarden op de websites en e-mailserver van bedrijven in Nederland onderzocht. Hiertoe zijn de websites van bedrijven, verkregen uit de CBS-enquête 'ICT-gebruik bij bedrijven', gescand met de testtool [Internet.nl](#) van Platform Internetstandaarden. Er zijn scans uitgevoerd van zowel de websites (Hoofdstuk 3) als de e-mailserver (Hoofdstuk 4). Doordat het onderzoek al sinds 2020 wordt uitgevoerd, kan per bedrijfsgrootteklasse en bedrijfstak een beeld verkregen worden van de ontwikkeling door de jaren heen. Uit het rapport kunnen de volgende conclusies worden getrokken:

- In 2025 had 73 procent van de bedrijven een website (2 of meer werkzame personen). Dit is 2 procentpunt minder dan in het jaar daarvoor.
- In 2025 had 82,6 procent van de bedrijven met een website (2 of meer werkzame personen) '.nl' als domeinextensie van de hoofdwebsite. De domeinextensie '.com' kwam met 12,9 procent op de tweede plaats.
- Bedrijven gebruiken steeds vaker veilige internetstandaarden. De gemiddelde eindscore voor de websitescan van alle bedrijven met een website (2 of meer werkzame personen) is sinds 2020 met 14,3 procentpunt toegenomen: van 60,4 procent in 2020 naar 74,7 procent in 2026. De gemiddelde eindscore voor de e-mailscan is ook toegenomen: van 58,9 procent in 2023 naar 73,2 procent in 2026.
- De verdelingen van de eindscores voor de website- en e-mailscans vertonen weinig variatie tussen de bedrijfsgrootteklassen en bedrijfstakken. Voor de verschillende categorieën zijn wel duidelijkere verschillen te zien. Zo slagen kleinere bedrijven bij de websitescan bijvoorbeeld vaker voor de categorie IPv6, terwijl grotere bedrijven vaker slagen voor de categorie HTTPS. Voor de e-mailscan slagen kleinere bedrijven vaker voor de categorieën DNSSEC en Beveiligd e-mailtransport, terwijl grotere bedrijven vaker slagen voor de categorie Authenticiteit.
- Over het algemeen slagen bedrijven het vaakst voor de categorie Autorisatie voor routing (RPKI). Dit geldt voor zowel de websitescan als de e-mailscan, met respectievelijk 87,1 en 88,8 procent van de bedrijven (2 of meer werkzame personen) in 2026.
- Bij zowel de website- als e-mailscan is voor de categorie IPv6 de laatste jaren de grootste groei te zien. Bij de e-mailscan slaagt 65,5 procent van de bedrijven met een website (2 of meer werkzame personen) in 2026 voor deze categorie, terwijl dat in 2023 nog maar 27,3 procent was. Bij de websitescan slaagt 41,0 procent van de bedrijven, tegenover 31,4 procent in 2023.

# Referenties

- CBS. Ict-gebruik bij kleine bedrijven; bedrijfstak en bedrijfsgrootte, 2020, 2020. URL <https://opendata.cbs.nl/statline/#/CBS/nl/dataset/84828NED/table?ts=1607697173178>.
- CBS. Ict-gebruik bij kleine bedrijven; bedrijfstak en bedrijfsgrootte, 2021, 2021. URL <https://opendata.cbs.nl/statline/#/CBS/nl/dataset/85183NED/table?dl=7AA1B>.
- CBS. Ict-gebruik bij kleine bedrijven; bedrijfstak en bedrijfsgrootte, 2022, 2022a. URL <https://opendata.cbs.nl/statline/#/CBS/nl/dataset/85407NED/table?dl=7AA1D>.
- CBS. Veiligheid van website van bedrijven, 2020, 2022b. URL <https://www.cbs.nl/nl-nl/publicatie/2022/23/veiligheid-van-websites-van-bedrijven-2020>.
- CBS. Ict-gebruik bij kleine bedrijven; bedrijfstak en bedrijfsgrootte, 2023, 2023a. URL <https://opendata.cbs.nl/statline/#/CBS/nl/dataset/85732NED/table?dl=A1A74>.
- CBS. Toepassing van internetstandaarden voor websites van bedrijven, 2022, 2023b. URL <https://www.cbs.nl/nl-nl/publicatie/2023/19/toepassing-van-internetstandaarden-voor-websites-van-bedrijven>.
- CBS. Ict-gebruik bij kleine bedrijven; bedrijfstak en bedrijfsgrootte, 2024, 2024a. URL <https://opendata.cbs.nl/statline/#/CBS/nl/dataset/86071NED/table?dl=B66F9>.
- CBS. Toepassing van internetstandaarden voor websites van bedrijven, 2023, 2024b. URL <https://www.cbs.nl/nl-nl/longread/aanvullende-statistische-diensten/2024/toepassing-van-internetstandaarden-voor-websites-van-bedrijven-2023>.
- CBS. Cybersecuritymonitor 2024, 2025a. URL <https://www.cbs.nl/nl-nl/longread/aanvullende-statistische-diensten/2025/cybersecuritymonitor-2024>.
- CBS. Ict-gebruik bij kleine bedrijven; bedrijfstak en bedrijfsgrootte, 2025, 2025b. URL <https://opendata.cbs.nl/#/CBS/nl/dataset/86116NED/table?ts=1765790688948>.
- CBS. Toepassing van internetstandaarden voor websites van bedrijven, 2024, 2025c. URL <https://www.cbs.nl/nl-nl/longread/aanvullende-statistische-diensten/2025/toepassing-van-internetstandaarden-voor-websites-van-bedrijven-2024>.
- CBS. Ict-gebruik bij bedrijven, 2026. URL <https://www.cbs.nl/nl-nl/onze-diensten/methoden/onderzoeksomschrijvingen/korte-onderzoeksomschrijvingen/ict-gebruik-bedrijven>.
- Abby Israëls, Léander Kuijvenhoven, Jan van der Laan, Jeroen Pannekoek, and Eric Schulte Nordholt. Imputatie, 2011. URL <https://www.cbs.nl/nl-nl/onze-diensten/methoden/statistische-methoden/throughput/throughput/imputatie>.
- SIDN. E-mailbeveiliging, 2026. URL <https://www.sidn.nl/moderne-internetstandaarden/e-mailbeveiliging>.

# A. Indelingen en gebruikte termen

## A.1. Overzicht indelingen

Tabel A.1.: Overzicht van de bedrijfstakken

Code	Bedrijfstak
C	Industrie
D-E	Energie, water, afvalbeheer
F	Bouwnijverheid
G	Handel
H	Vervoer en opslag
I	Horeca
J	Informatie en communicatie
K	Financiële dienstverlening
L	Verhuur en handel van onroerend goed
M	Specialistische zakelijke diensten
N	Verhuur en overige zakelijke diensten
Q	Gezondheids- en welzijnszorg
ICT	ICT-sector

Tabel A.2.: Samenstelling van de ICT-sector

Code	Bedrijfstak
26.1	Vervaardiging van elektronische componenten en printplaten
26.2	Vervaardiging van computers en randapparatuur
26.3	Vervaardiging van communicatieapparatuur
26.4	Vervaardiging van consumentenelektronica
26.8	Vervaardiging van informatiedragers
46.5	Groothandel in ICT apparatuur
58.2	Uitgeverijen van software
61	Telecommunicatie
62	Dienstverlenende activiteiten op het gebied van informatietechnologie
63.1	Gegevensverwerking, webhosting en aanverwante activiteiten, webportals
95.1	Reparatie van computers en communicatieapparatuur

## A.2. Overzicht subtesten websitecan

Tabel A.3.: Subtesten categorie 'IPv6' voor de websitescan

Testomschrijving	Variabelenaam	Verplicht	Uitleg
IPv6-adressen voor nameservers	tests_web_ipv6_ns_address_verdict	Ja	Twee of meer nameservers van de domeinnaam hebben IPv6.
IPv6-bereikbaarheid van nameservers	tests_web_ipv6_ns_reach_verdict	Ja	Alle nameservers die een IPv6-adres hebben zijn bereikbaar via IPv6.
IPv6-adressen voor webservers	tests_web_ipv6_ws_address_verdict	Ja	Ten minste een van de webservers heeft een IPv6-adres.
IPv6-bereikbaarheid van webservers	tests_web_ipv6_ws_reach_verdict	Ja	Alle webservers met een IPv6-adres zijn bereikbaar via IPv6.
Gelijke website op IPv6 en IPv4	tests_web_ipv6_ws_similar_verdict	Ja	De website via IPv6 lijkt identiek via IPv4.

Tabel A.4.: Subtesten categorie 'DNSSEC' voor de websitescan

Testomschrijving	Variabelenaam	Verplicht	Uitleg
DNSSEC aanwezig	tests_web_dnssec_exist_verdict	Ja	De domein is met DNSSEC ondertekend.
DNSSEC geldig	tests_web_dnssec_valid_verdict	Ja	De domeinnaam is veilig oftewel 'secure', omdat zijn DNSSEC-handtekening geldig is.

Tabel A.5.: Subtesten categorie 'HTTPS' voor de websitescan

Testomschrijving	Variabelenaam	Verplicht	Uitleg
HTTPS beschikbaar	tests_web_https_ http_available_verdict	Ja	De website biedt HTTPS aan.
HTTPS-doorverwijzing	tests_web_https_ http_redirect_verdict	Ja	De webserver verwijst bezoekers automatisch door van HTTP naar HTTPS op dezelfde domeinnaam.
HTTP-compressie	tests_web_https_ http_compress_verdict	Ja	De webserver ondersteunt geen HTTP-compressie.
HSTS	tests_web_https_ http_hsts_verdict	Ja	De webserver biedt een HSTS-policy aan.
TLS-versie	tests_web_https_ tls_version_verdict	Ja	De webserver ondersteunt alleen veilige TLS-versies.
Ciphers (algoritmeselectie)	tests_web_https_ tls_ciphers_verdict	Ja	De webserver ondersteunt alleen veilige ciphers.
Cipher-volgorde	tests_web_https_ tls_cipherorder_verdict	Ja	De webserver dwingt zijn eigen cipher-voorkeur af ('I'), en biedt ciphers aan conform de voorgeschreven volgorde ('II').
Sleuteluitwisselings-parameters	tests_web_https_ tls_keyexchange_verdict	Ja	De webserver ondersteunt veilige parameters voor Diffie-Hellman-sleuteluitwisseling.
Hashfunctie voor sleuteluitwisseling	tests_web_https_tls_ keyexchange- hash_verdict	Nee	De webserver ondersteunt een veilige hashfunctie voor sleuteluitwisseling.
TLS-compressie	tests_web_https_ tls_compress_verdict	Nee	De webserver ondersteunt geen TLS-compressie.
Secure renegotiation	tests_web_https_ tls_secreneg_verdict		De webserver ondersteunt secure renegotiation.
Client initiated renegotiation	tests_web_https_ tls_clientreneg_verdict	Nee	De webserver staat geen client-initiated renegotiation toe.
0-RTT	tests_web_https_ tls_0rtt_verdict	Ja	De webserver ondersteunt geen 0-RTT.
OCSP stapling	tests_web_https_ tls_ocsp_verdict	Nee	De webserver ondersteunt OCSP en de data in het antwoord is valide.
Vertrouwensketen van certificaat	tests_web_https_ cert_chain_verdict	Ja	De vertrouwensketen van het websitecertificaat is compleet en ondertekend door een vertrouwde certificaatautoriteit.
Publieke sleutel van certificaat	tests_web_https_ cert_pubkey_verdict	Ja	De digitale handtekening van het websitecertificaat gebruikt veilige parameters
Handtekening van certificaat	tests_web_https_ cert_sig_verdict	Ja	het websitecertificaat is ondertekend met een voldoende algoritme voor hashing.
Domeinnaam op certificaat	tests_web_https_ cert_domain_verdict	Ja	De domeinnaam van de website komt overeen met de domeinnaam op het websitecertificaat.
CAA voor domein	tests_web_https_ tls_caa_verdict	Nee	De domeinnaam heeft een geldige, voldoende beschermende CAA.
DANE aanwezig	tests_web_https_ dane_exist_verdict	Nee	De websitedomein bevat een TLSA-record voor DANE.
DANE geldig	tests_web_https_ dane_valid_verdict	Nee	De DANE-fingerprint op de domeinnaam is geldig voor het websitecertificaat.

Tabel A.6.: Subtesten categorie 'Beveiligingsopties' voor de websitescan

Testomschrijving	Variabelenaam	Verplicht	Uitleg
X-Frame-Options	tests_web_appsecpriv_x_frame_options_verdict	Nee	De webserver biedt veilig ingestelde X-Frame-Options aan.
X-Content-Type-Options	tests_web_appsecpriv_x_content_type_options_verdict	Nee	De webserver biedt X-Content-Type-Options aan.
Content-Security-Policy	tests_web_appsecpriv_csp_verdict	Nee	De webserver biedt Content-Security-Policy (CSP) aan.
Referrer-Policy	tests_web_appsecpriv_referrer_policy_verdict	Nee	De webserver biedt een Referrer-Policy aan.
security.txt	tests_web_appsecpriv_securitytxt_verdict	Nee	De webserver biedt een security.txt-bestand op de juiste plaats aan.

Tabel A.7.: Subtesten categorie 'RPKI' voor de websitescan

Testomschrijving	Variabelenaam	Verplicht	Uitleg
Aanwezigheid van Route Origin Authorisation voor nameserver van domein	tests_web_ns_rpki_exists_verdict	Ja	Voor alle IP-adressen van de nameservers is een RPKI Route Origin Authorisation (ROA) gepubliceerd.
Geldigheid van route-aankondiging voor nameserver van domein	tests_web_ns_rpki_valid_verdict	Ja	'Alle IP-adressen van de nameservers hebben een 'valid' validatiestatus, voor RPKI ROA
Aanwezigheid van Route Origin Authorisation voor webserver	tests_web_rpki_exists_verdict	Ja	Voor alle IP-adressen van de webserver is een RPKI ROA gepubliceerd.
Geldigheid van route-aankondiging voor webserver	tests_web_rpki_valid_verdict	Ja	Alle IP-adressen van de webserver hebben een 'valid' validatiestatus, voor RPKI ROA.

## A.3. Overzicht subtesten e-mailscan

Tabel A.8.: Subtesten categorie 'IPv6' voor de e-mailscan

Testomschrijving	Variabelenaam	Verplicht	Uitleg
IPv6-adressen voor nameservers	tests_mail_ipv6_ns_address_verdict	Ja	Twee of meer nameservers van de domeinnaam hebben een IPv6-adres.
IPv6-bereikbaarheid van nameservers	tests_mail_ipv6_ns_reach_verdict	Ja	Alle nameservers die een IPv6-adres hebben zijn bereikbaar via IPv6.
IPv6-adressen voor mailservers	tests_mail_ipv6_mx_address_verdict	Ja	Alle ontvangende mailservers op de domeinnaam hebben een IPv6-adres.
IPv6-bereikbaarheid van mailservers	tests_mail_ipv6_mx_reach_verdict	Ja	Alle ontvangende mailservers met een IPv6-adres zijn bereikbaar via IPv6.

Tabel A.9.: Subtesten categorie 'DNSSEC' voor de e-mailscan

Testomschrijving	Variabelenaam	Verplicht	Uitleg
DNSSEC aanwezig voor het e-mailadresdomein	tests_mail_dnssec_mailto_exist_verdict	Ja	Het e-mailadresdomein is met DNSSEC ondertekend.
DNSSEC geldig voor het e-mailadresdomein	tests_mail_dnssec_mailto_valid_verdict	Ja	Het e-mailadresdomein is veilig oftewel 'secure', omdat de DNSSEC-handtekening geldig is.
DNSSEC aanwezig voor het e-mailserverdomein	tests_mail_dnssec_mx_exist_verdict	Ja	Alle mailserverdomeinen zijn ondertekend met DNSSEC.
DNSSEC geldig voor het e-mailserverdomein	tests_mail_dnssec_mx_valid_verdict	Ja	Alle ondertekende domeinnamen van de mailservers zijn veilig oftewel 'secure', omdat de DNSSEC-handtekeningen geldig zijn.

Tabel A.10.: Subtesten categorie 'Authenticiteit' voor de e-mailscan

Testomschrijving	Variabelenaam	Verplicht	Uitleg
DMARC aanwezigheid	tests_mail_auth_dmarc_exist_verdict	Ja	De domeinnaam heeft een DMARC-record.
DMARC policy	tests_mail_auth_dmarc_policy_verdict	Ja	De DMARC-policy is voldoende strikt.
DKIM aanwezigheid	tests_mail_auth_dkim_exist_verdict	Ja	De domeinnaam ondersteunt DKIM-records.
SPF aanwezigheid	tests_mail_auth_spf_exist_verdict	Ja	De domeinnaam heeft een SPF-record.
SPF policy	tests_mail_auth_spf_policy_verdict	Ja	De SPF-policy is voldoende strikt.

Tabel A.11.: Subtesten categorie 'Beveiligd e-mailtransport (STARTTLS en DANE)' voor de e-mailscan

Testomschrijving	Variabelenaam	Verplicht	Uitleg
STARTTLS beschikbaar	tests_mail_starttls_ tls_available_verdict	Ja	Alle mailservers bieden STARTTLS aan.
TLS-versie	tests_mail_starttls_ tls_version_verdict	Ja	De mailservers ondersteunen alleen veilige TLS-versies.
Ciphers (algoritmeselectie)	tests_mail_starttls_ tls_ciphers_verdict	Ja	De mailservers ondersteunen alleen veilige ciphers.
Cipher-volgorde	tests_mail_starttls_ tls_cipherorder_verdict	Ja	De mailservers dwingen hun eigen cipher-voorkeur af ('I'), en bieden ciphers aan conform de voorgeschreven volgorde ('II').
Sleuteluitwisselings-parameters	tests_mail_starttls_ tls_keyexchange_verdict	Ja	De mailservers ondersteunen veilige parameters voor Diffie-Hellman-sleuteluitwisseling.
Hashfunctie voor sleuteluitwisseling	tests_mail_starttls_tls_ keyexchange- hash_verdict	Nee	Alle mailservers ondersteunen veilige hashfuncties voor sleuteluitwisseling.
TLS-compressie	tests_mail_starttls_ tls_compress_verdict	Ja	Alle mailservers ondersteunen geen TLS-compressie.
Secure renegotiation	tests_mail_starttls_ tls_secreneg_verdict	Ja	De mailservers ondersteunen secure renegotiation.
Client-initiated renegotiation	tests_mail_starttls_ tls_clientreneg_verdict	Nee	De mailservers staan geen client-initiated renegotiation toe.
0-RTT	tests_mail_starttls_ tls_0rtt_verdict	Ja	De mailservers ondersteunt geen 0-RTT.
Vertrouwensketen van certificaat	tests_mail_starttls_ cert_chain_verdict	Nee	De vertrouwensketen van alle mailservercertificaten is compleet en ondertekend door een vertrouwde certificaatautoriteit.
Publieke sleutel van certificaat	tests_mail_starttls_ cert_pubkey_verdict	Ja	De digitale handtekeningen van alle mailservercertificaten gebruiken veilige parameters.
Handtekening van certificaat	tests_mail_starttls_ cert_sig_verdict	Ja	Alle mailservercertificaten zijn ondertekend met een veilig algoritme voor hashing.
Domeinnaam op certificaat	tests_mail_starttls_ cert_domain_verdict	Nee	De domeinnamen van alle mailservers komen overeen met de domeinnamen op de mailservercertificaten.
CAA voor mailserver	tests_mail_starttls_ tls_caa_verdict	Nee	De mailserver heeft een geldige, voldoende beschermende CAA.
DANE aanwezig	tests_mail_starttls_ dane_exist_verdict	Ja	Alle mailserverdomeinen bevatten een TLSA-record voor DANE.
DANE geldig	tests_mail_starttls_ dane_valid_verdict	Ja	Alle mailservers hebben ten minste een geldige DANE-fingerprint.
DANE- vervangingschema	tests_mail_starttls_ dane_rollover_verdict	Nee	Alle mailserver-domeinen hebben een actief DANE-schema voor het betrouwbaar vervangen van certificaat-sleutels.

Tabel A.12.: Subtesten categorie 'RPKI' voor de e-mailscan

Testomschrijving	Variabelenaam	Verplicht	Uitleg
Aanwezigheid van Route Origin Authorisation voor nameserver van domein	tests_mail_ns_ rpki_exists_verdict	Ja	Voor alle IP-adressen van de nameservers is een RPKI Route Origin Authorisation (ROA) gepubliceerd.
Geldigheid van route-aankondiging voor nameserver van domein	tests_mail_ns_ rpki_valid_verdict	Ja	Alle IP-adressen van de nameservers hebben een 'valid' validatiestatus, voor RPKI ROA.
Aanwezigheid van Route Origin Authorisation voor nameserver van mailservers	tests_mail_mx_ns_ rpki_exists_verdict	Ja	Voor alle IP-adressen van de nameservers van de mailserver(s) is een RPKI Route Origin Authorisation (ROA) gepubliceerd.
Geldigheid van route-aankondiging voor nameserver van mailservers	tests_mail_mx_ns_ rpki_valid_verdict	Ja	Alle IP-adressen van de nameservers van de ontvangende mailservers hebben een 'valid' validatiestatus, voor RPKI ROA.
Aanwezigheid van Route Origin Authorisation voor ontvangende mailservers	tests_mail_ rpki_exists_verdict	Ja	Voor alle IP-adressen van de ontvangende mailserver(s) is een RPKI Route Origin Authorisation (ROA) gepubliceerd.
Geldigheid van route-aankondiging voor ontvangende mailservers	tests_mail_ rpki_valid_verdict	Ja	Alle IP-adressen van de ontvangende mailservers hebben een 'valid' validatiestatus, voor RPKI ROA.



## A.4. Overzicht termen

Tabel A.13.: Termenlijst

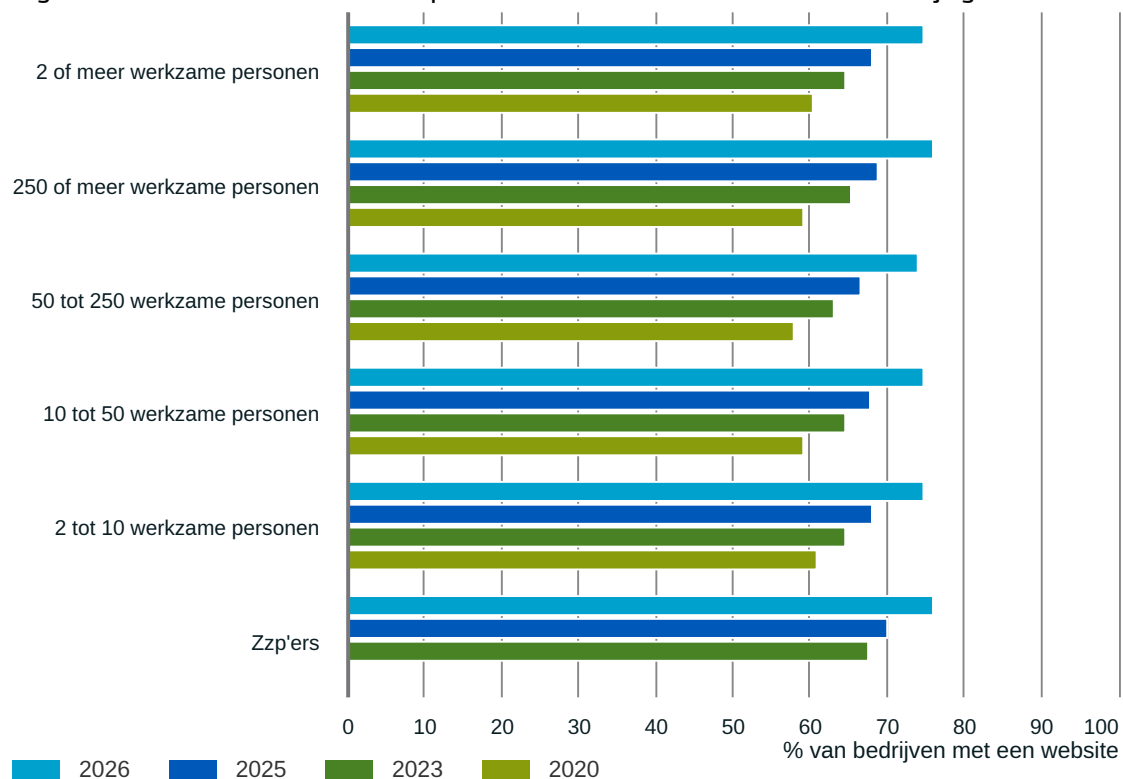
Term	Uitleg
Domeinnaam	Een domeinnaam is het unieke, herkenbare webadres dat wordt gebruikt om websites te vinden op het internet, bijvoorbeeld <code>www.cbs.nl</code> of <code>google.com</code> .
IP-adres	Het IP-adres van een website is een unieke, numerieke code die de fysieke locatie van de server waar de website op staat identificeert. Het functioneert als een digitaal "huisadres" waarmee computers en browsers de server kunnen vinden om de website te laden. Hierbij is IPv4 de oude standaard, en IPv6 de opvolger met langere codes en betere beveiliging.
E-mailadresdomein	Een e-mailadresdomein is het gedeelte achter het apenstaartje (@) in een e-mailadres, zoals <code>gmail.com</code> of <code>cbs.nl</code> . Het identificeert de server die de e-mail afhandelt en bepaalt de mailprovider.
Domain name server (DNS)	Het DNS is een systeem van gelinkte servers die alle adresinformatie van o.a. domeinnamen en e-mailadresdomeinen bevatten. Belangrijke taken zijn o.a. betrouwbaar domeinnamen aan IP-adressen koppelen, en e-mailadresdomeinen aan mailservers koppelen.
Nameserver	Een server in het DNS-netwerk waarop de koppelinformatie tussen domeinnamen en o.a. IP-adressen staat van een collectie domeinnamen. Een domeinnaam kan zijn koppelinformatie op meerdere nameservers hebben.
A/AAAA-record	Het bestand in het DNS waarin de koppelinformatie tussen de domeinnaam en respectievelijk IPv4 en IPv6 van een webserver staat.
MX-record (mail-exchange)	Het bestand in het DNS waarin de koppelinformatie tussen het e-mailadresdomein en het mailserverdomein staat.
DNSSEC (Domain Name System Security Extensions)	Een beveiligingsstandaard die DNS-informatie voorziet van een digitale handtekening, waarmee de authenticiteit en integriteit van DNS-records wordt gegarandeerd.
HTTP (Hypertext Transfer Protocol)	Het fundamentele communicatieprotocol voor het World Wide Web, gebruikt door browsers (clients) om data zoals HTML-pagina's op te vragen bij servers.
HTTPS (Hypertext Transfer Protocol secure)	Een beveiligde versie van HTTP. HTTPS gebruikt een SSL/TLS-certificaat om gegevens te beveiligen, waardoor bijvoorbeeld wachtwoorden en creditcardgegevens niet kunnen worden onderschept.
HTTP-compressie	Vermindert de bestandsgrootte van tekstgebaseerde webinhoud (HTML, CSS, JavaScript) op de server voordat deze naar de browser wordt gestuurd. Het toestaan van HTTP-compressie is onveilig. Het is dus niet goed als een domein dit ondersteunt (volgens <code>internet.nl</code> ).
HTTP Strict Transport Security (HSTS)	Een beveiligingsmechanisme dat webbrowsers dwingt om uitsluitend via een beveiligde HTTPS-verbinding met een website te communiceren.
Transport Layer Security (TLS)	Het standaard cryptografische protocol voor het beveiligen van internetverbindingen, e-mail en andere communicatie.
Cipher suite	Vastgelegde combinatie van algoritmes (key exchange, bulk encryption, en message authentication code) voor beveiligde verbindingen via TLS.
De Diffie-Hellman-sleuteluitwisseling	Een cryptografisch protocol waarmee twee partijen via een onbeveiligd kanaal veilig een gedeeld geheim (sleutel) kunnen afleiden zonder dit direct te versturen.
Hashfunctie	Een wiskundig algoritme dat invoerdata van willekeurige grootte omzet in een unieke reeks tekens met vaste lengte, de 'hashwaarde' of 'vingerafdruk'.
TLS-compressie	Onveilige manier van het verminderen van data binnen TLS. Het toestaan van TLS-compressie is onveilig. Het is dus niet goed als een domein dit ondersteunt (volgens <code>internet.nl</code> ).
Secure renegotiation	Een beveiligingsmechanisme (binnen TLS/SSL) dat voorkomt dat aanvallers tussen twee partijen (Man-in-the-Middle) nieuwe versleutelde gegevens in een bestaande verbinding injecteren.
Client-initiated renegotiation	Een beveiligingsrisico (binnen SSL/TLS) waarbij een client herhaaldelijk nieuwe handshakes aanvraagt. Dit verbruikt disproportioneel veel serverbronnen, wat kan leiden tot een Denial of Service (DoS)-aanval. Het is dus niet goed als een domein dit ondersteunt (volgens <code>internet.nl</code> ).
Zero Round Trip Time Resumption (0-RTT)	Een optie in TLS versie 1.3 waarmee applicatiedata wordt getransporteerd tijdens het eerste handshake-bericht. 0-RTT biedt echter geen bescherming tegen replay-aanvallen op de TLS-laag en dient daarom uitgezet te worden (volgens <code>internet.nl</code> ).
OCSP (Online Certificate Status Protocol)	Een real-time browserprotocol dat de geldigheid van een SSL/TLS-certificaat controleert bij de uitgever (CA). Het vertelt browsers of een certificaat geldig, ingetrokken of onbekend is, wat veiliger is dan oudere methoden. Het voorkomt het gebruik van gecompromitteerde certificaten.
Websitecertificaat	Een digitaal bestand dat een beveiligde, versleutelde verbinding tussen de browser van een bezoeker en de webserver tot stand brengt. De geldigheid kan gecheckt worden met een hiërarchisch vertrouwensketen systeem.
CAA-record (Certification Authority Authorization)	Specificeert welke certificaatautoriteiten (CA's) geautoriseerd zijn om SSL/TLS-certificaten uit te geven voor dat domein. Te vinden in de nameserver.
TLSA-record (Transport Layer Security Authentication)	Een DNS-record waarmee via DANE (DNS-based Authentication of Named Entities) de vingerafdruk van een TLS/SSL-certificaat wordt gekoppeld aan een domeinnaam.
X-Frame-Options	Een beveiligingsheader die websites tegen clickjacking-aanvallen beschermt door te bepalen of een browser de pagina mag tonen in een <frame>, <iframe> of <object>. Het wordt veelal gebruikt om te voorkomen dat kwaadwillenden de site in een onzichtbare laag op een andere site laden.
X-Content-Type	Een beveiligingsheader die voorkomt dat webbrowsers het mediatype (MIME-type) van bestanden "raden" of sniffen. Met de correcte instellingen dwingt dit webbrowser altijd het Content-Type zoals gedeclareerd door jouw webserver te volgen.
Content-Security-Policy (CSP)	Een beveiligingsheader die bepaalt welke bronnen (scripts, stijlen, afbeeldingen) een browser mag laden op een website
Referrer-Policy header	Een HTTP-beveiligingsheader waarmee de beheerder controleert hoeveel informatie (de URL) over de herkomst van de bezoekers wordt gedeeld wanneer zij naar andere sites klikken.
security.txt-bestand	Een gestandaardiseerd tekstbestand (RFC 9116) dat organisaties op hun webserver plaatsen om contactgegevens en beleid voor het melden van beveiligingslekken te publiceren.
Resource Public Key Infrastructure (RPKI)	Een cryptografisch beveiligingsframework dat de veiligheid van internetrouting (BGP) verhoogt door IP-adresblokken te koppelen aan rechtmatige houders.
Route Origin Authorisation (ROA)	Een digitaal certificaat, onderdeel van RPKI, dat bevestigt welk autonoom systeem (ASN) een specifiek IP-adresblok mag adverteren. Het voorkomt routekaping
DMARC-record	Een DNS-tekstrecord (TXT) dat e-mailfraude (spoofing/phishing) tegengaat door ontvangers te instrueren hoe om te gaan met onbevoegde e-mails. De policy geeft aan wat de instructies zijn in de record.
DKIM-record (DomainKeys Identified Mail)	Een DNS-tekstrecord (TXT) dat e-mails beveiligd door een digitale handtekening toe te voegen, waarmee de authenticiteit van de afzender wordt gegarandeerd en spoofing/phishing wordt verminderd.
SPF-record (Sender Policy Framework)	Een DNS-tekstrecord (TXT) dat specificeert welke mailservers en IP-adressen namens het domein e-mails mogen verzenden. De policy geeft aan wat de instructies zijn in de record.
STARTTLS	Een commando dat een onversleutelde e-mailverbinding (via SMTP, POP3 of IMAP) omzet in een beveiligde TLS-verbinding, waardoor communicatie tussen mailservers of clients wordt versleuteld.

## B. Alle websitescansuitslagen

In deze bijlage worden de uitslagen van de websitescans weergegeven. De gemiddelde eindscores en de uitslagen per categorie zijn te vinden in Paragraaf B.1. De resultaten voor alle subtesten worden gegeven in: Paragraaf B.2 voor de categorie IPv6, Paragraaf B.3 voor de categorie DNSSEC, Paragraaf B.4 voor de categorie HTTPS, Paragraaf B.5 voor de categorie Beveiligingsopties, en Paragraaf B.6 voor de categorie RPKI. Zie Paragraaf A.2 voor een korte uitleg per subtest. Tot slot wordt de verdeling van de eindscores getoond voor alle jaren in Paragraaf B.7. In de figuren wordt telkens een selectie van jaren getoond. Om de cijfers voor alle jaargangen van de websitescans te bekijken, kan bij elk figuur op de knop 'Toon data' worden geklikt<sup>1</sup>.

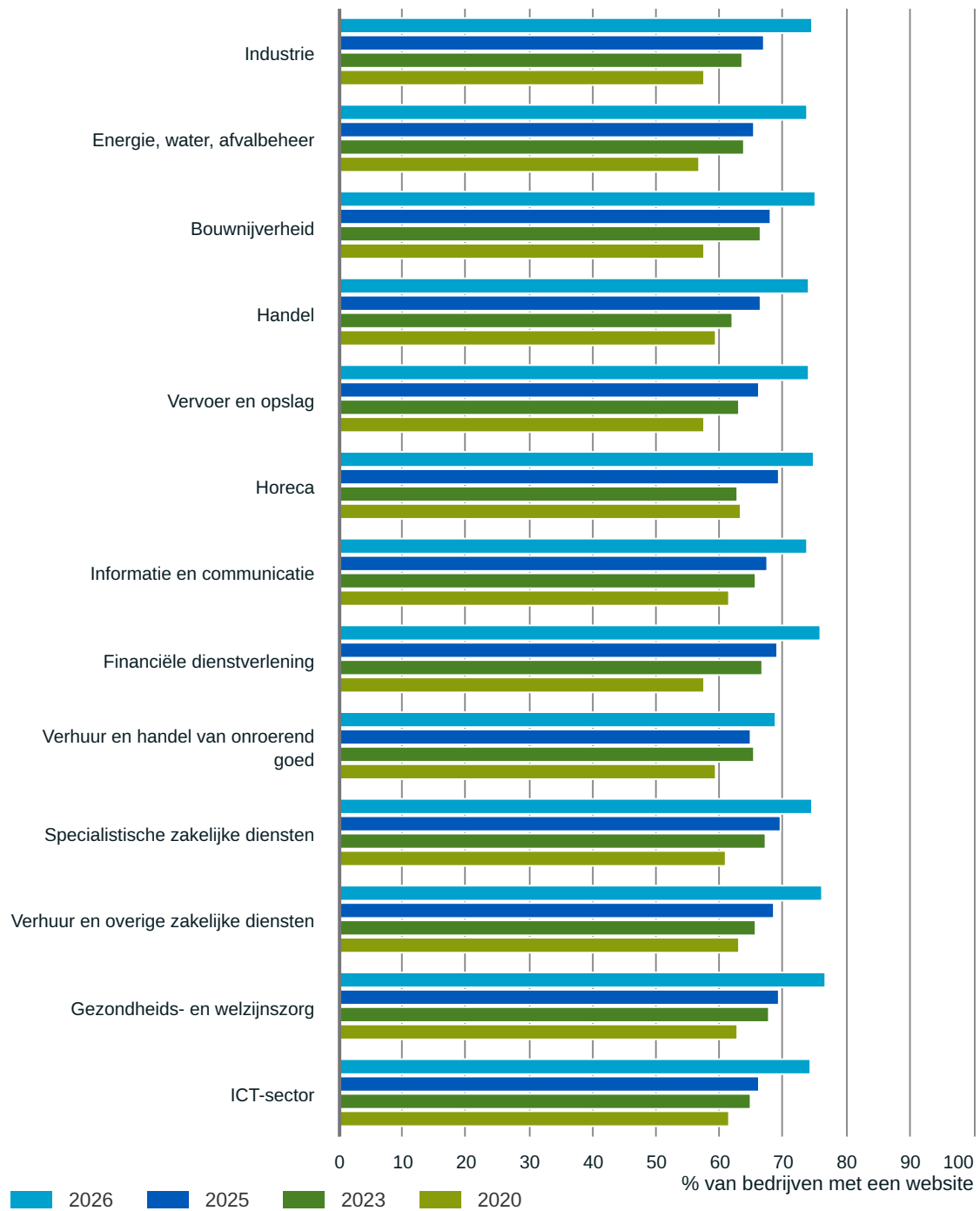
### B.1. Eindscore en categoriescores voor alle jaren

Figuur B.1.: Gemiddelde eindscore op Internet.nl voor de websitescan naar bedrijfsgrootteklasse

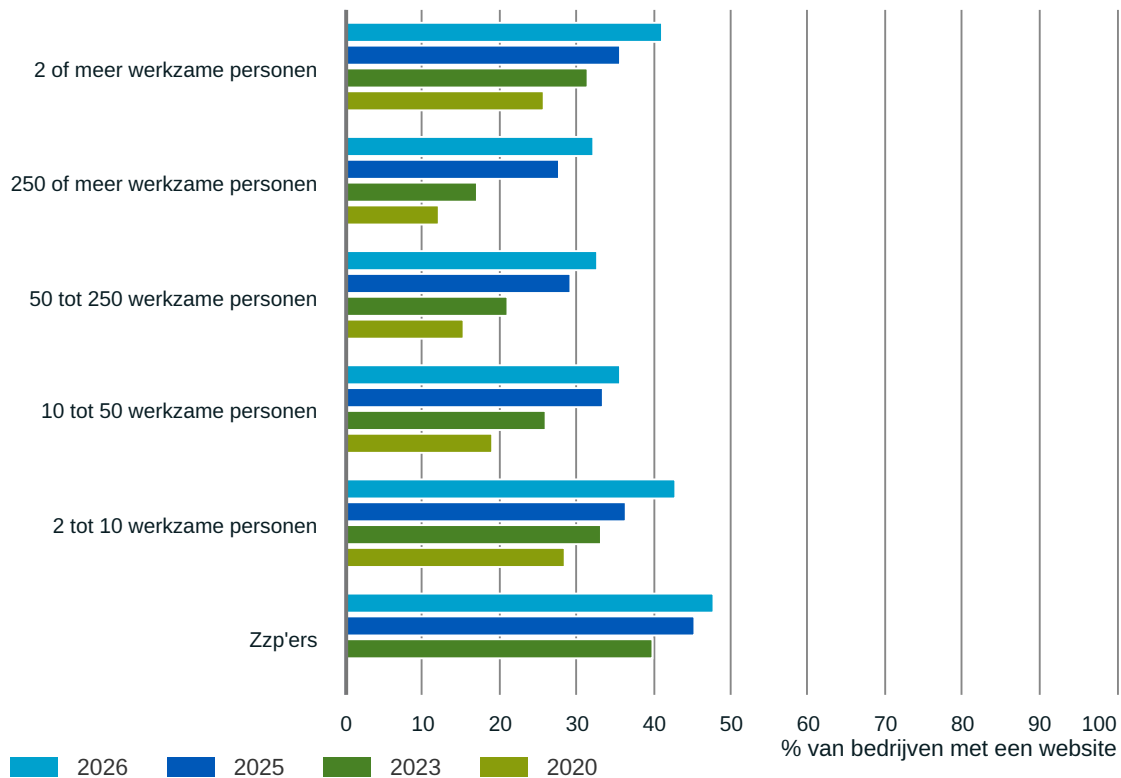


<sup>1</sup>De functionaliteit om de data te tonen is alleen beschikbaar voor de webversie van dit rapport.

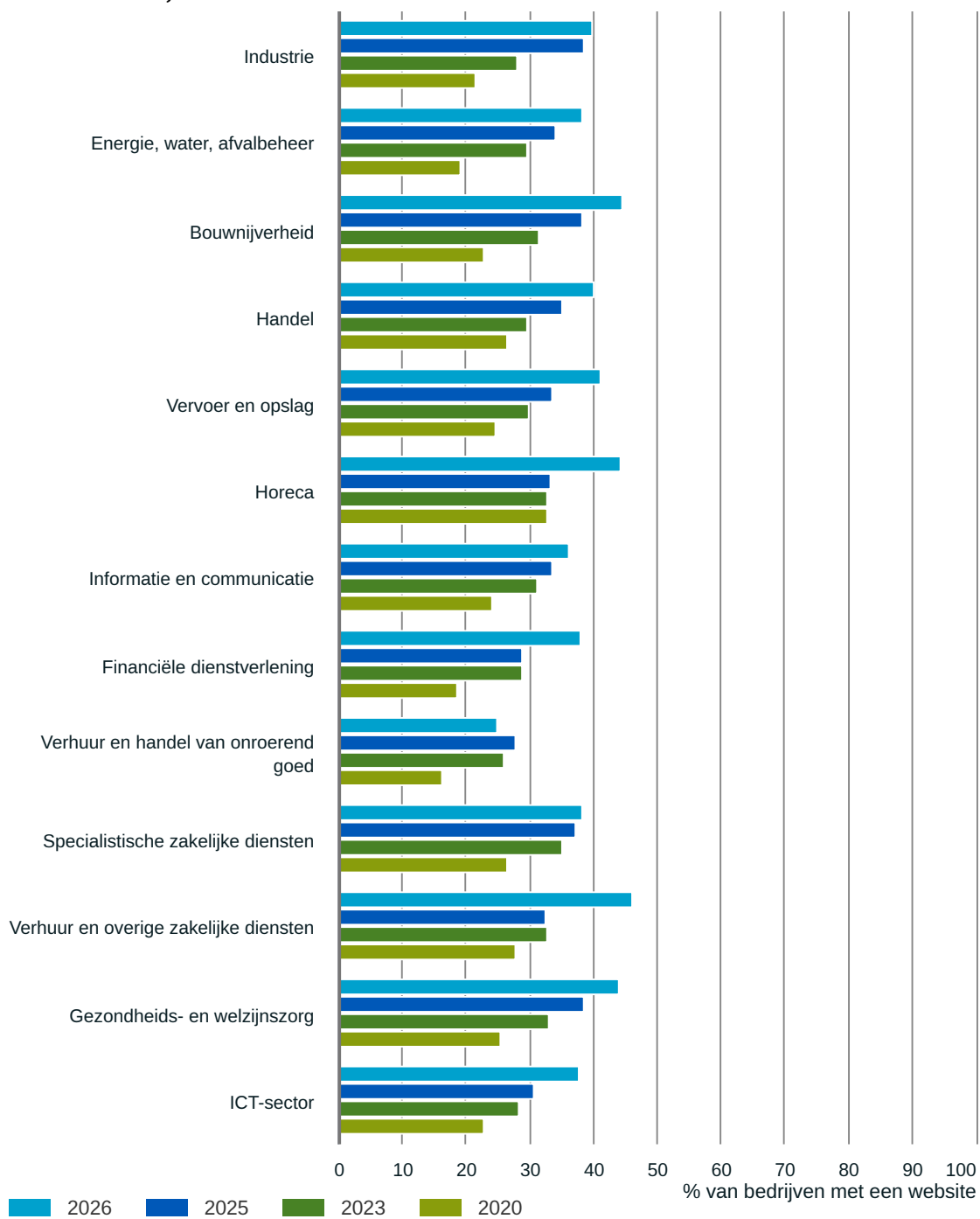
Figuur B.2.: Gemiddelde eindscore op Internet.nl voor de websitescan naar bedrijfstak (2 of meer werkzame personen)



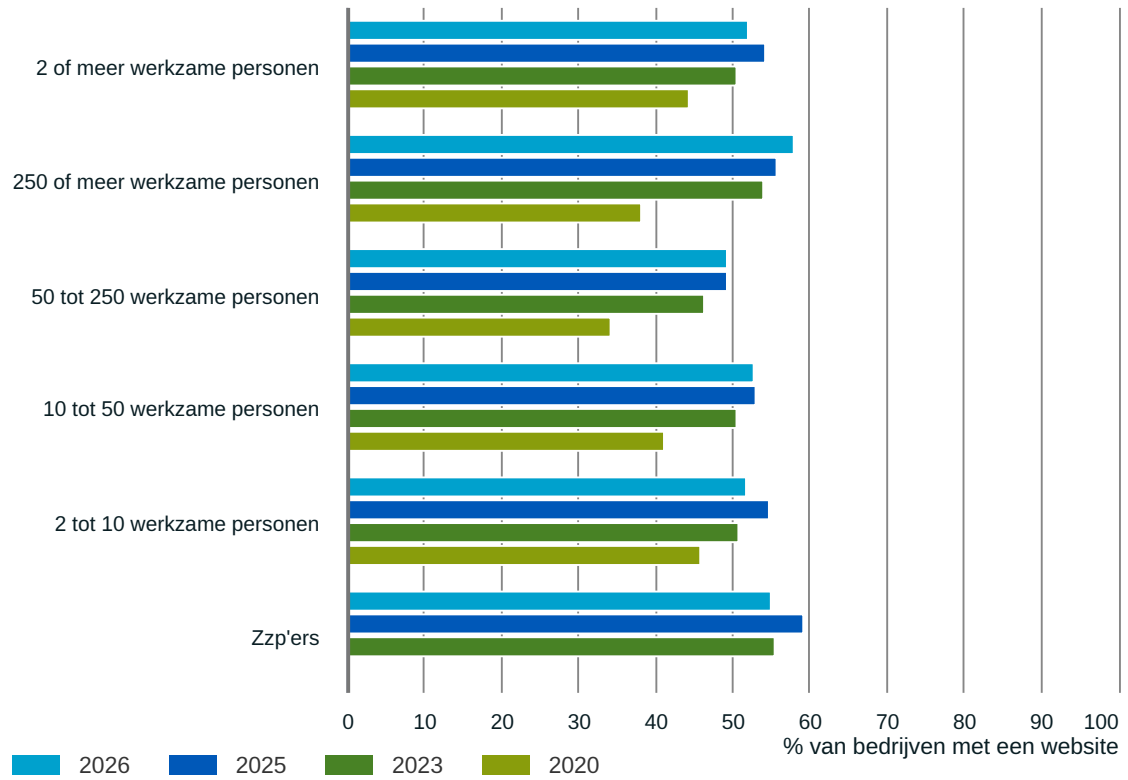
Figuur B.3.: Bedrijven met geslaagde categorie 'IPv6' naar bedrijfsgrootteklasse



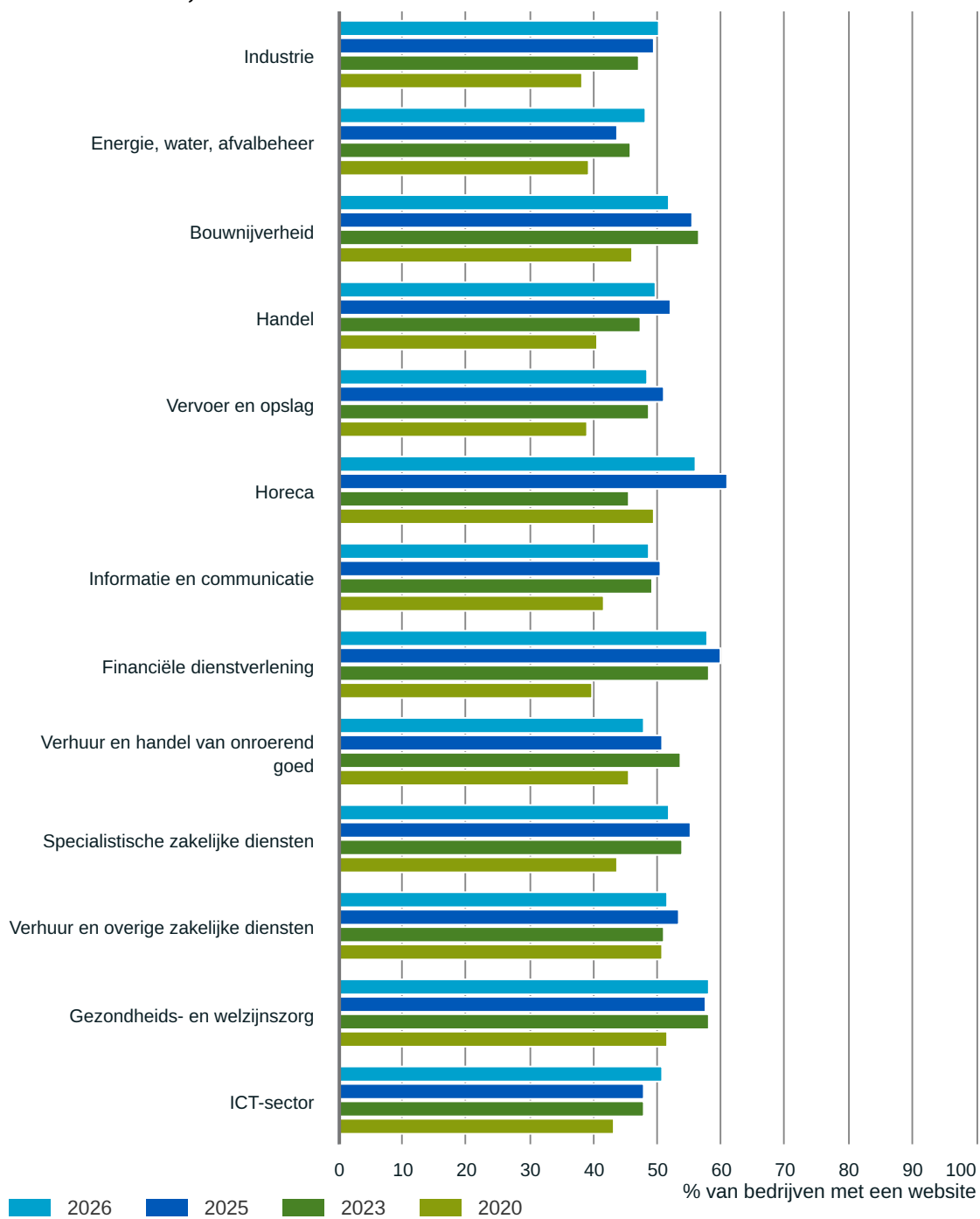
Figuur B.4.: Bedrijven met geslaagde categorie 'IPv6' naar bedrijfstak (2 of meer werkzame personen)



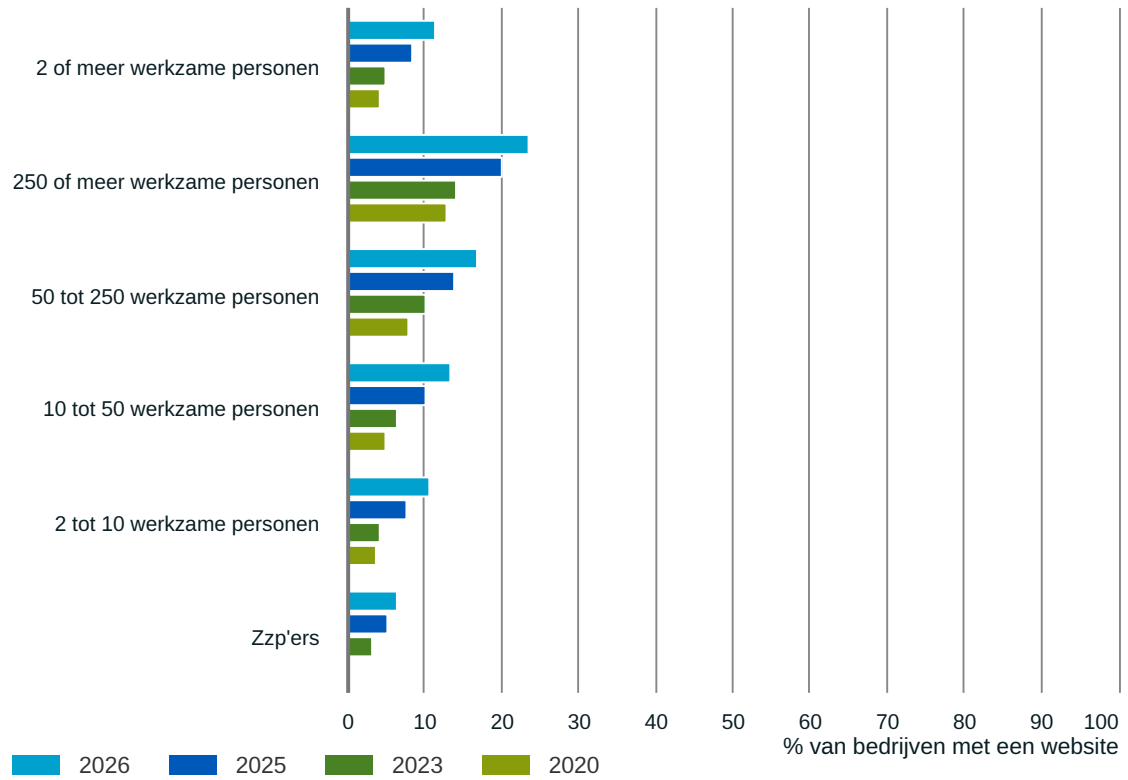
Figuur B.5.: Bedrijven met geslaagde categorie 'DNSSEC' naar bedrijfsgrootteklasse



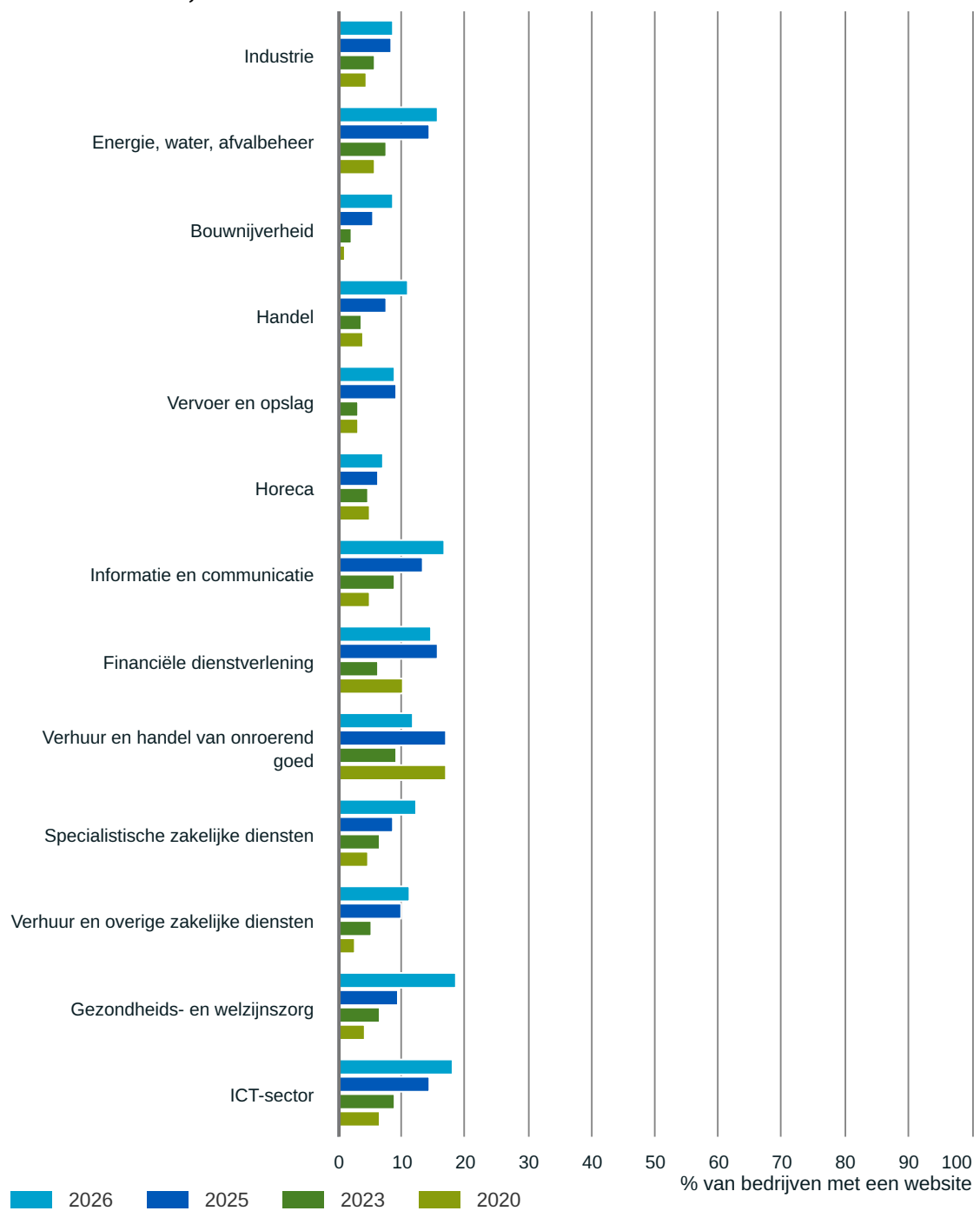
Figuur B.6.: Bedrijven met geslaagde categorie 'DNSSEC' naar bedrijfstak (2 of meer werkzame personen)



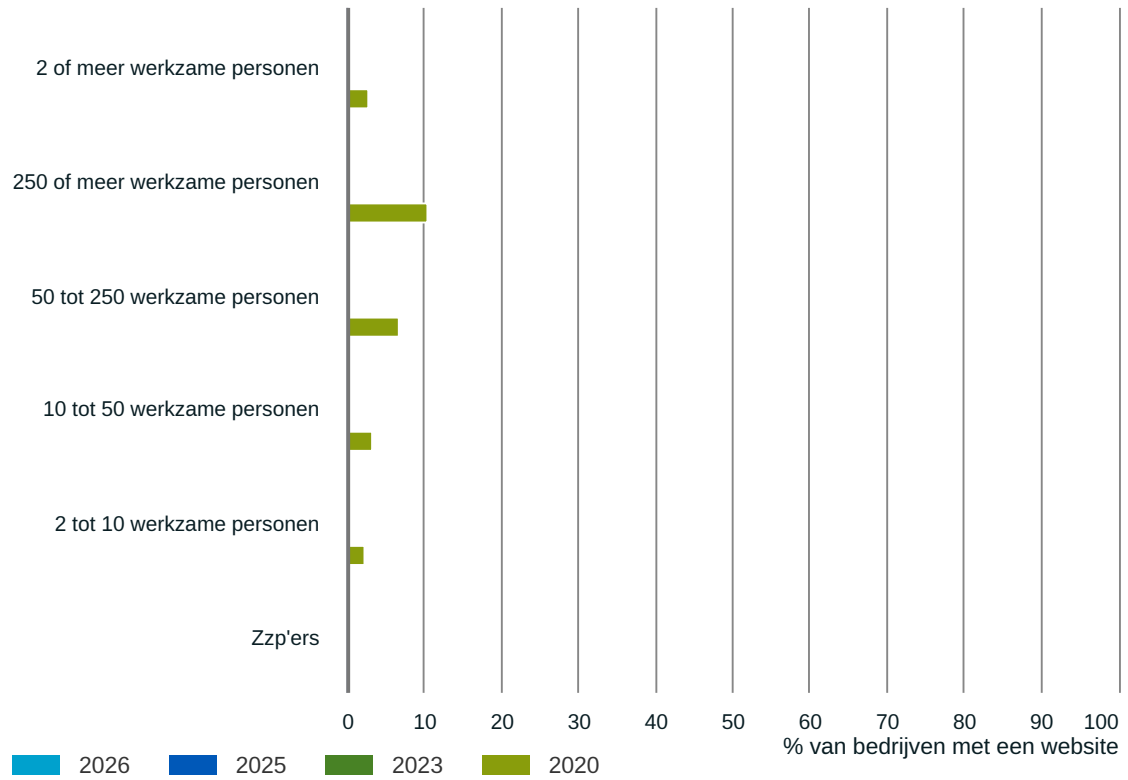
Figuur B.7.: Bedrijven met geslaagde categorie 'HTTPS' naar bedrijfsgrootteklasse



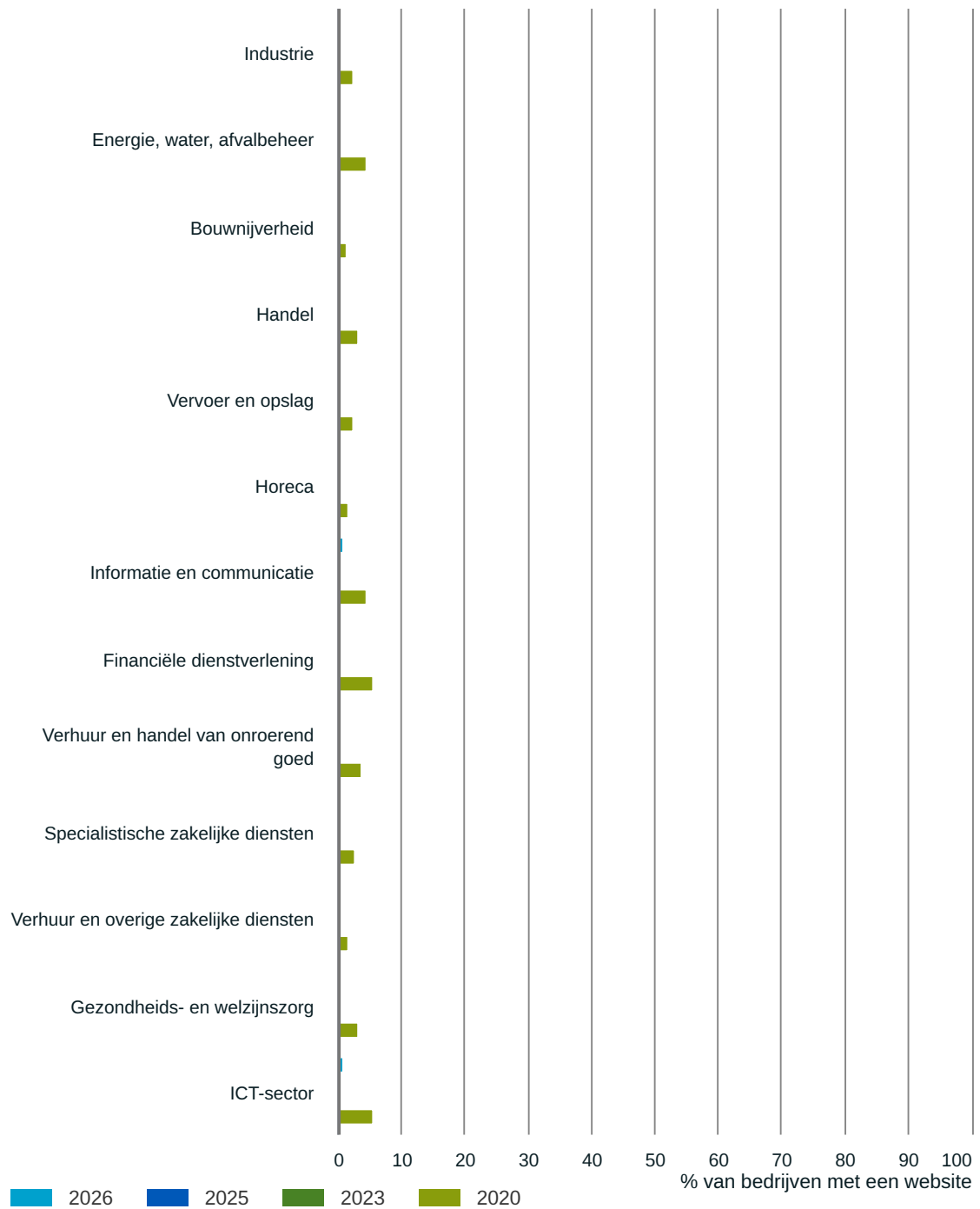
Figuur B.8.: Bedrijven met geslaagde categorie 'HTTPS' naar bedrijfstak (2 of meer werkzame personen)



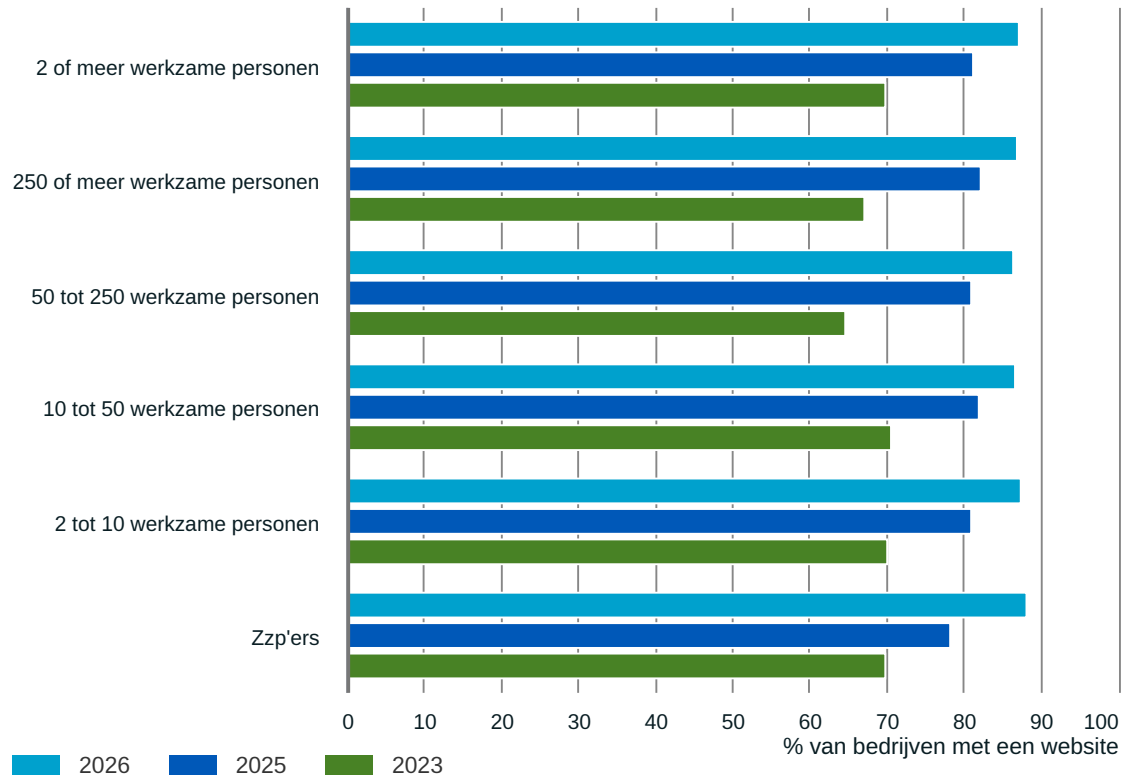
Figuur B.9.: Bedrijven met geslaagde categorie 'Beveiligingsopties' naar bedrijfsgrootteklasse



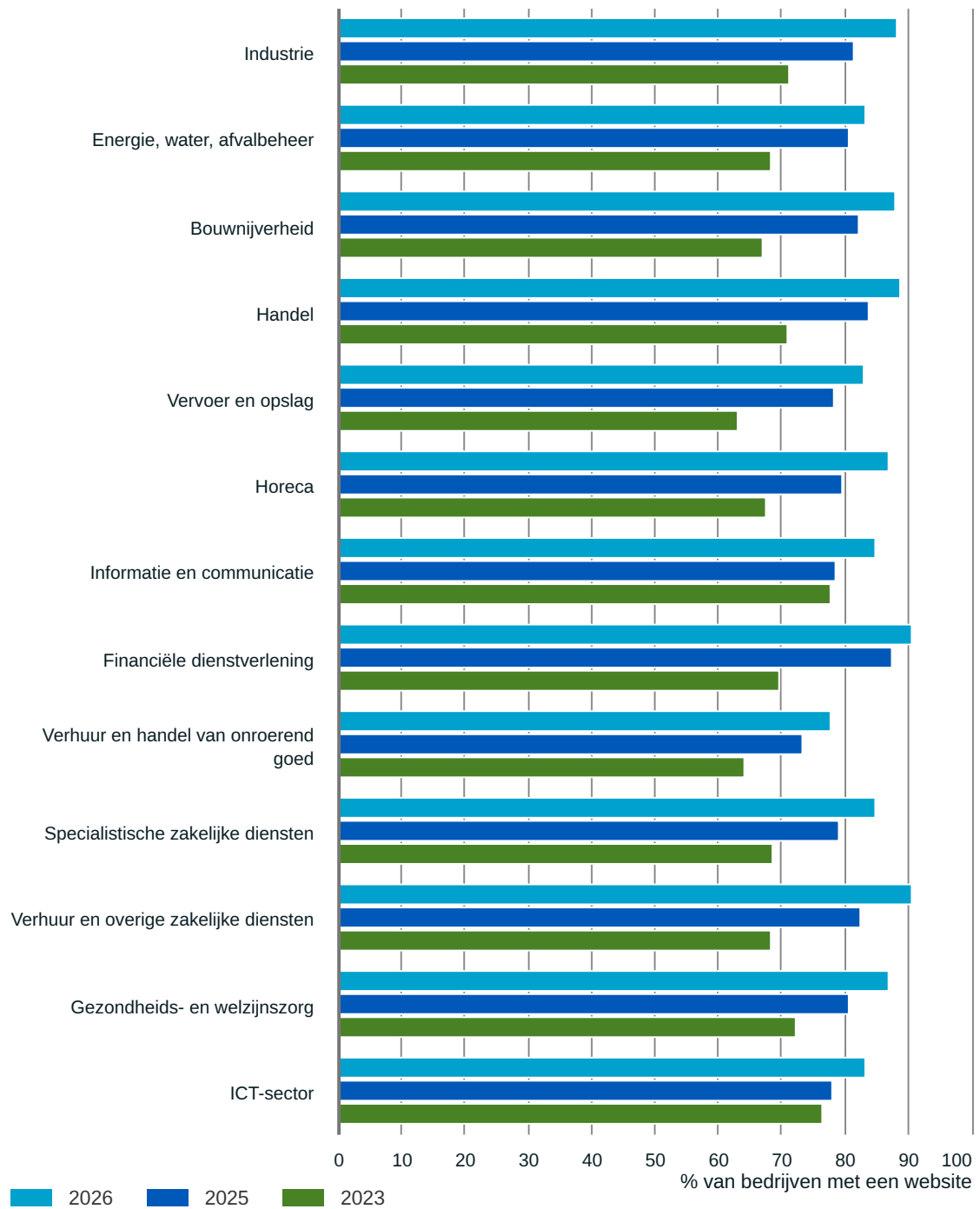
Figuur B.10.: Bedrijven met geslaagde categorie 'Beveiligingsopties' naar bedrijfstak (2 of meer werkzame personen)



Figuur B.11.: Bedrijven met geslaagde categorie 'RPKI' naar bedrijfsgrootteklasse

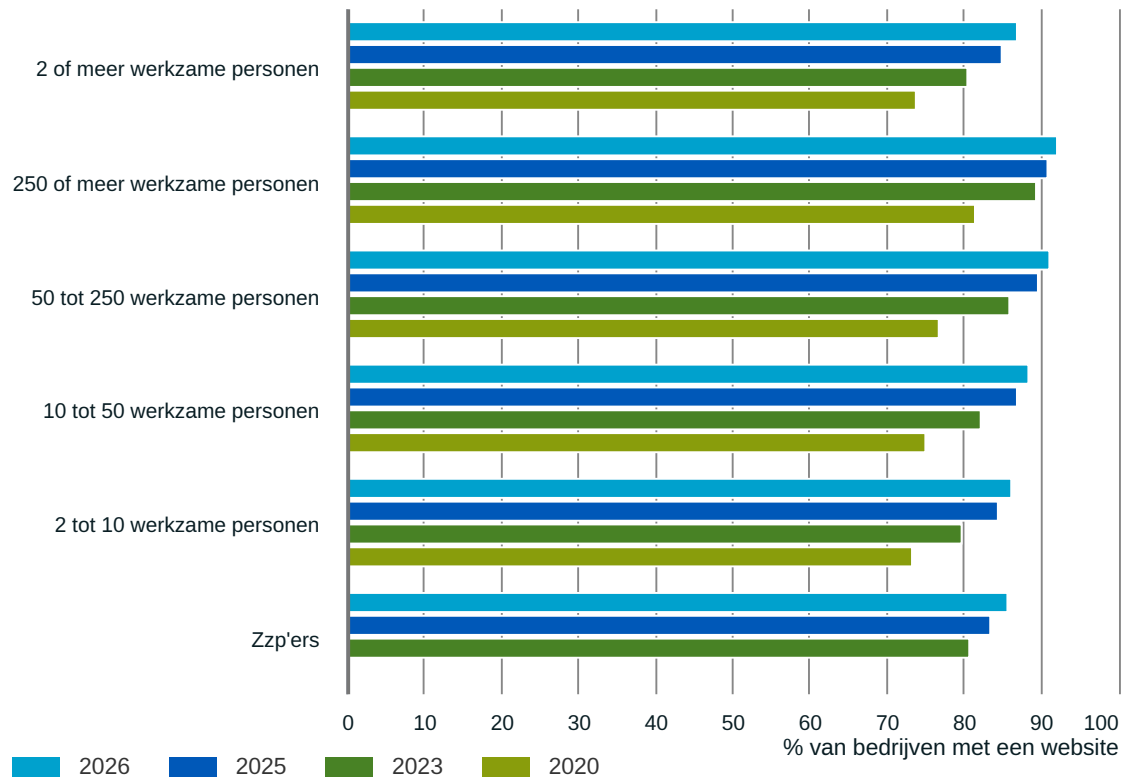


Figuur B.12.: Bedrijven met geslaagde categorie 'Autorisatie voor routing (RPKI)' naar bedrijfstak (2 of meer werkzame personen)

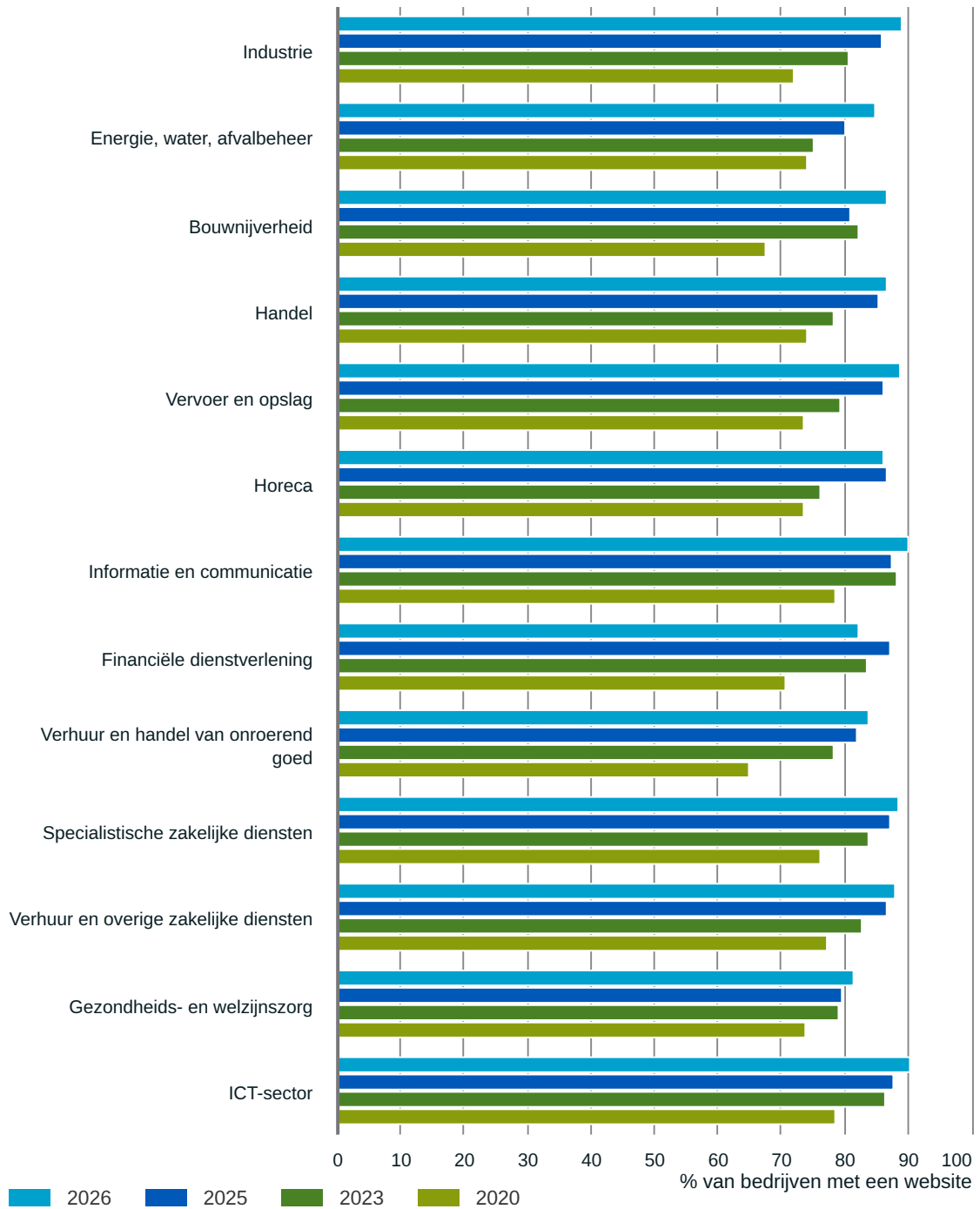


## B.2. Websitescanuitslagen voor categorie IPv6

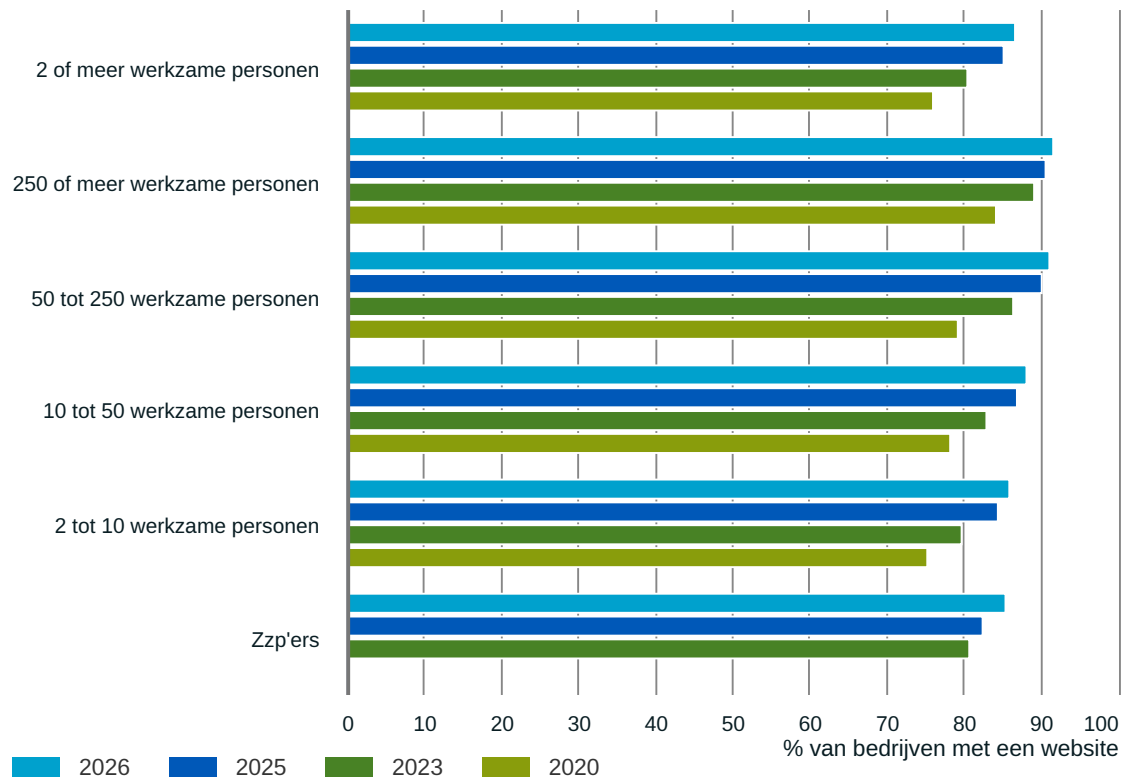
Figuur B.13.: Percentage van bedrijven met een website met geslaagde websitetest 'IPv6-adressen voor nameservers' naar bedrijfsgrootteklasse



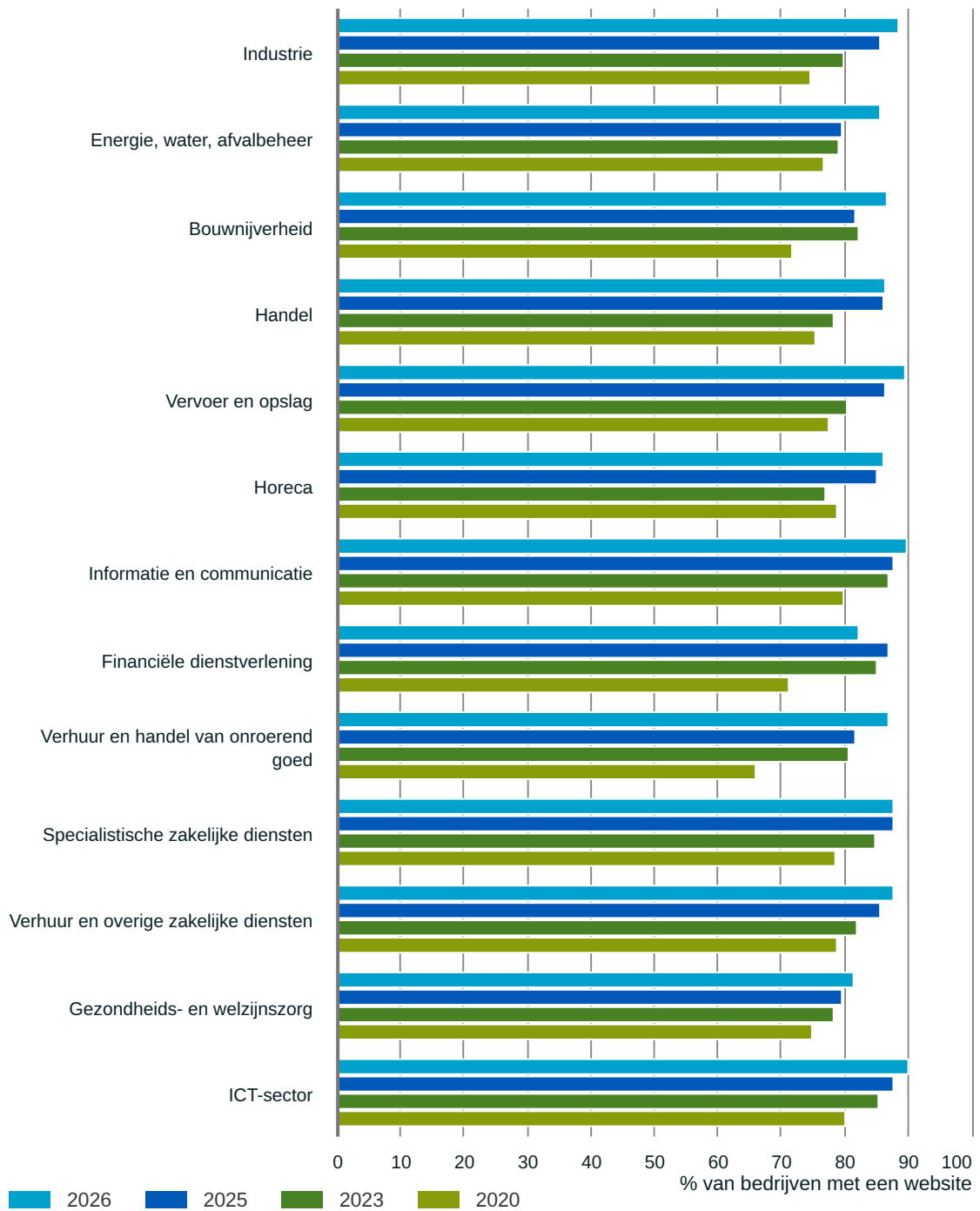
Figuur B.14.: Percentage van bedrijven met een website met geslaagde websitetest 'IPv6-adressen voor nameservers' naar bedrijfstak (2 of meer werkzame personen)



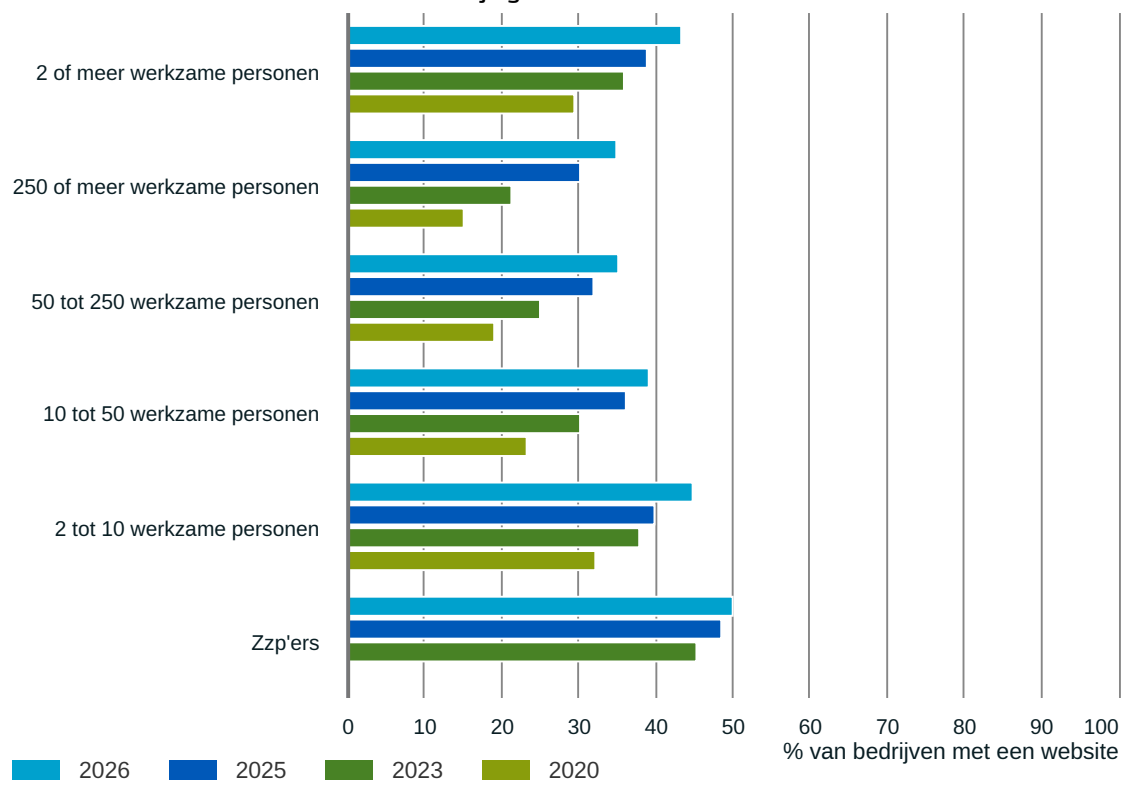
Figuur B.15.: Percentage van bedrijven met een website met geslaagde websitetest 'IPv6-bereikbaarheid van nameservers' naar bedrijfsgrootteklasse



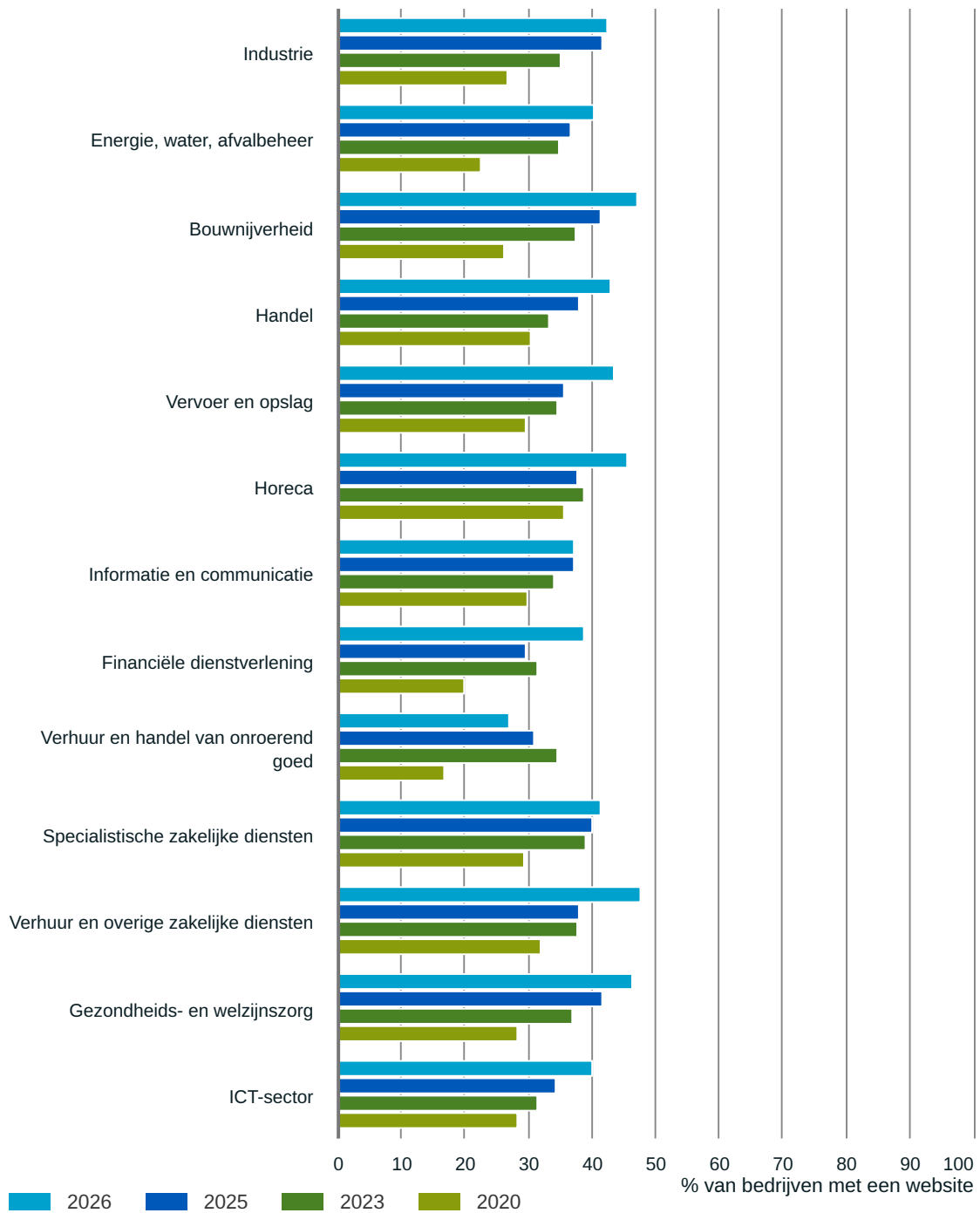
Figuur B.16.: Percentage van bedrijven met een website met geslaagde websitetest 'IPv6-bereikbaarheid van nameservers' naar bedrijfstak (2 of meer werkzame personen)



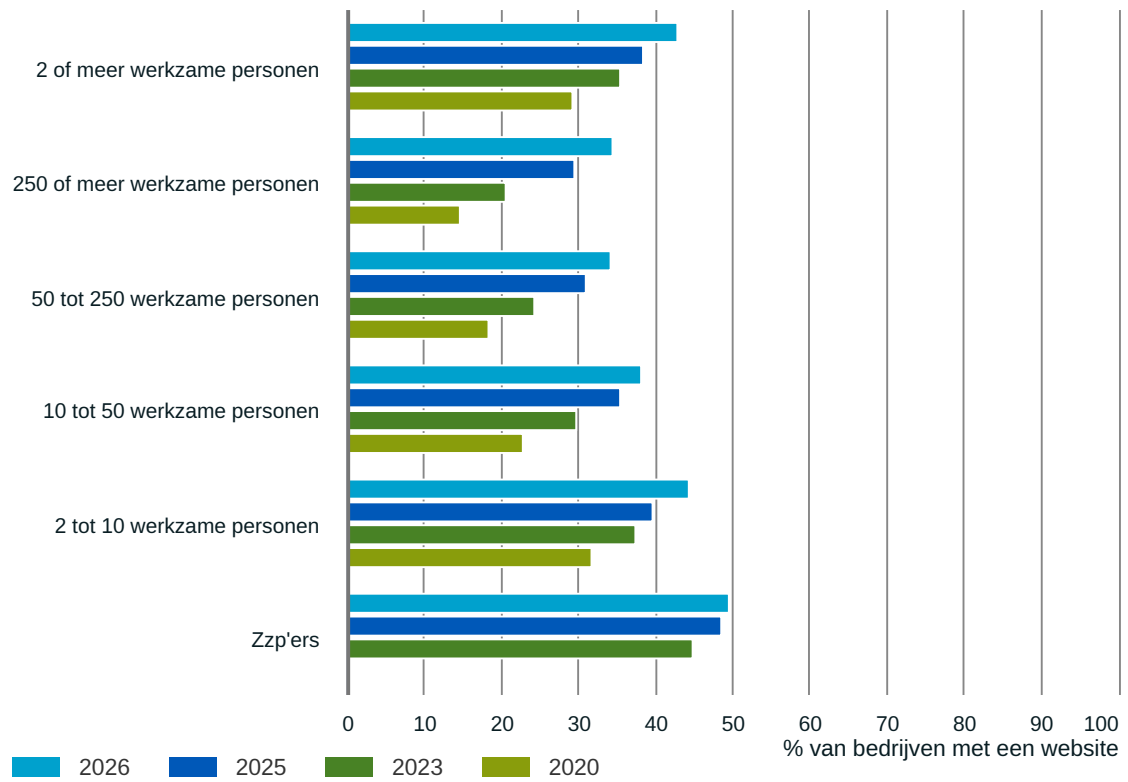
Figuur B.17.: Percentage van bedrijven met een website met geslaagde websitetest 'IPv6-adressen voor webserver' naar bedrijfsgrootteklasse



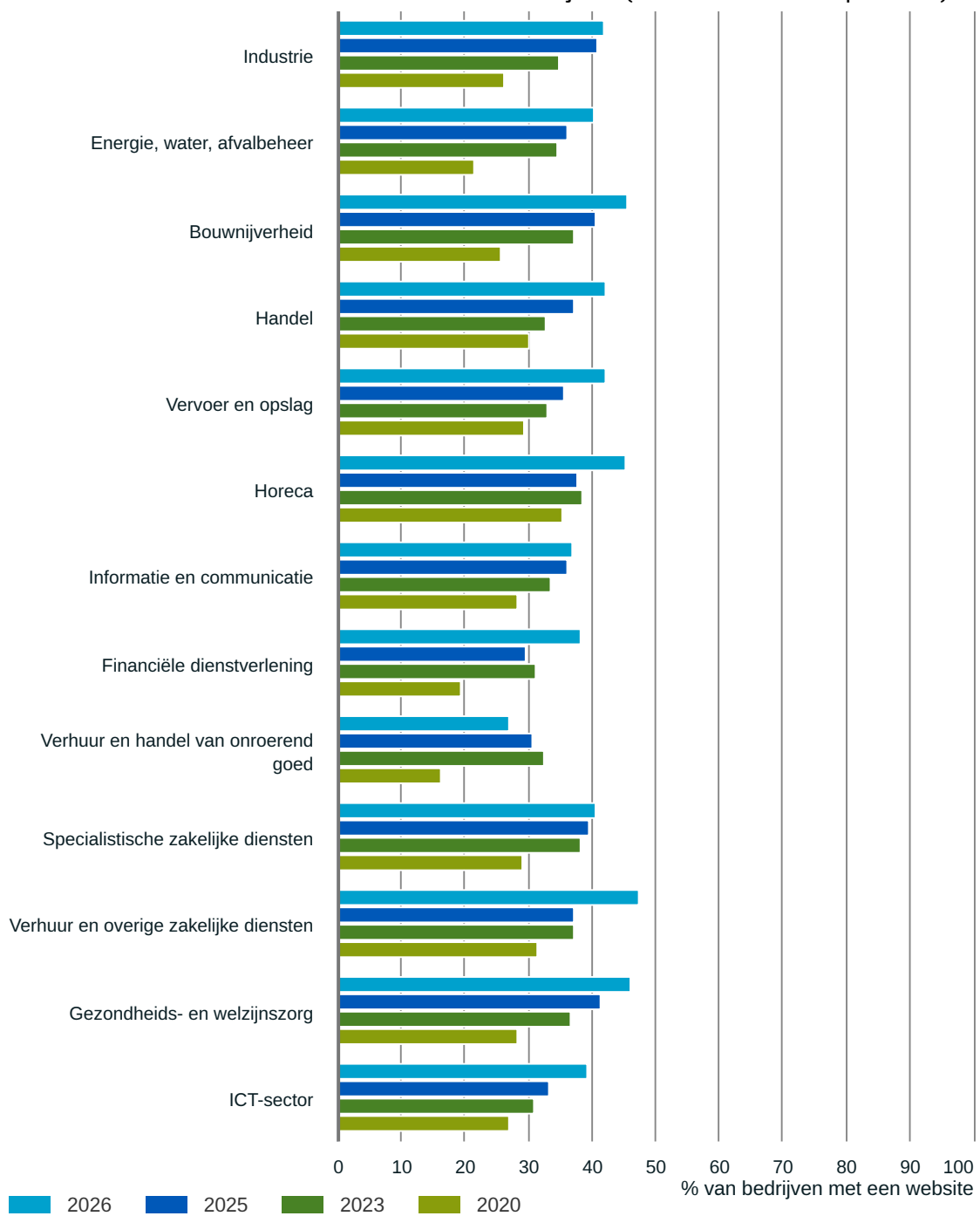
Figuur B.18.: Percentage van bedrijven met een website met geslaagde websitetest 'IPv6-adressen voor webserver' naar bedrijfstak (2 of meer werkzame personen)



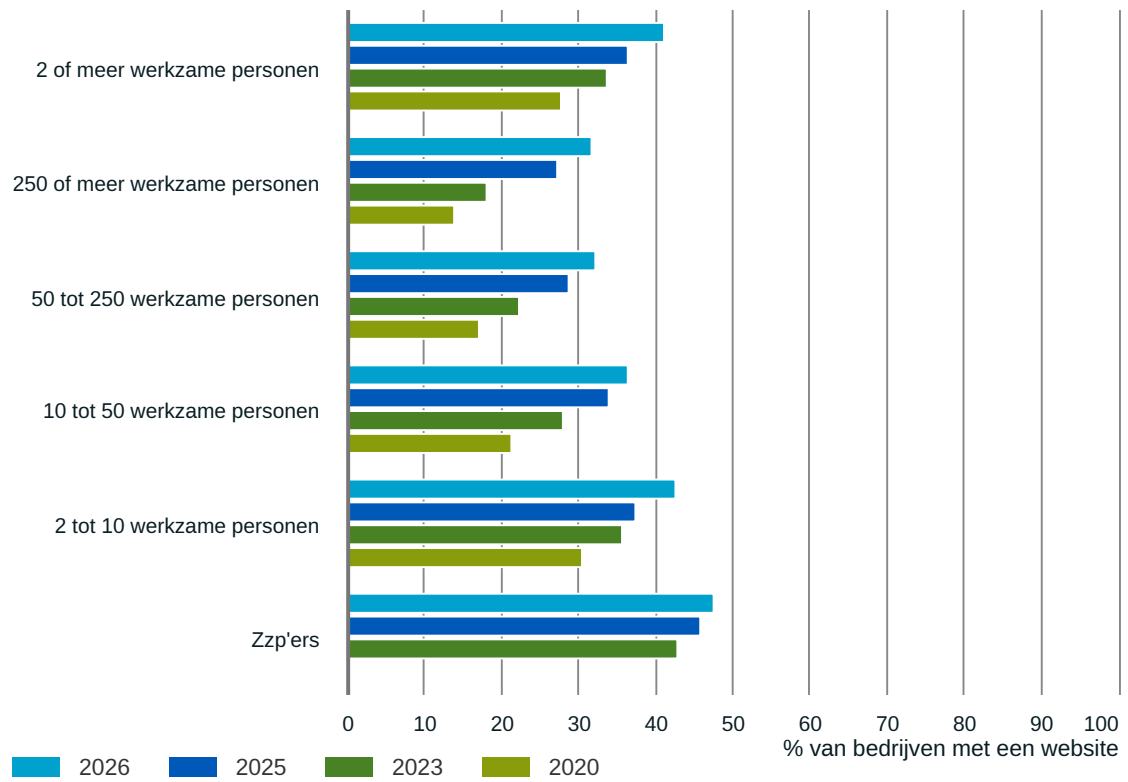
Figuur B.19.: Percentage van bedrijven met een website met geslaagde websitetest 'IPv6-bereikbaarheid van webserver' naar bedrijfsgrootteklasse



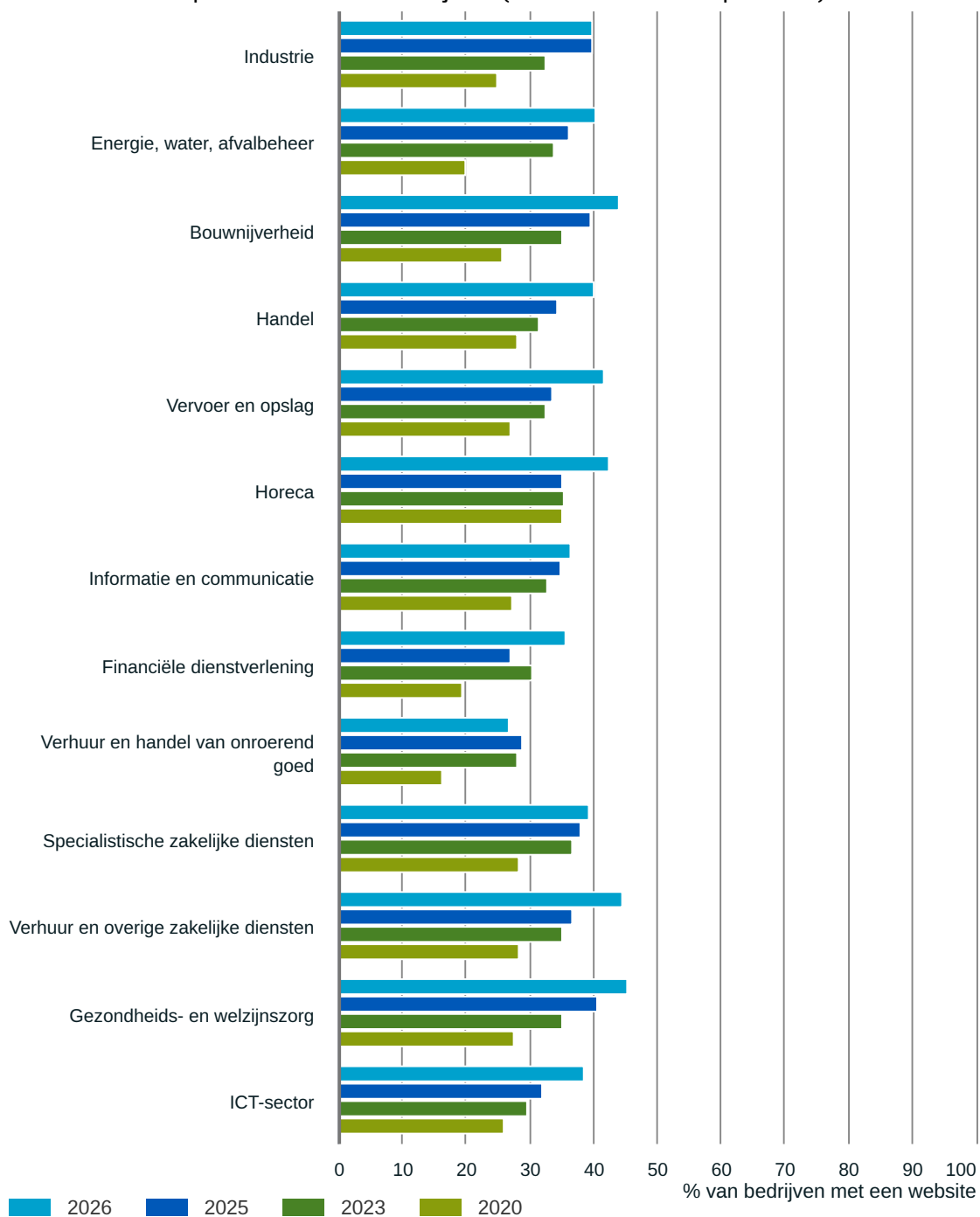
Figuur B.20.: Percentage van bedrijven met een website met geslaagde websitetest 'IPv6-bereikbaarheid van webserver' naar bedrijfstak (2 of meer werkzame personen)



Figuur B.21.: Percentage van bedrijven met een website met geslaagde websitetest 'Gelijke website op IPv4 en IPv6' naar bedrijfsgrootteklasse

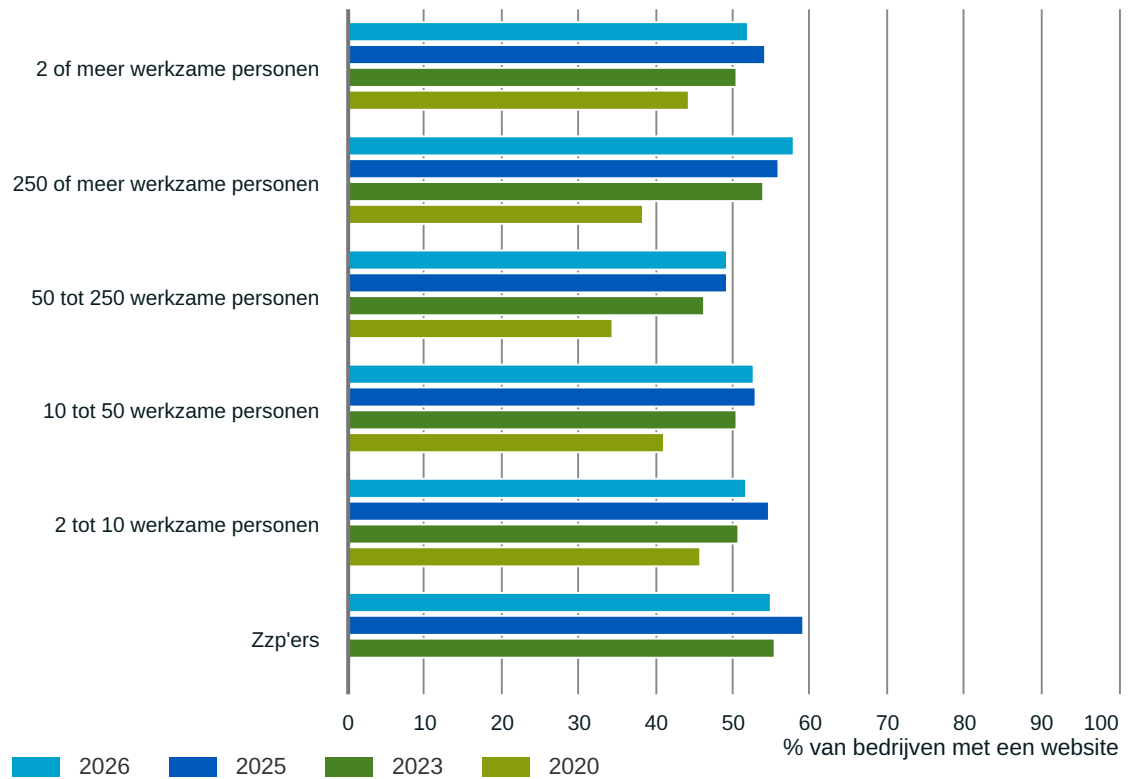


Figuur B.22.: Percentage van bedrijven met een website met geslaagde websitetest 'Gelijke website op IPv4 en IPv6' naar bedrijfstak (2 of meer werkzame personen)

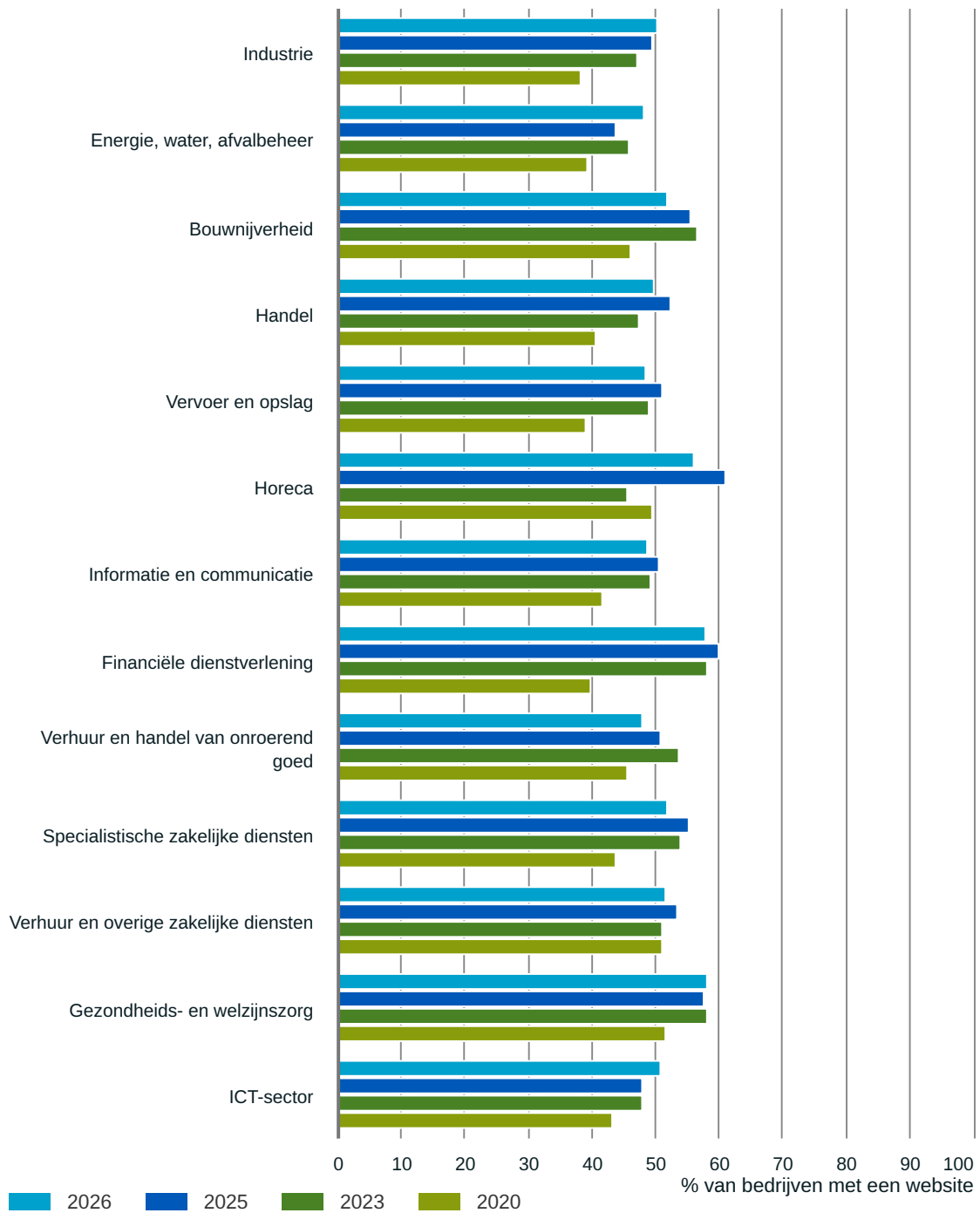


### B.3. Websitescanuitslagen voor categorie DNSSEC

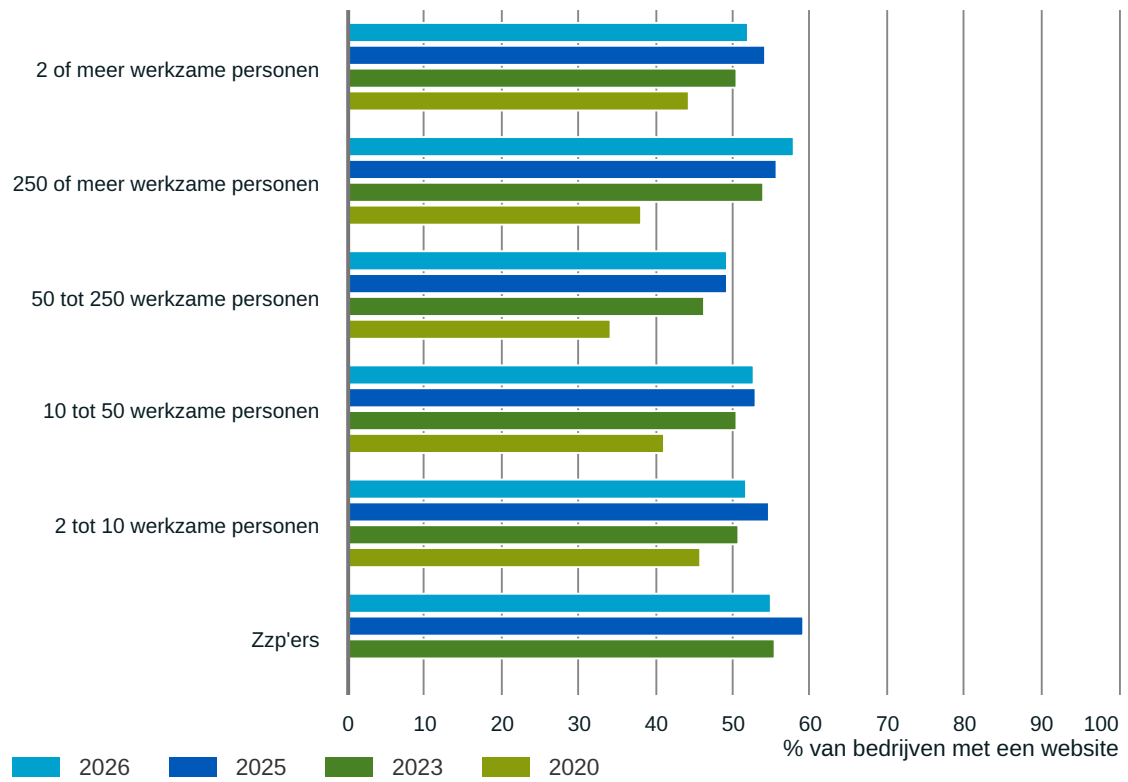
Figuur B.23.: Percentage van bedrijven met een website met geslaagde websitetest 'DNSSEC aanwezig' naar bedrijfsgrootteklasse



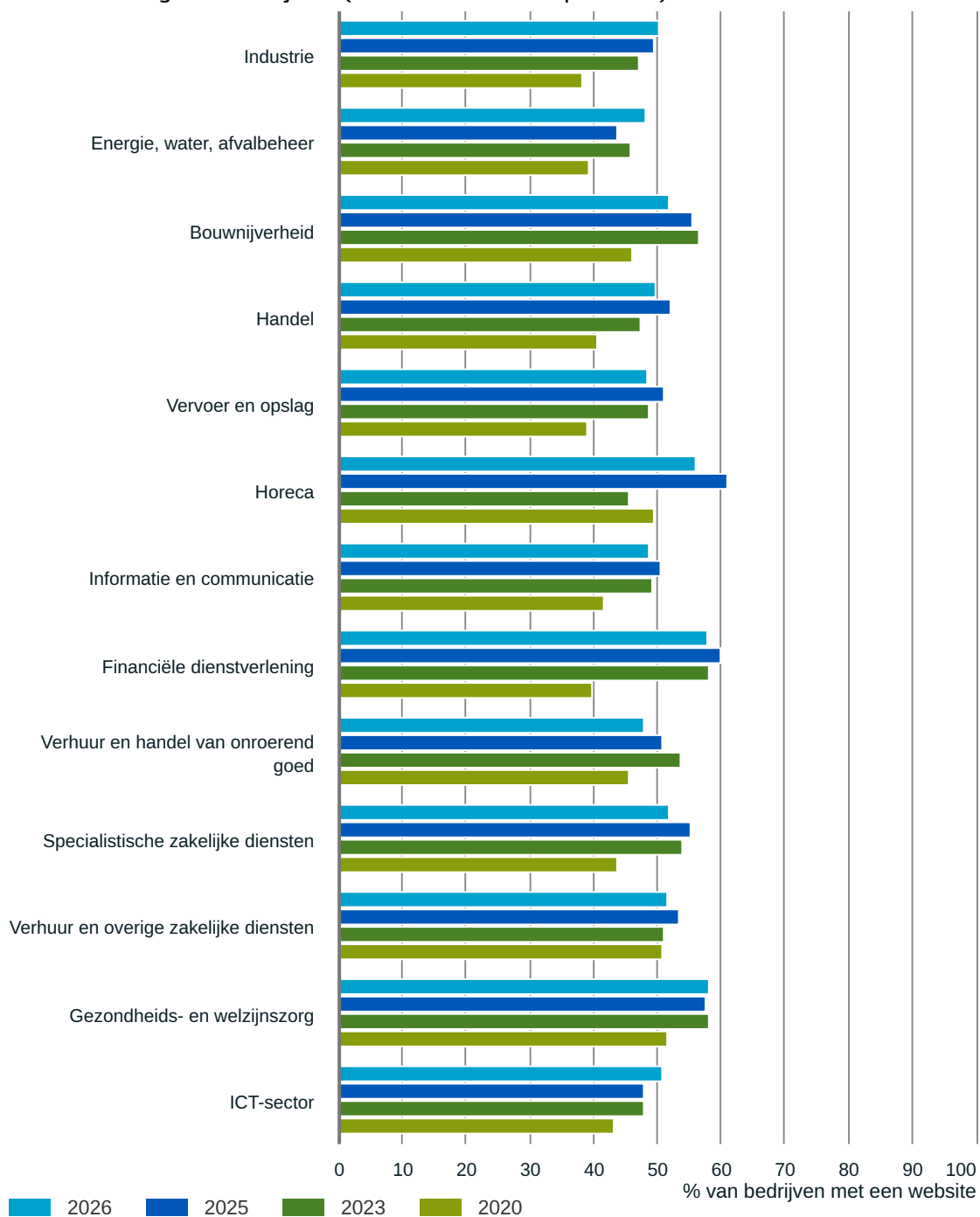
Figuur B.24.: Percentage van bedrijven met een website met geslaagde websitetest 'DNSSEC aanwezig' naar bedrijfstak (2 of meer werkzame personen)



Figuur B.25.: Percentage van bedrijven met een website met geslaagde websitetest 'DNSSEC geldig' naar bedrijfsgrootteklasse

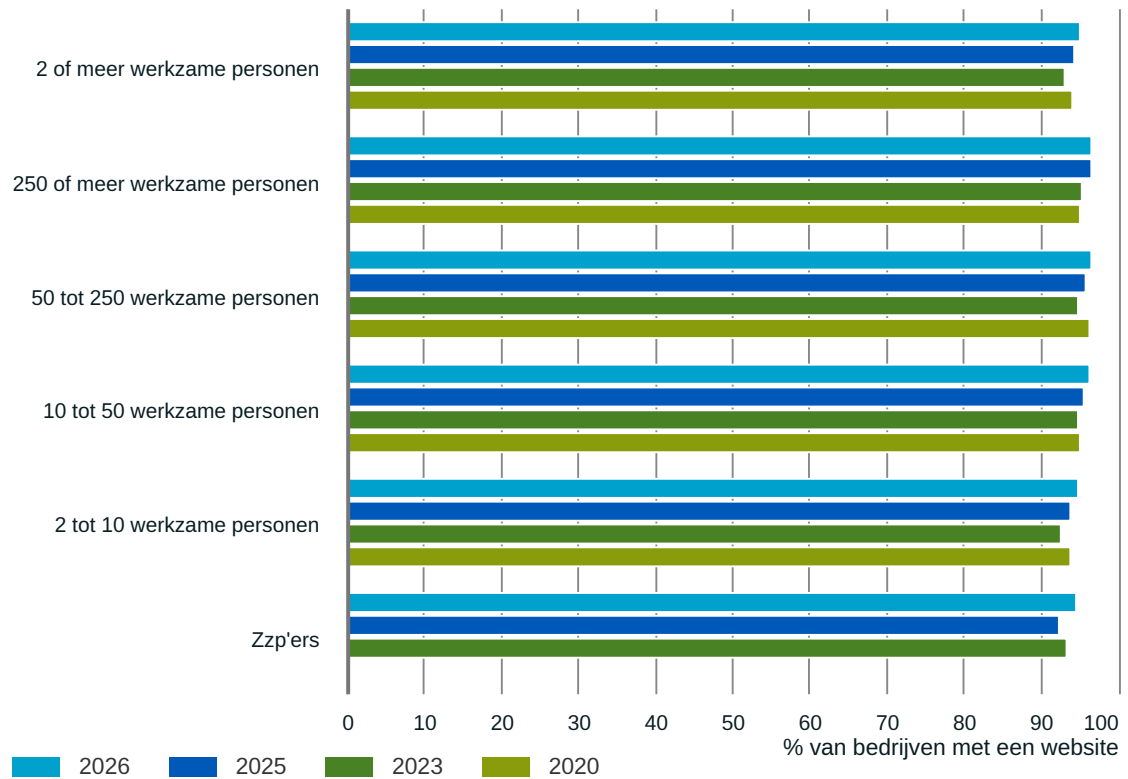


Figuur B.26.: Percentage van bedrijven met een website met geslaagde websitetest 'DNSSEC geldig' naar bedrijfstak (2 of meer werkzame personen)

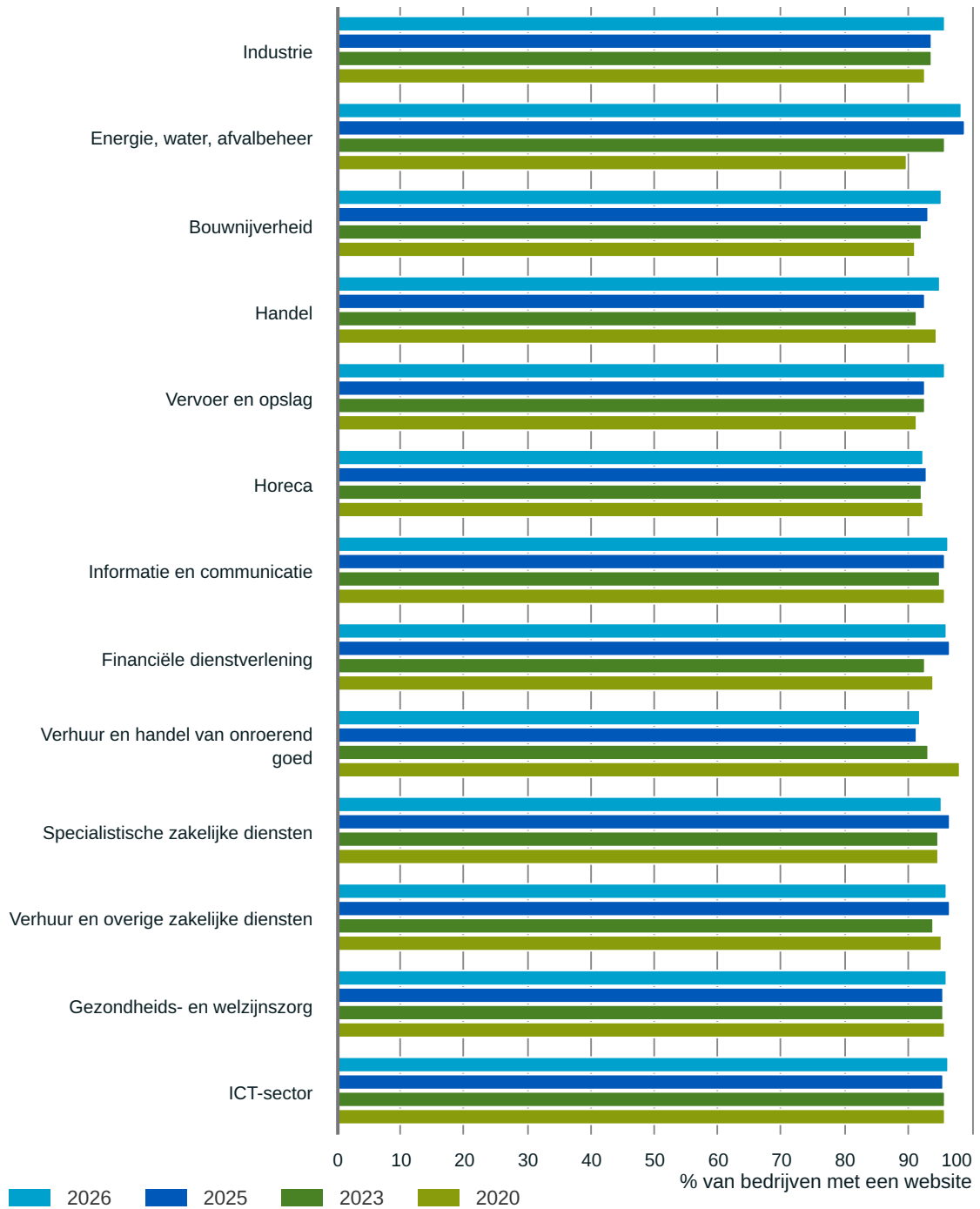


## B.4. Websitescanuitslagen voor categorie HTTPS

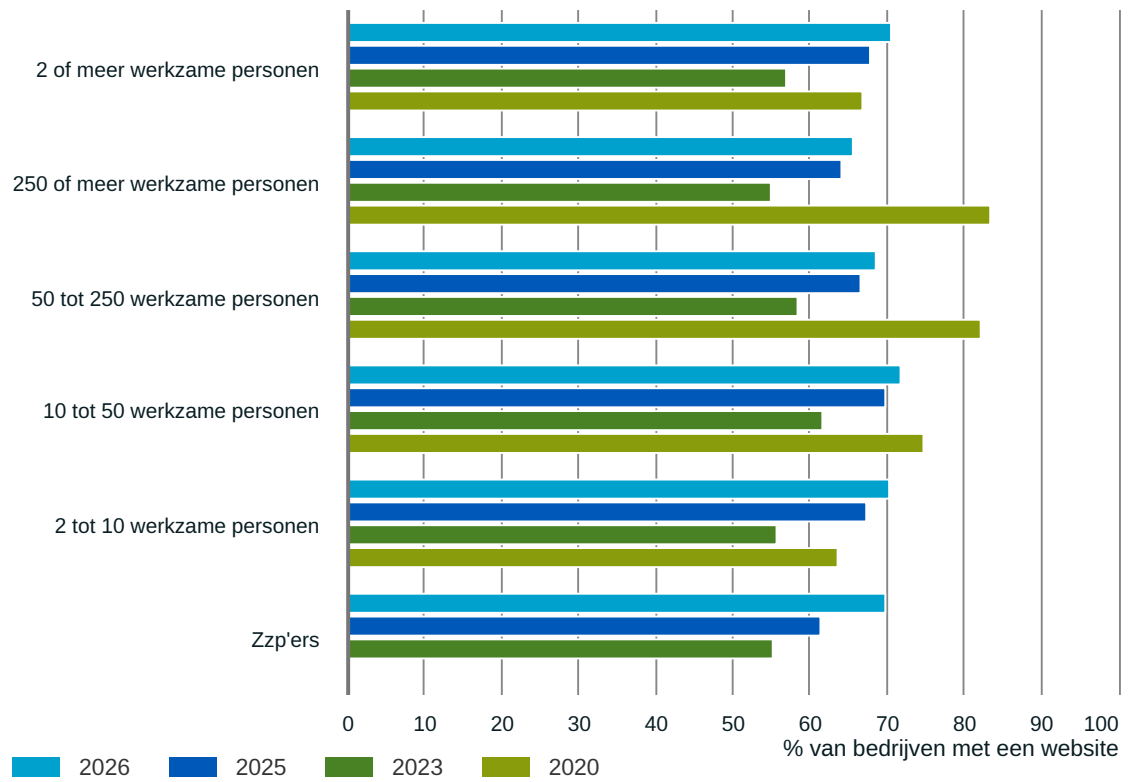
Figuur B.27.: Percentage van bedrijven met een website met geslaagde websitetest 'HTTPS beschikbaar' naar bedrijfsgrootteklasse



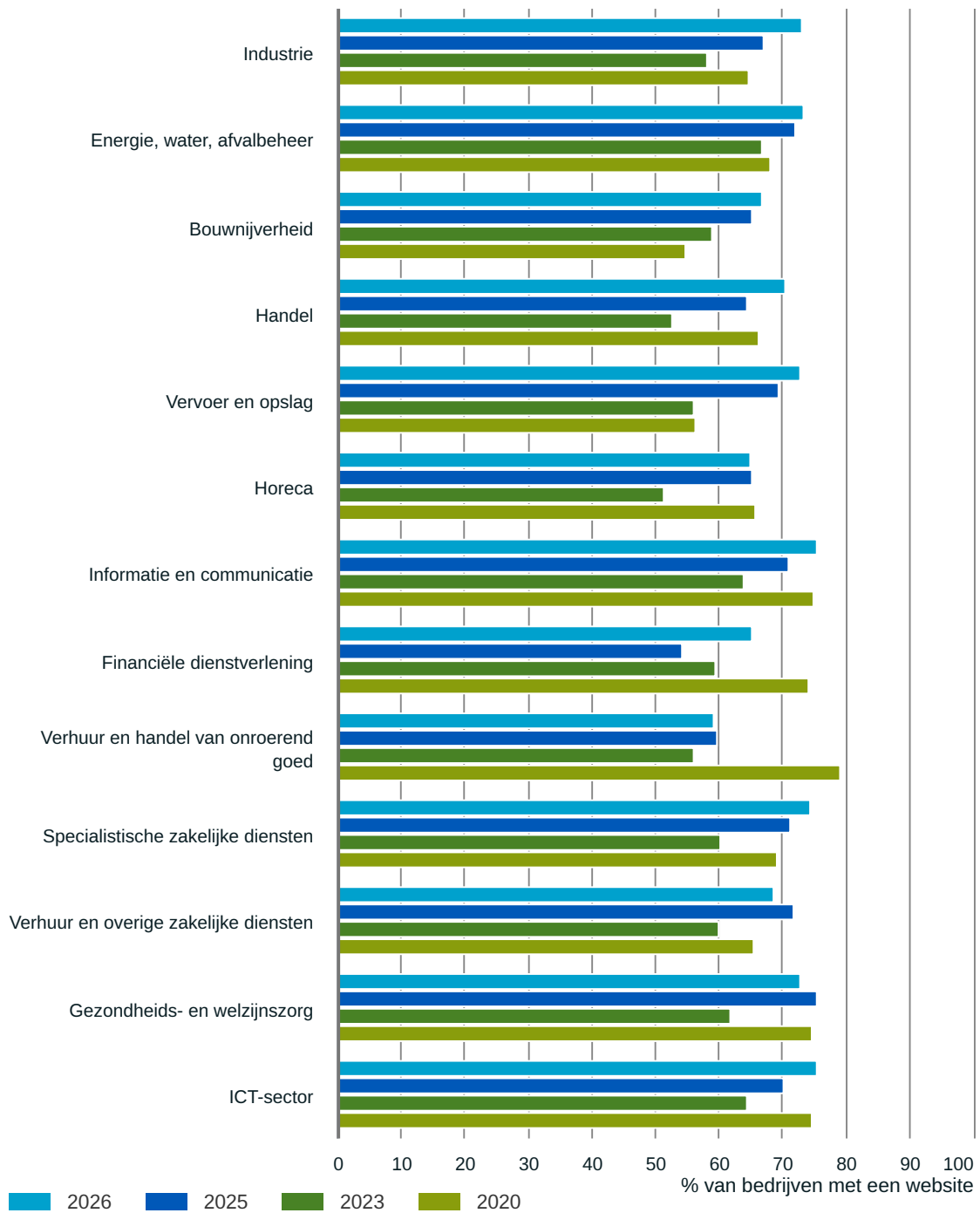
Figuur B.28.: Percentage van bedrijven met een website met geslaagde websitetest 'HTTPS beschikbaar' naar bedrijfstak (2 of meer werkzame personen)



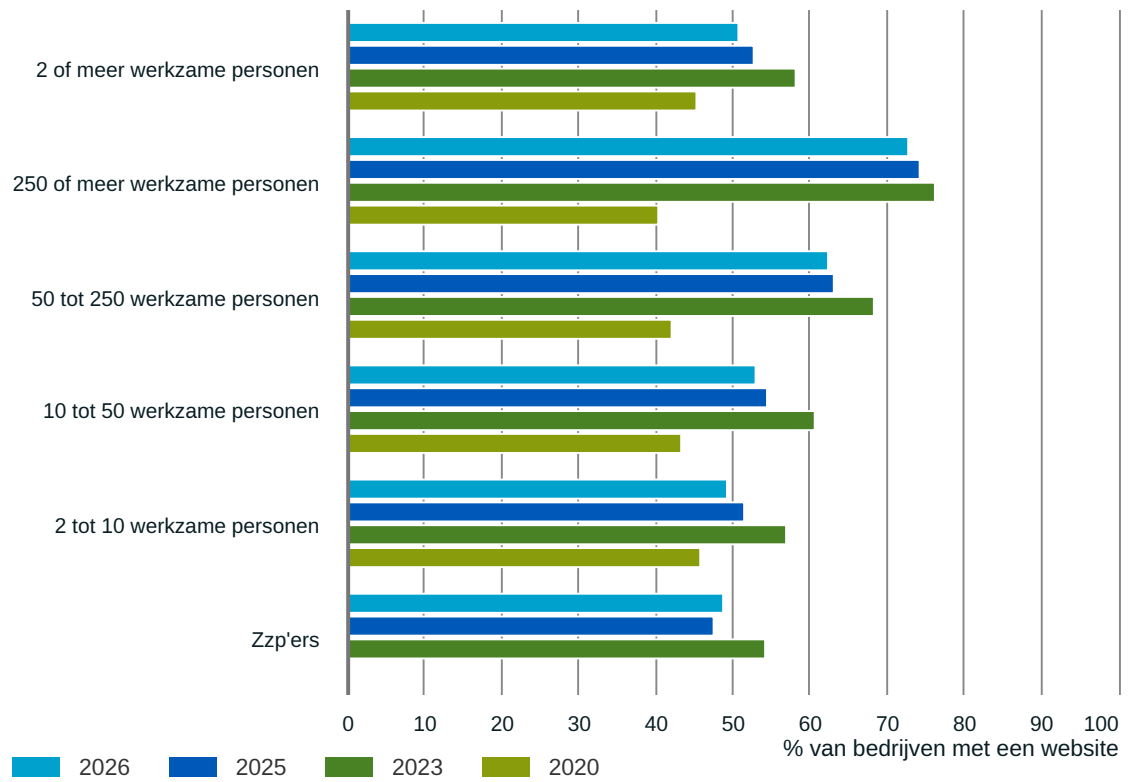
Figuur B.29.: Percentage van bedrijven met een website met geslaagde websitetest 'HTTPS-doorverwijzing' naar bedrijfsgrootteklasse



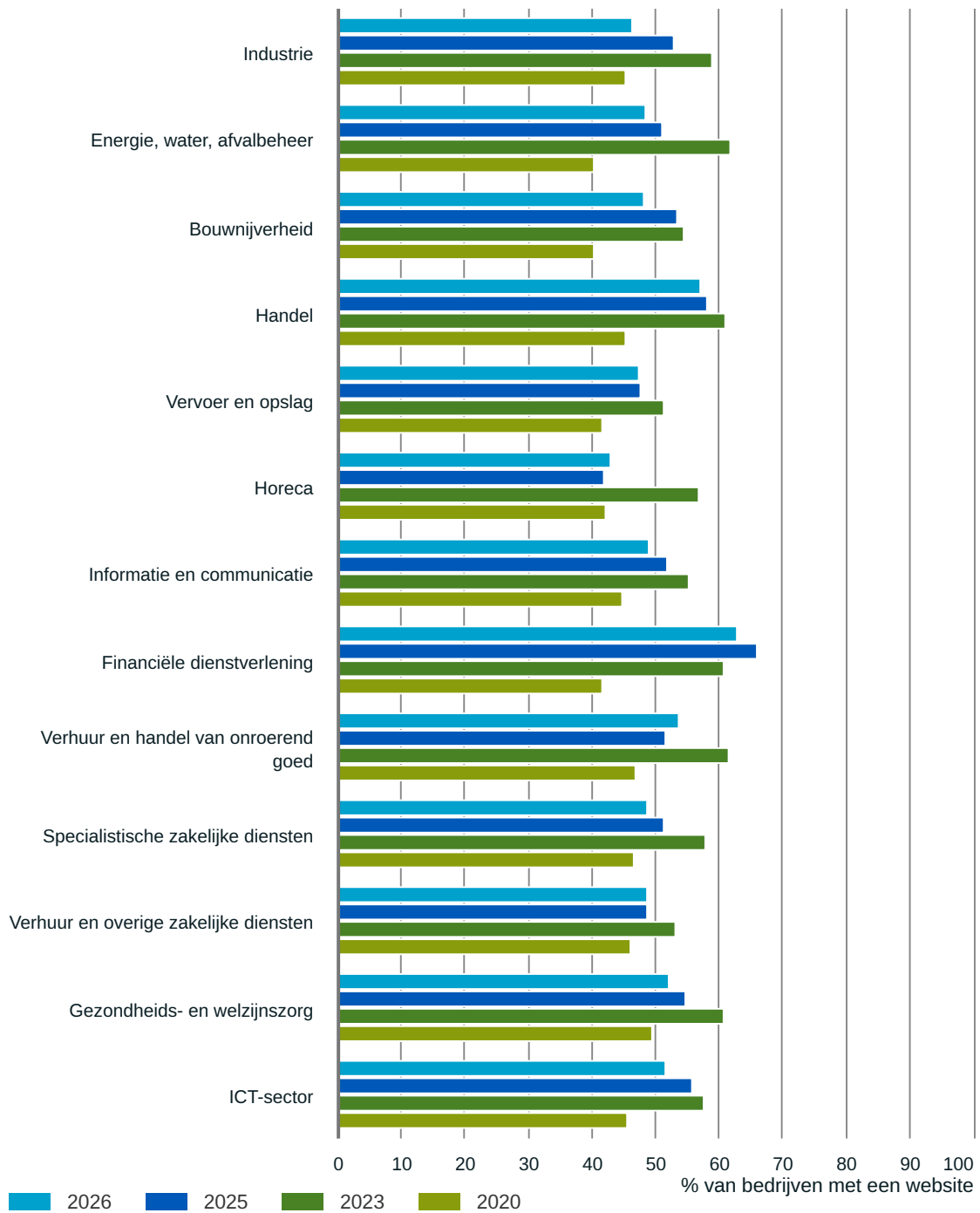
Figuur B.30.: Percentage van bedrijven met een website met geslaagde websitetest 'HTTPS-doorverwijzing' naar bedrijfstak (2 of meer werkzame personen)



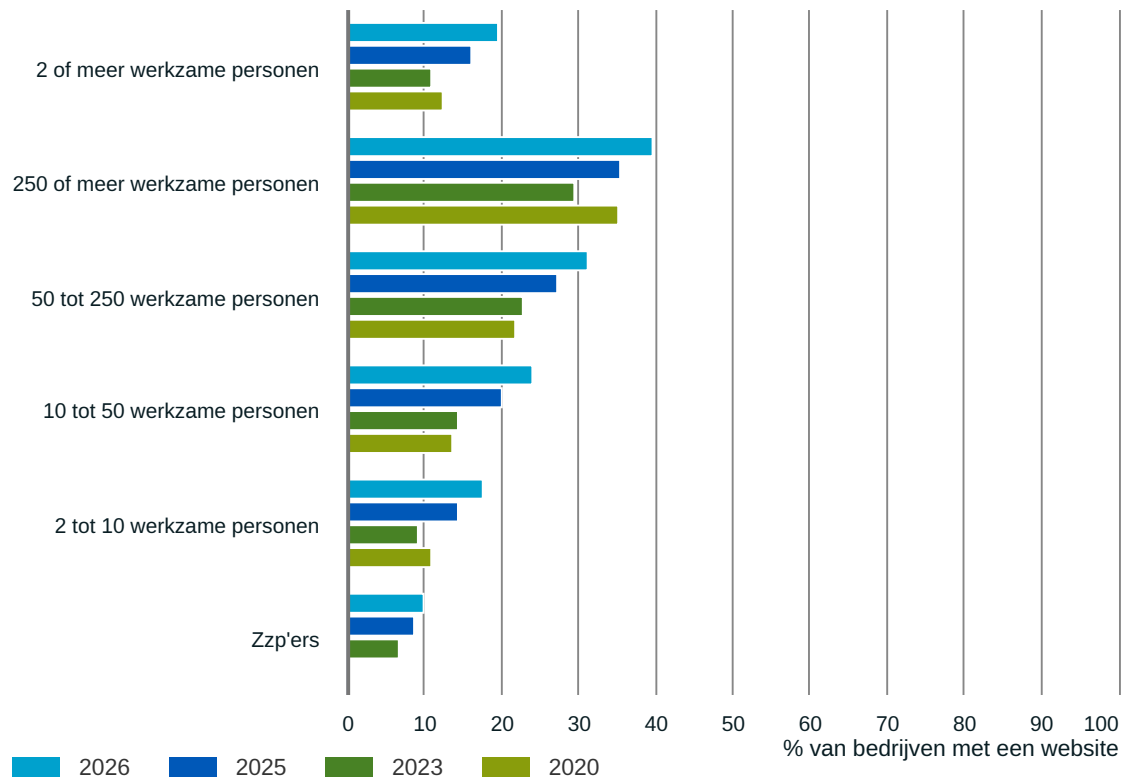
Figuur B.31.: Percentage van bedrijven met een website met geslaagde websitetest 'HTTP-compressie' naar bedrijfsgrootteklasse



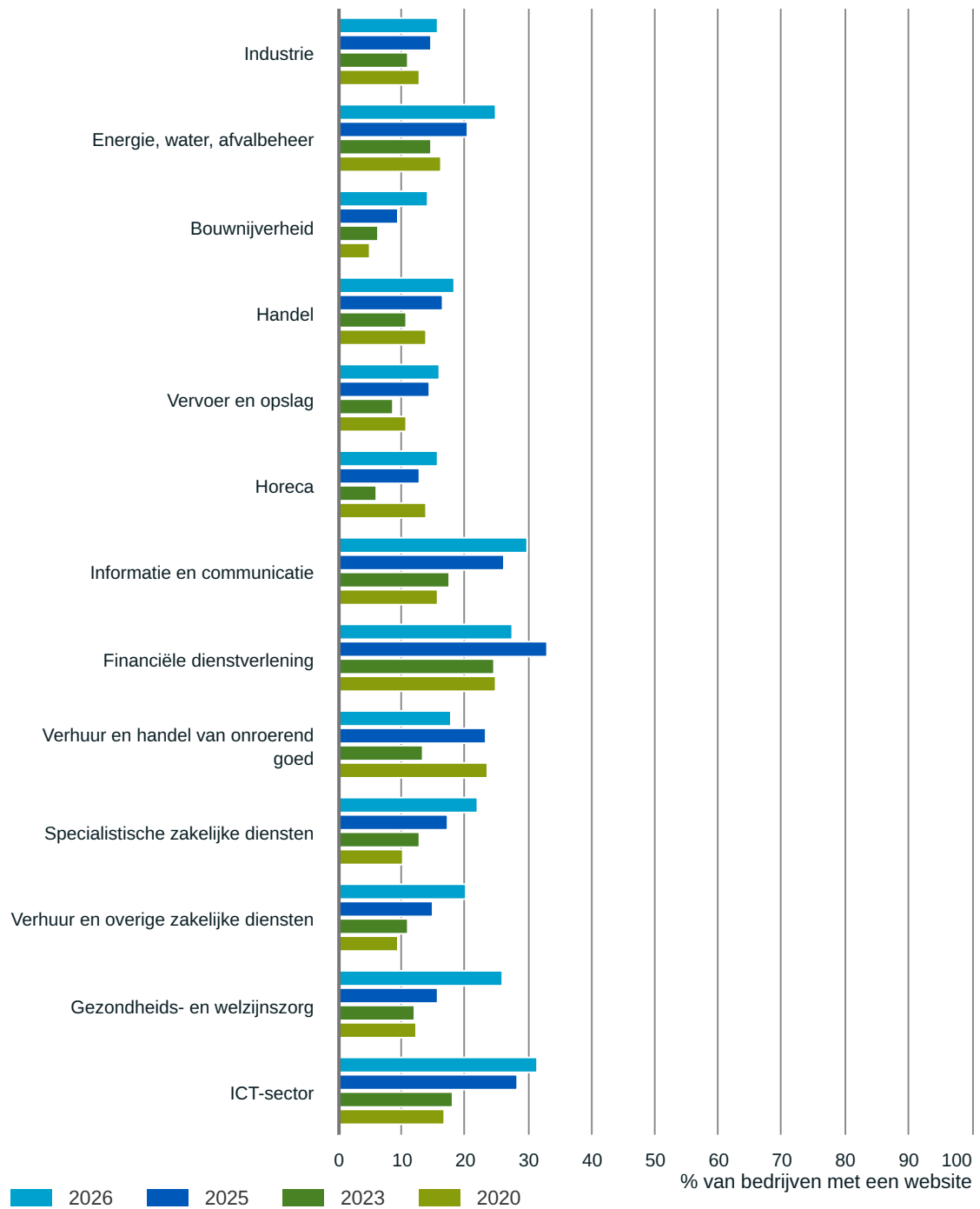
Figuur B.32.: Percentage van bedrijven met een website met geslaagde websitetest 'HTTP-compressie' naar bedrijfstak (2 of meer werkzame personen)



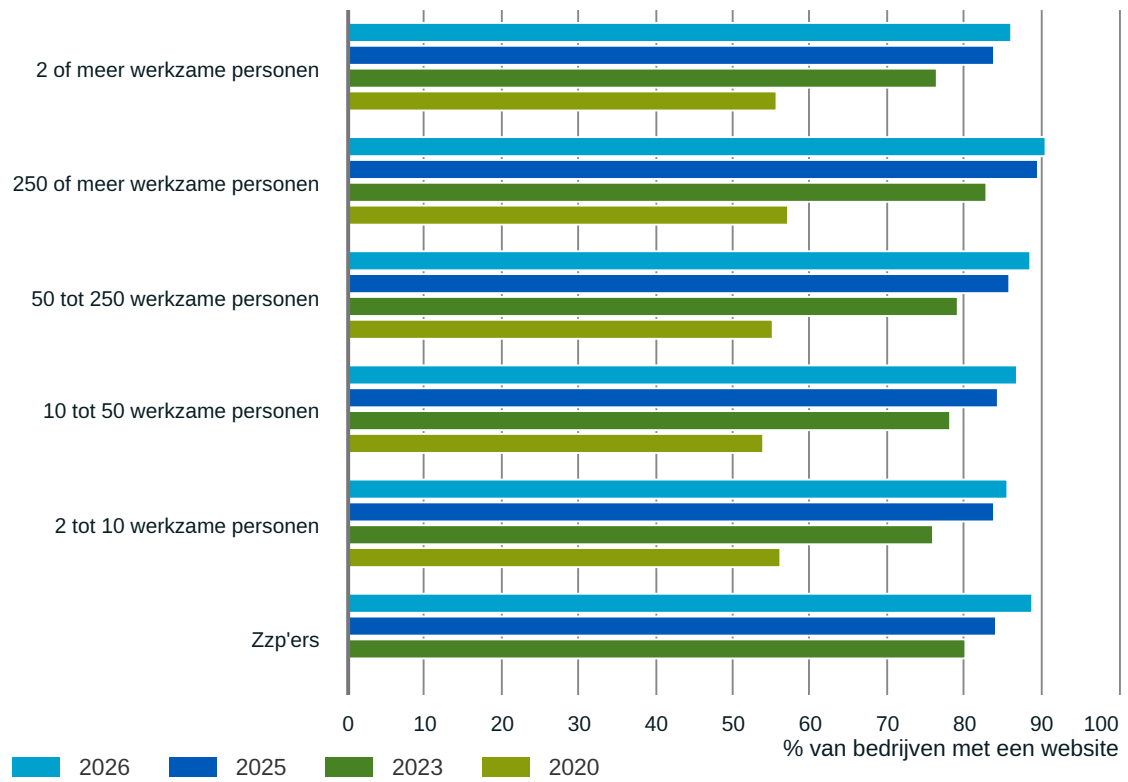
Figuur B.33.: Percentage van bedrijven met een website met geslaagde websitetest 'HSTS' naar bedrijfsgrootteklasse



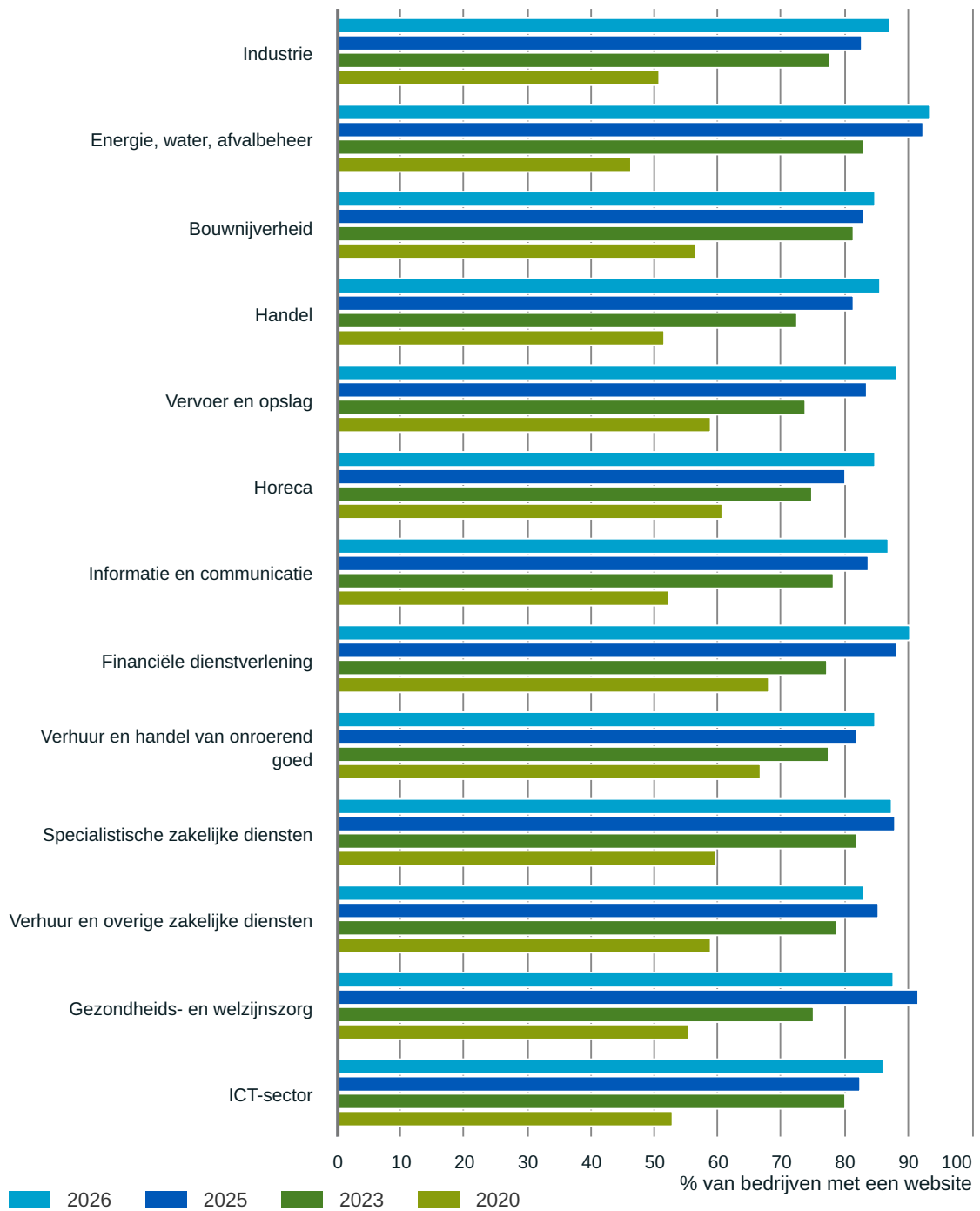
Figuur B.34.: Percentage van bedrijven met een website met geslaagde websitetest 'HSTS' naar bedrijfstak (2 of meer werkzame personen)



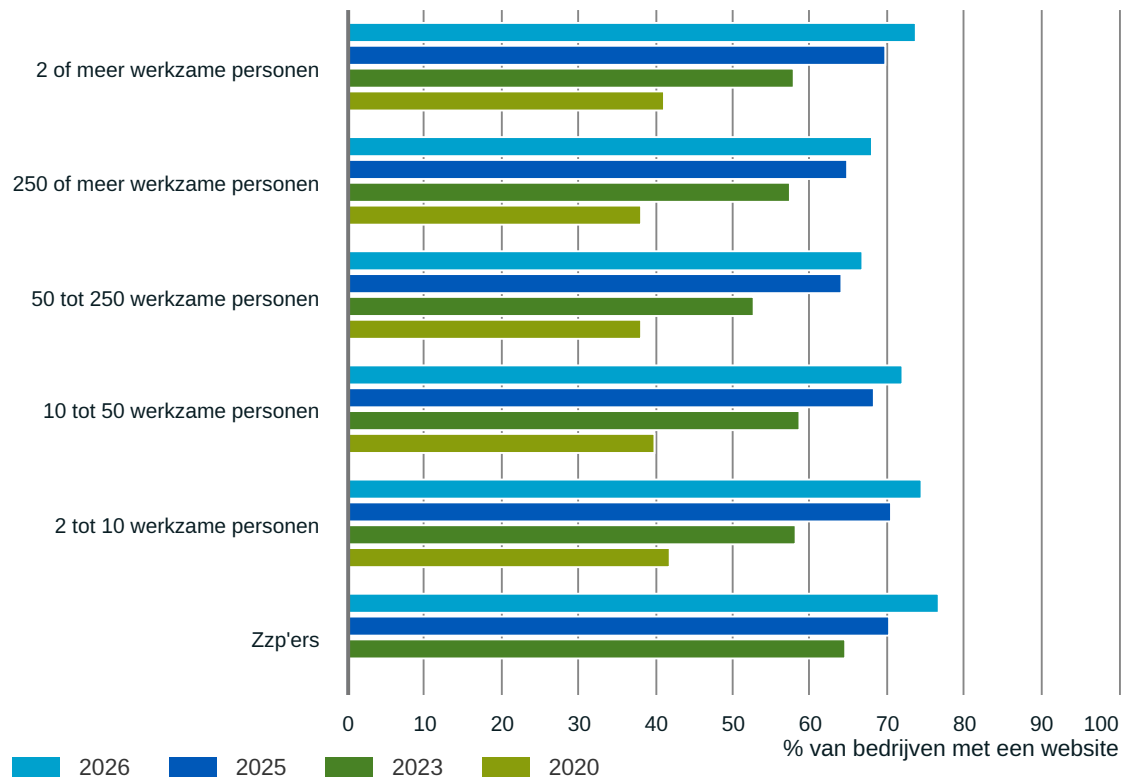
Figuur B.35.: Percentage van bedrijven met een website met geslaagde websitetest 'TLS-versie' naar bedrijfsgrootteklasse



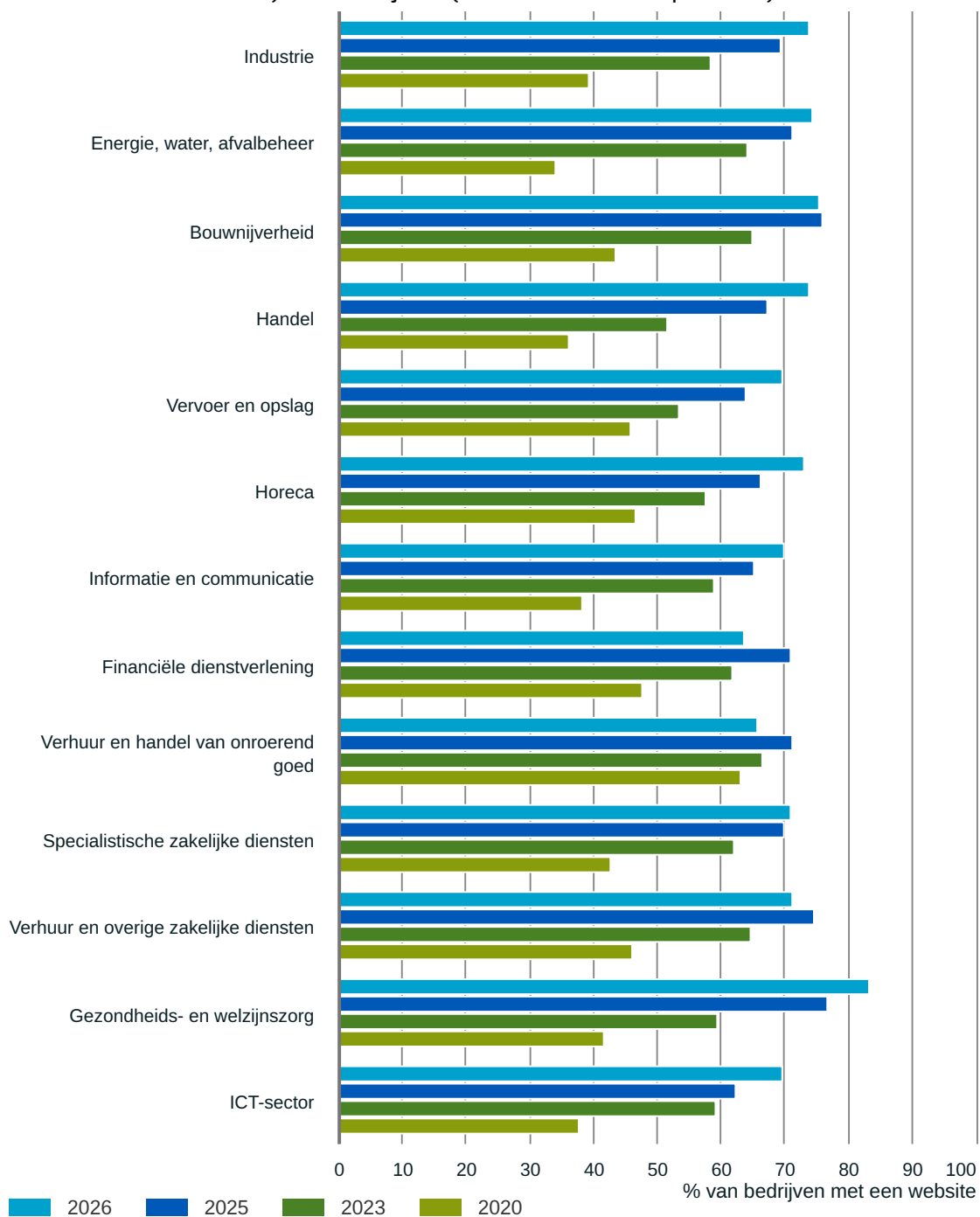
Figuur B.36.: Percentage van bedrijven met een website met geslaagde websitetest 'TLS-versie' naar bedrijfstak (2 of meer werkzame personen)



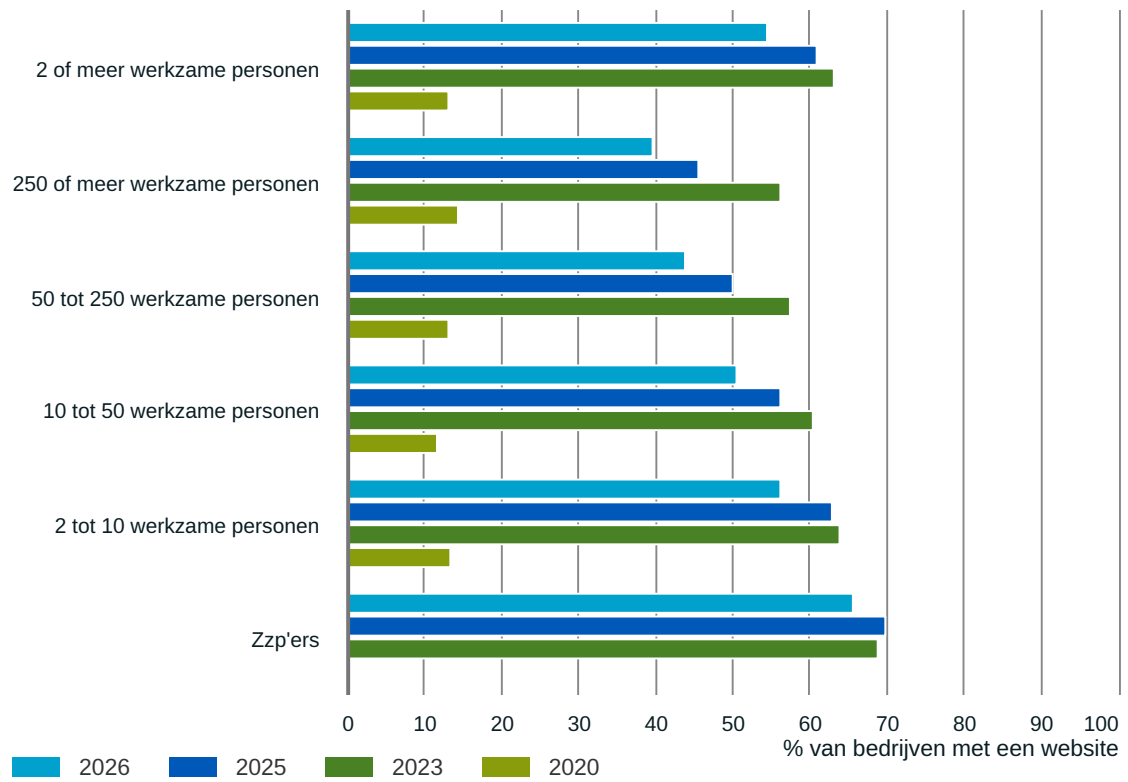
Figuur B.37.: Percentage van bedrijven met een website met geslaagde websitetest 'Ciphers (algoritmeselectie)' naar bedrijfsgrootteklasse



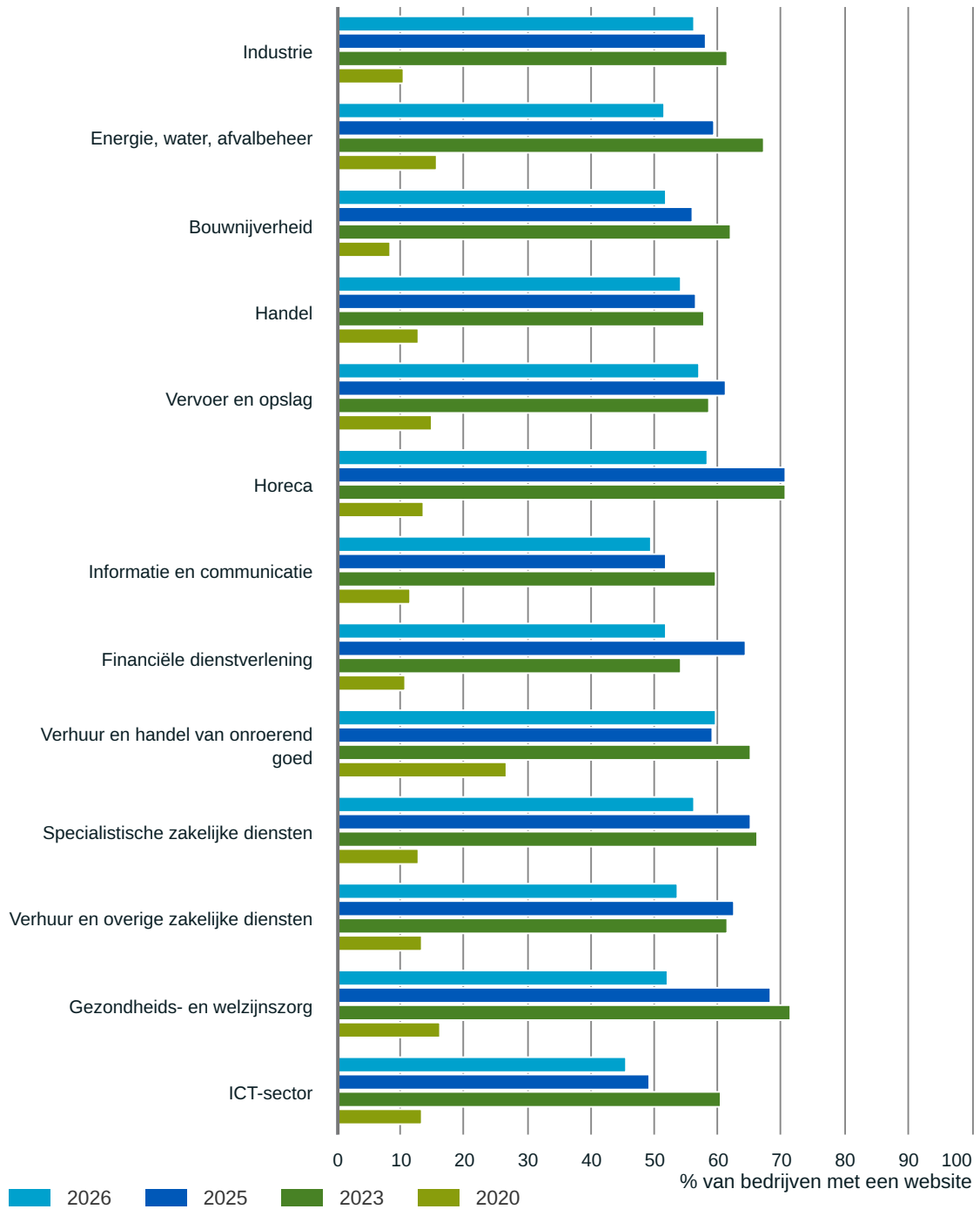
Figuur B.38.: Percentage van bedrijven met een website met geslaagde websitetest 'Ciphers (algoritmeselectie)' naar bedrijfstak (2 of meer werkzame personen)



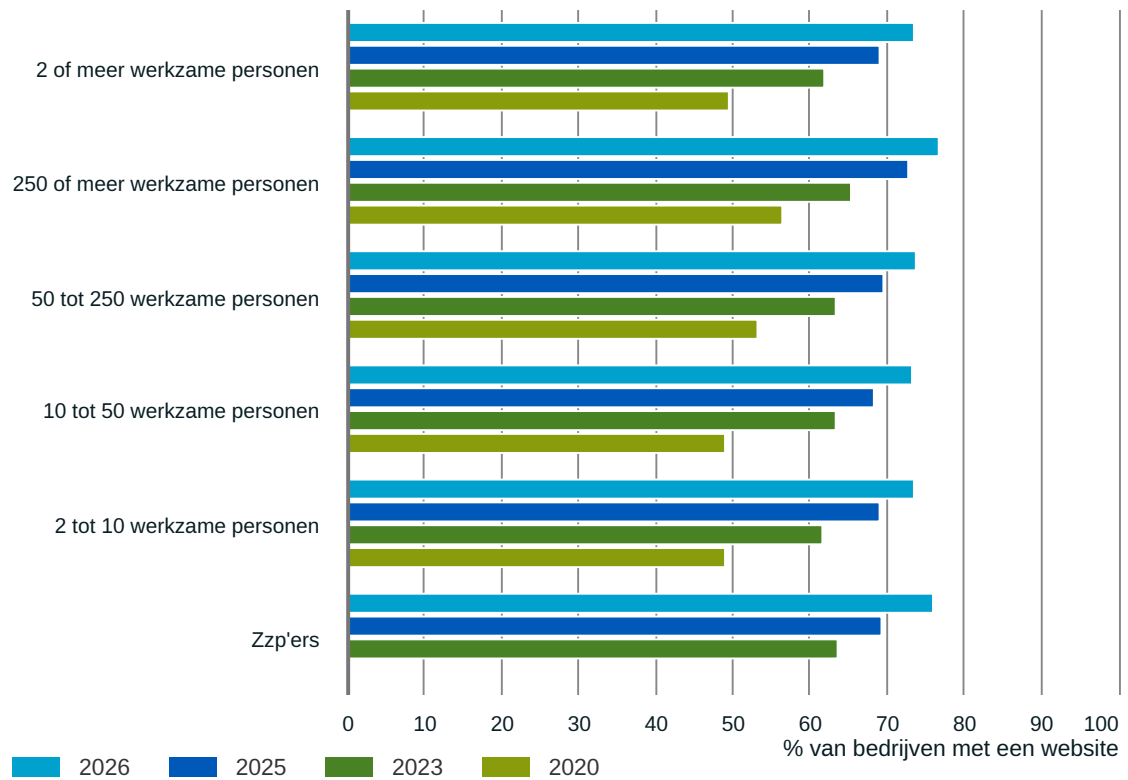
Figuur B.39.: Percentage van bedrijven met een website met geslaagde websitetest 'Cijfer-  
volgorde' naar bedrijfsgrootteklasse



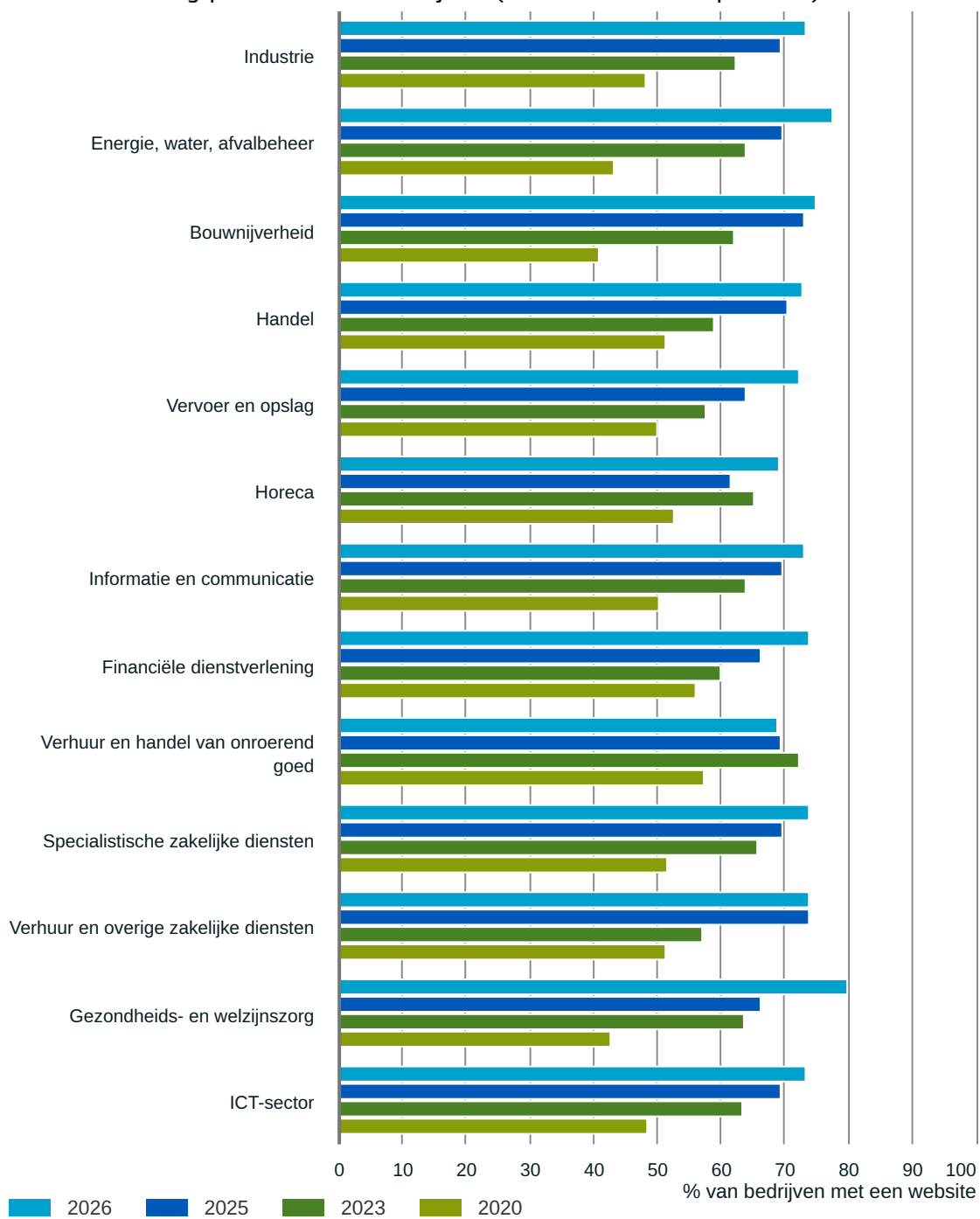
Figuur B.40.: Percentage van bedrijven met een website met geslaagde websitetest 'Cijfer-  
volgorde' naar bedrijfstak (2 of meer werkzame personen)



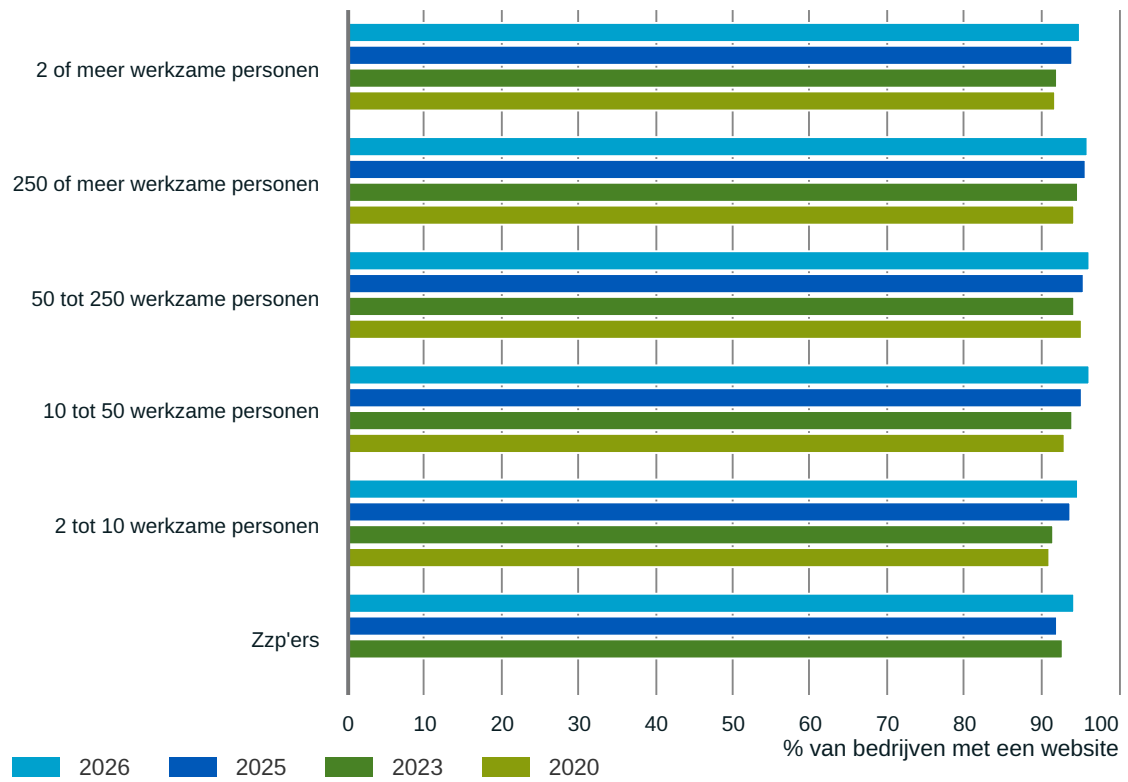
Figuur B.41.: Percentage van bedrijven met een website met geslaagde websitetest 'Sleuteluitwisselingsparameters' naar bedrijfsgrootteklasse



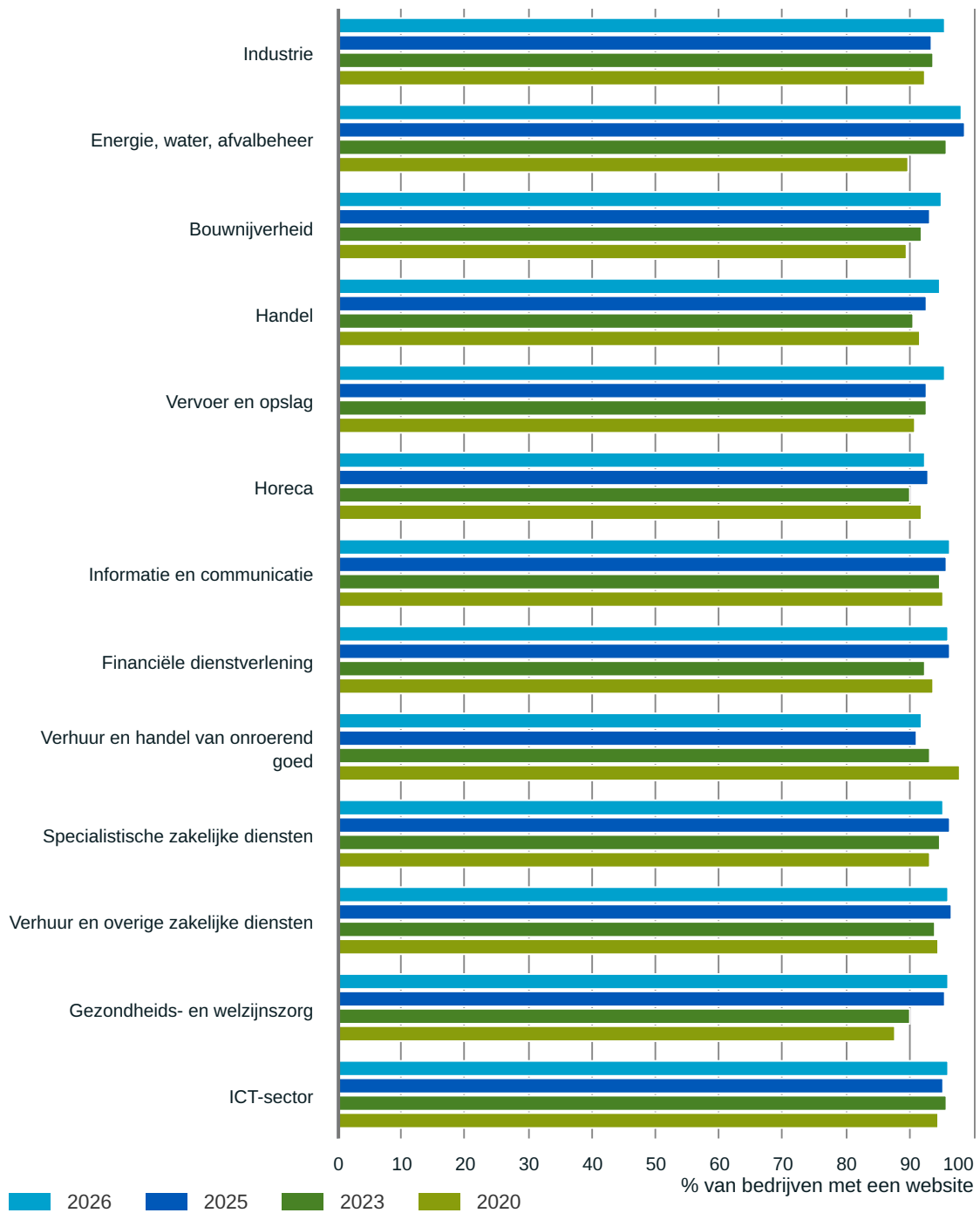
Figuur B.42.: Percentage van bedrijven met een website met geslaagde websitetest 'Sleuteluitwisselingsparameters' naar bedrijfstak (2 of meer werkzame personen)



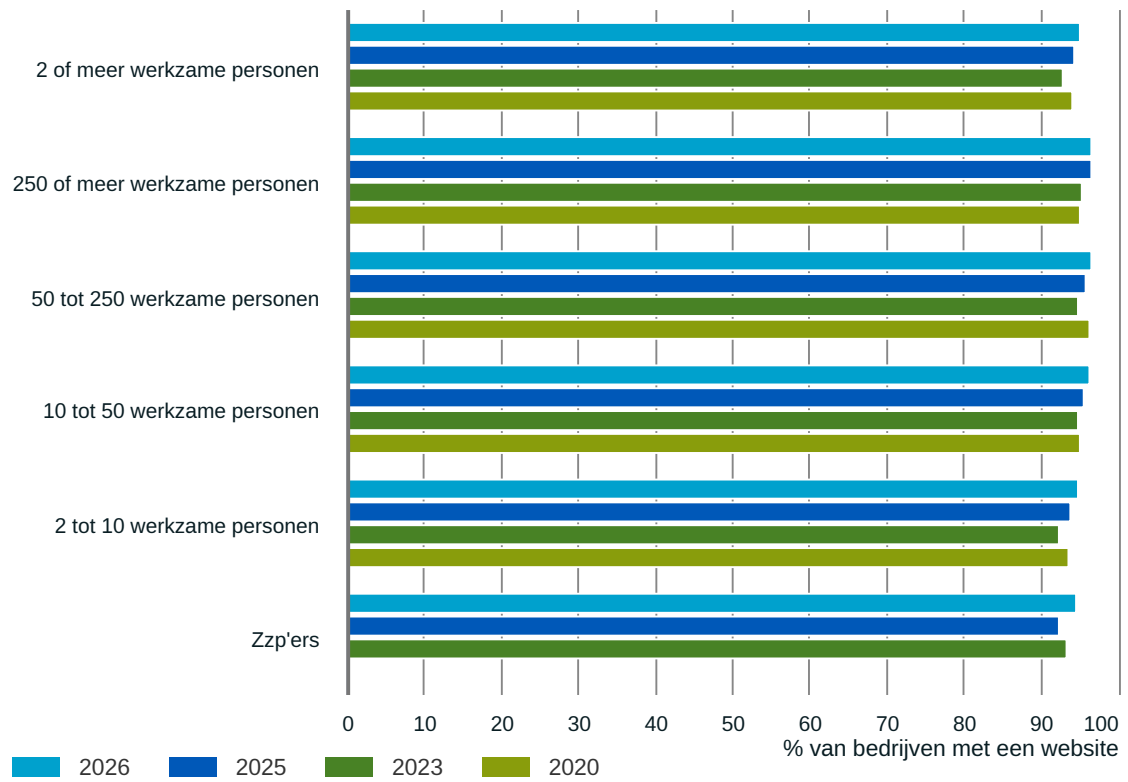
Figuur B.43.: Percentage van bedrijven met een website met geslaagde websitetest 'Hashfunctie voor sleuteluitwisseling' naar bedrijfsgrootteklasse



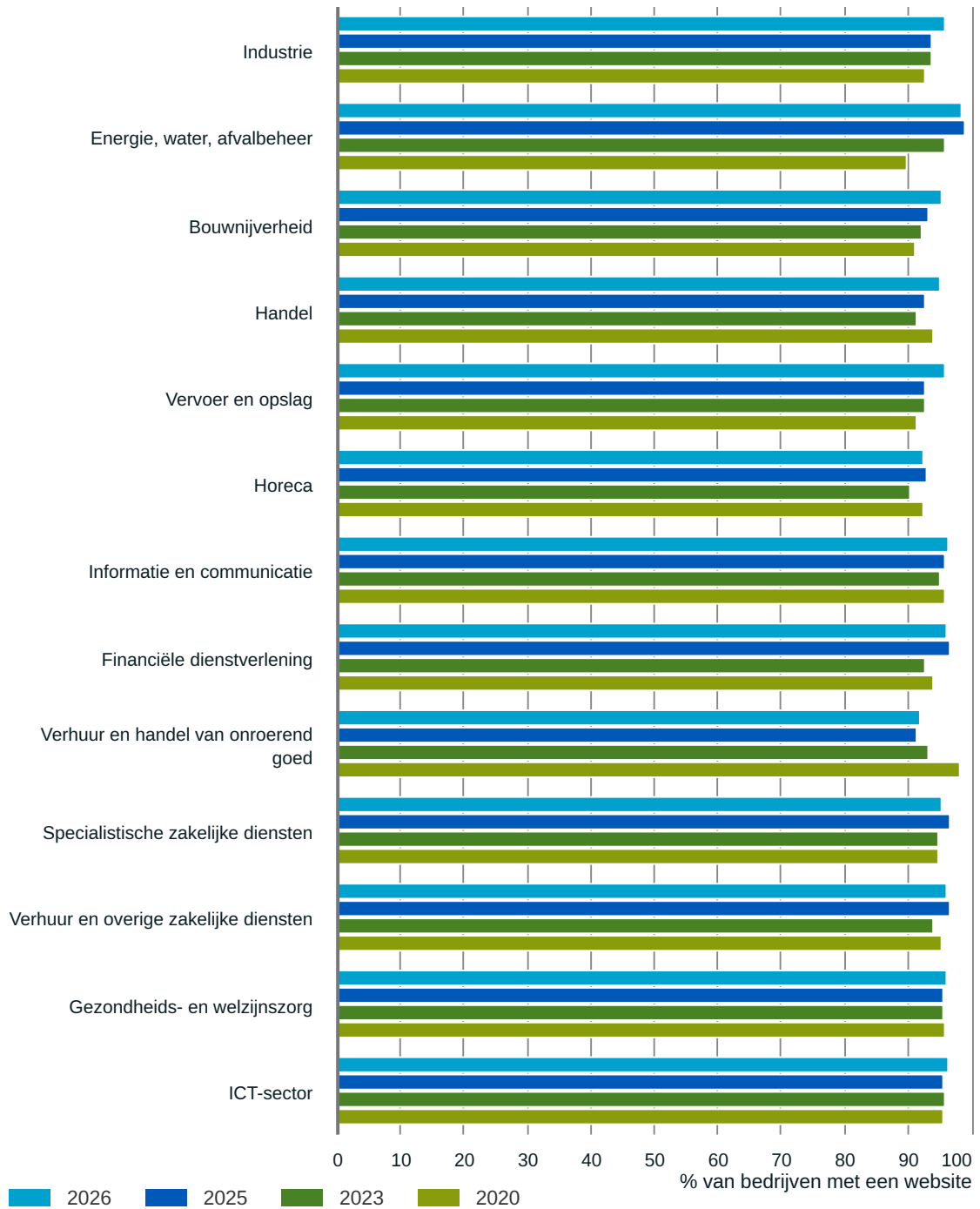
Figuur B.44.: Percentage van bedrijven met een website met geslaagde websitetest 'Hashfunctie voor sleuteluitwisseling' naar bedrijfstak (2 of meer werkzame personen)



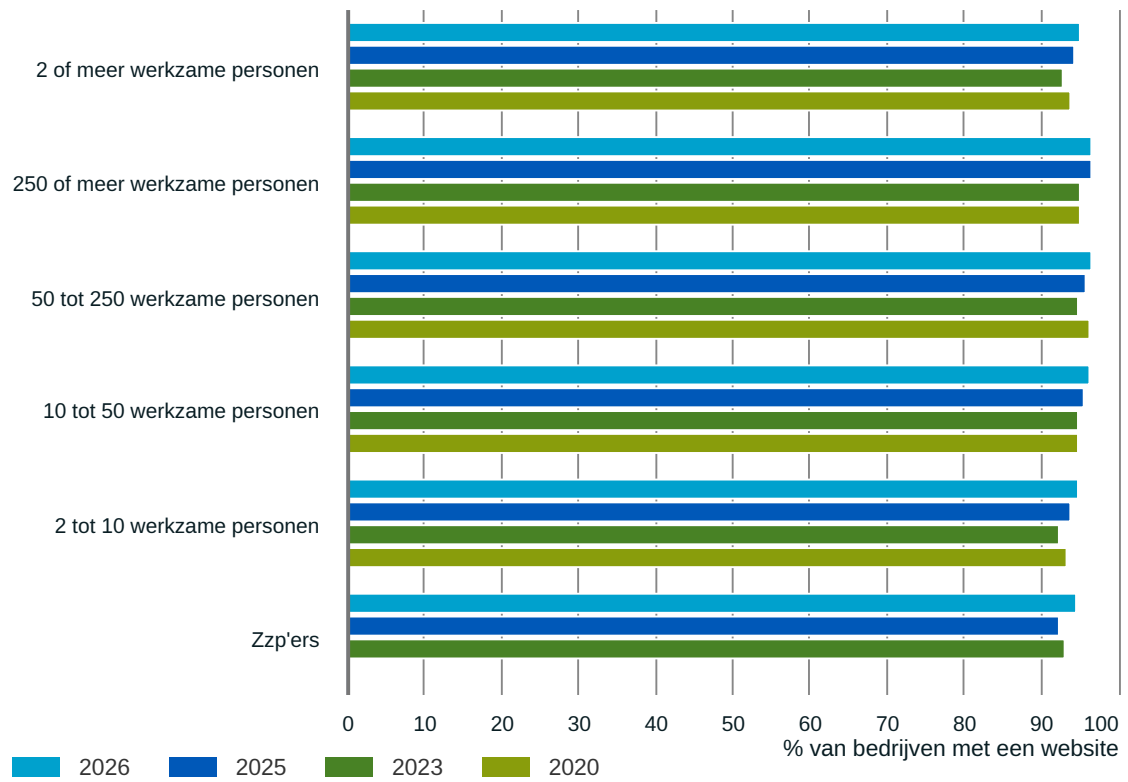
Figuur B.45.: Percentage van bedrijven met een website met geslaagde websitetest 'TLS-compressie' naar bedrijfsgrootteklasse



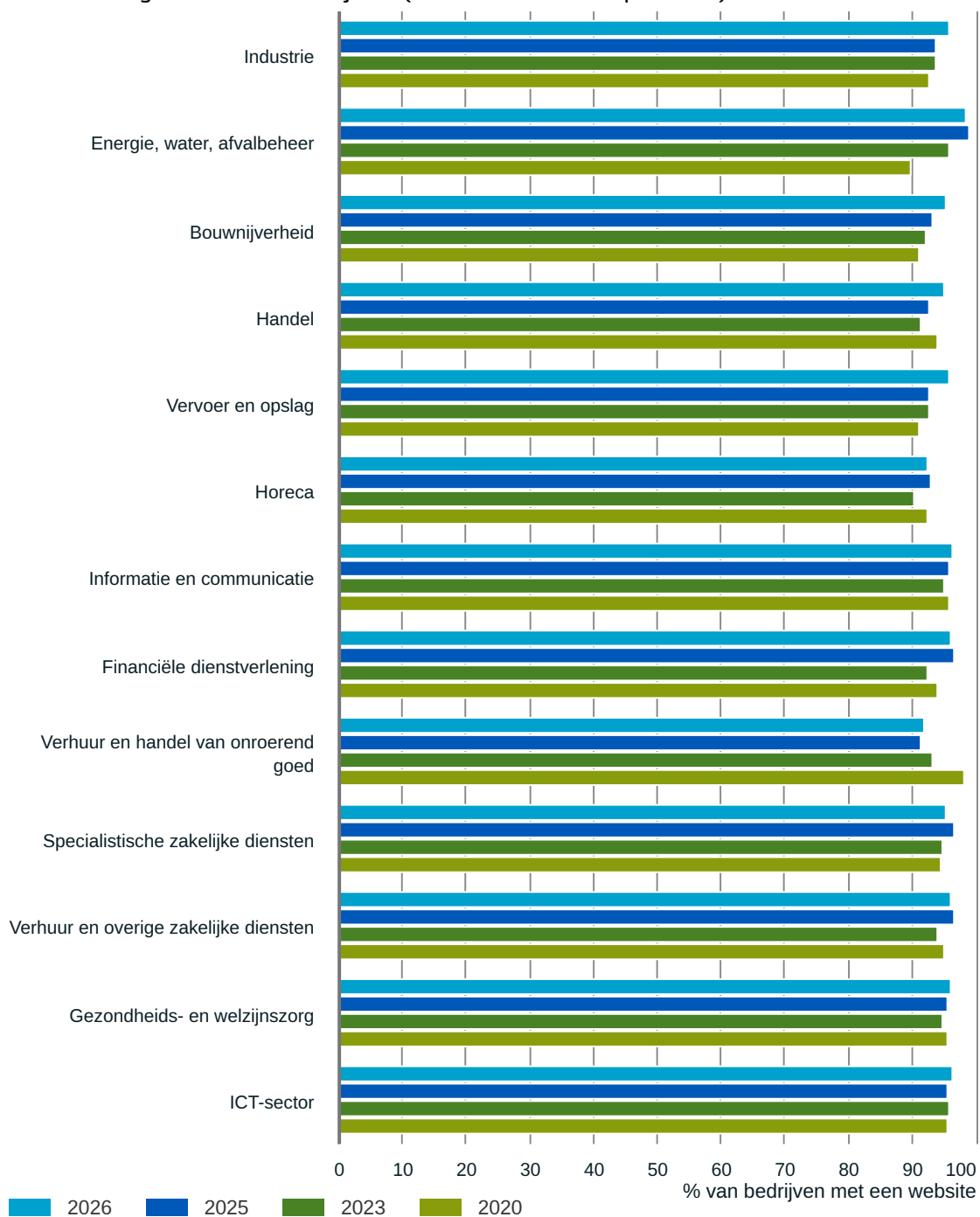
Figuur B.46.: Percentage van bedrijven met een website met geslaagde websitetest 'TLS-compressie' naar bedrijfstak (2 of meer werkzame personen)



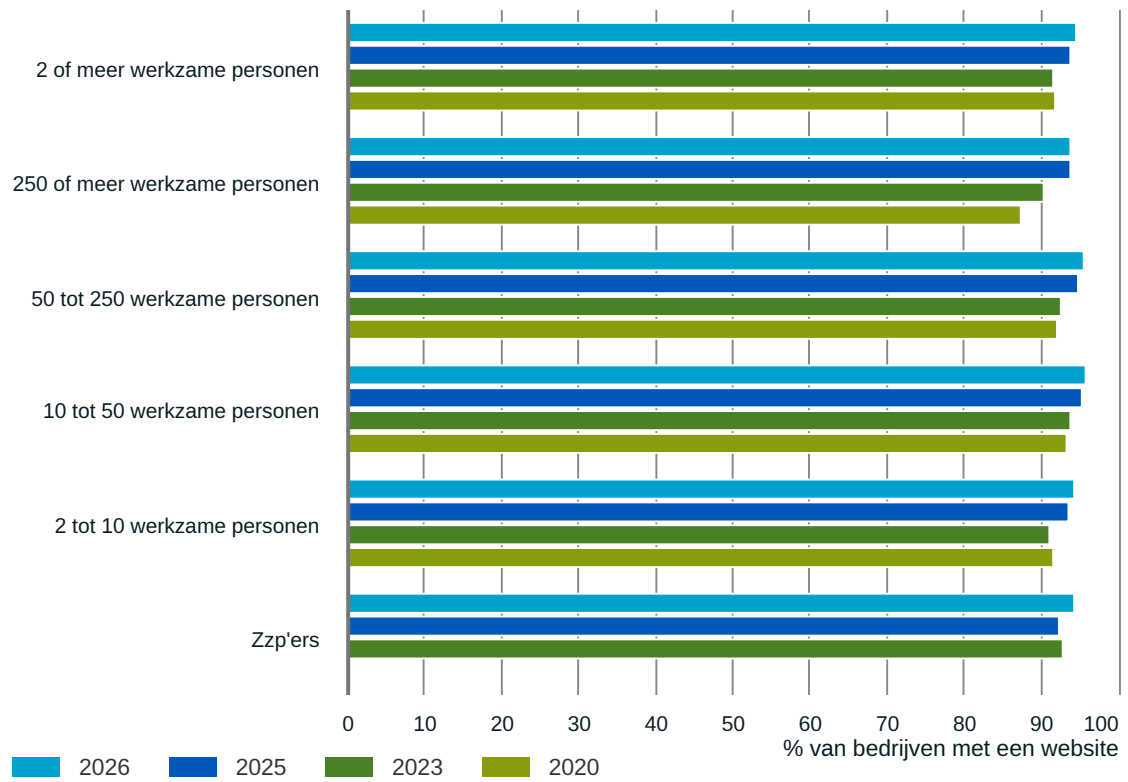
Figuur B.47.: Percentage van bedrijven met een website met geslaagde websitetest 'Secure renegotiation' naar bedrijfsgrootteklasse



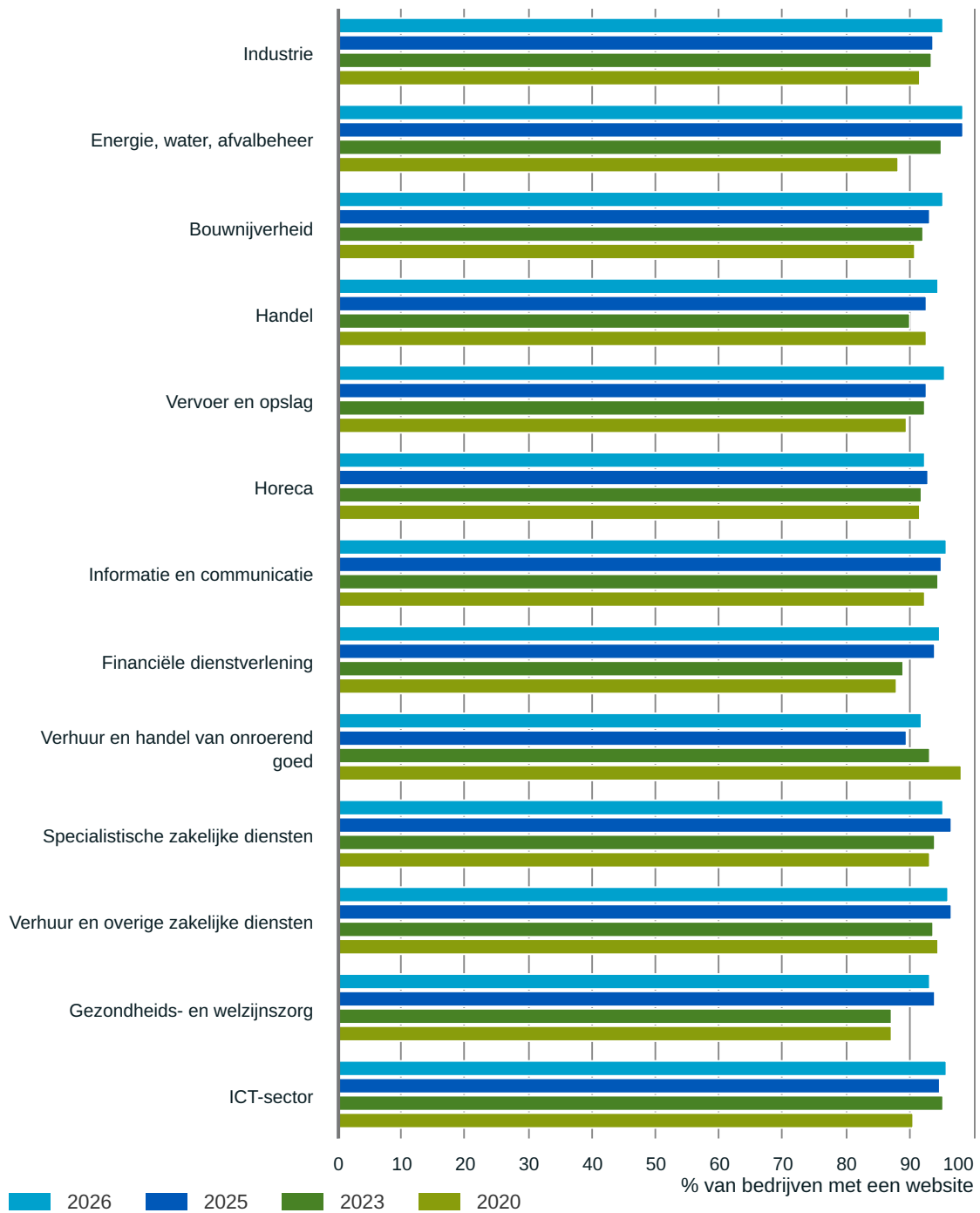
Figuur B.48.: Percentage van bedrijven met een website met geslaagde websitetest 'Secure renegotiation' naar bedrijfstak (2 of meer werkzame personen)



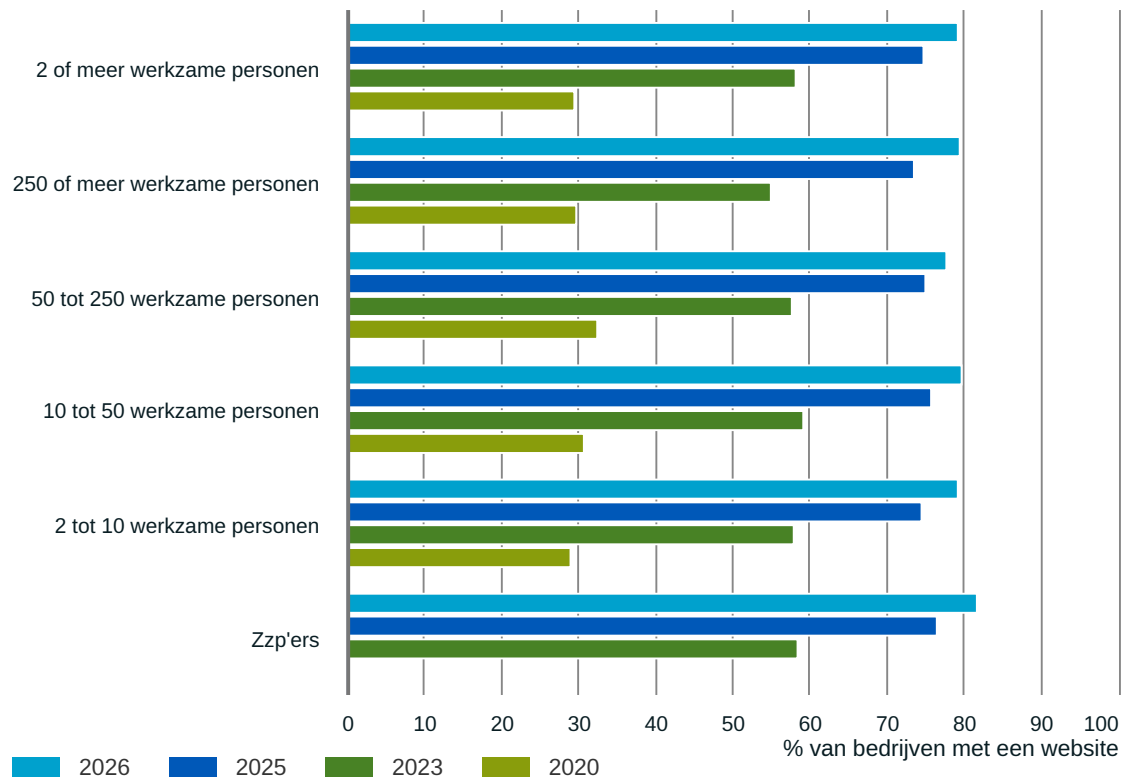
Figuur B.49.: Percentage van bedrijven met een website met geslaagde websitetest 'Client initiated renegotiation' naar bedrijfsgrootteklasse



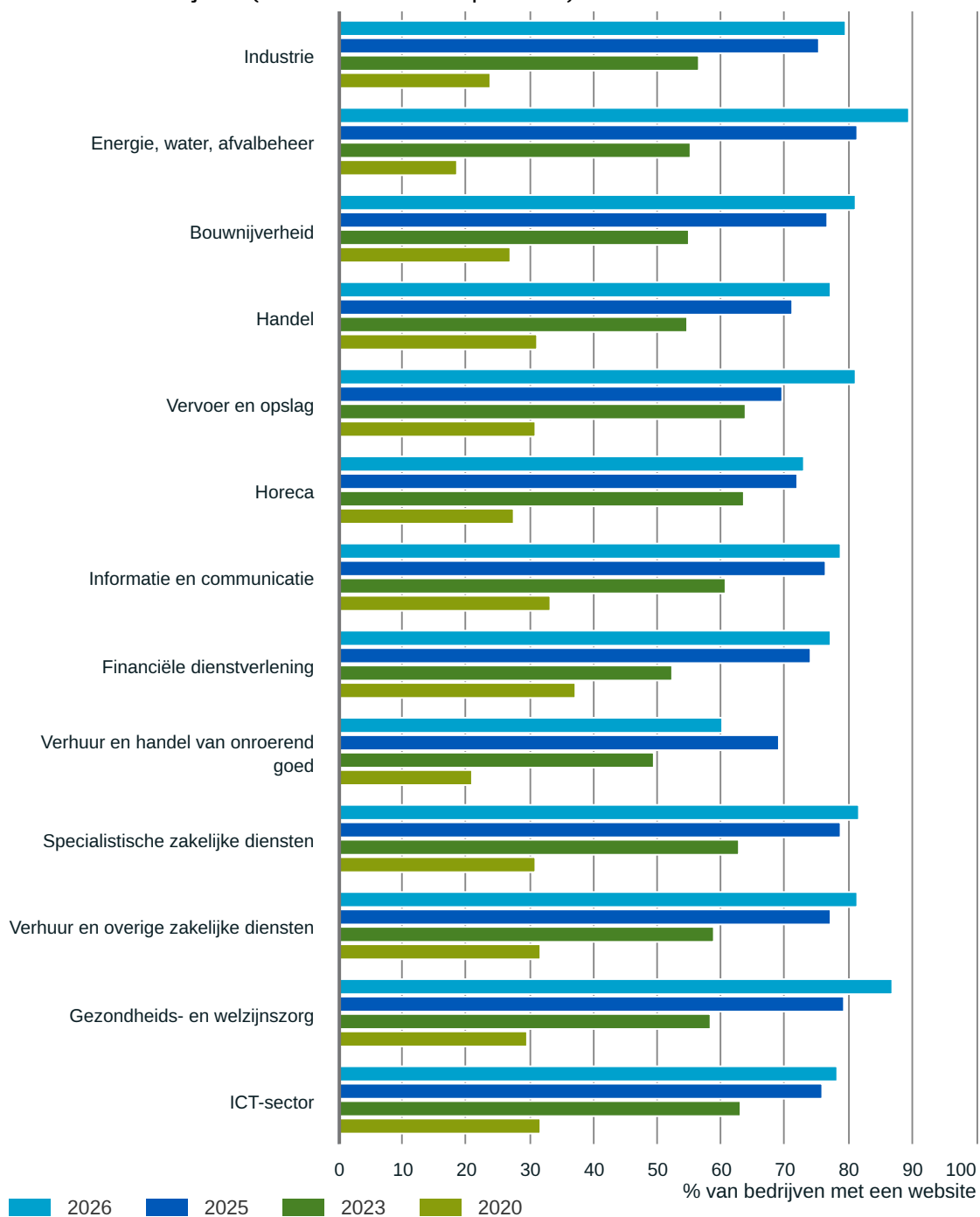
Figuur B.50.: Percentage van bedrijven met een website met geslaagde websitetest 'Client initiated renegotiation' naar bedrijfstak (2 of meer werkzame personen)



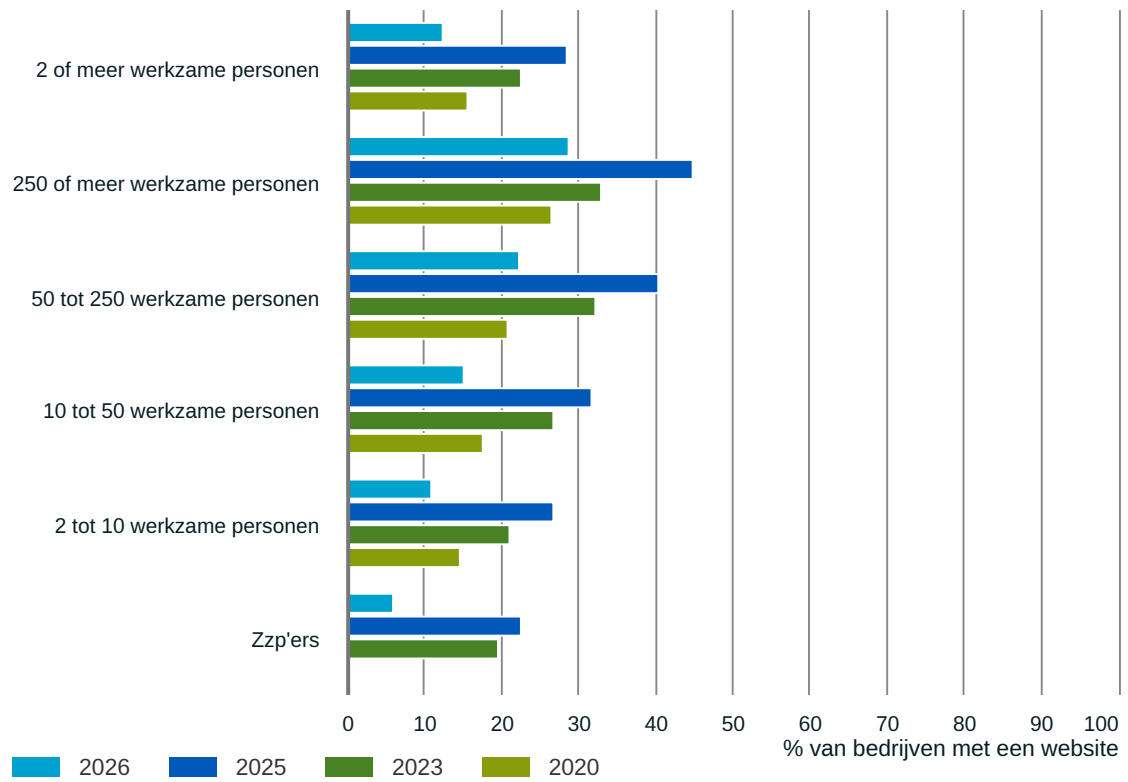
Figuur B.51.: Percentage van bedrijven met een website met geslaagde websitetest '0-RTT' naar bedrijfsgrootteklasse



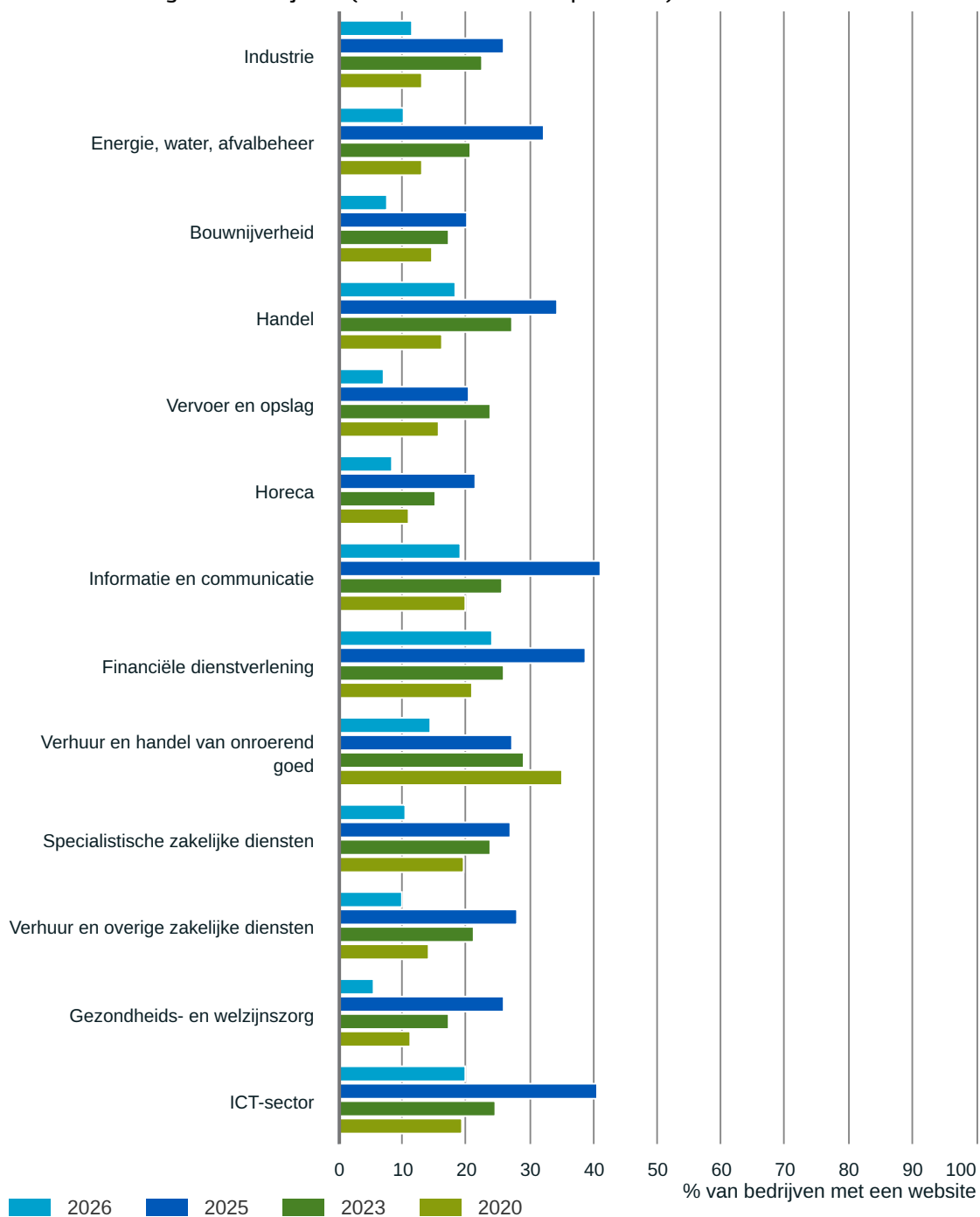
Figuur B.52.: Percentage van bedrijven met een website met geslaagde websitetest '0-RTT' naar bedrijfstak (2 of meer werkzame personen)



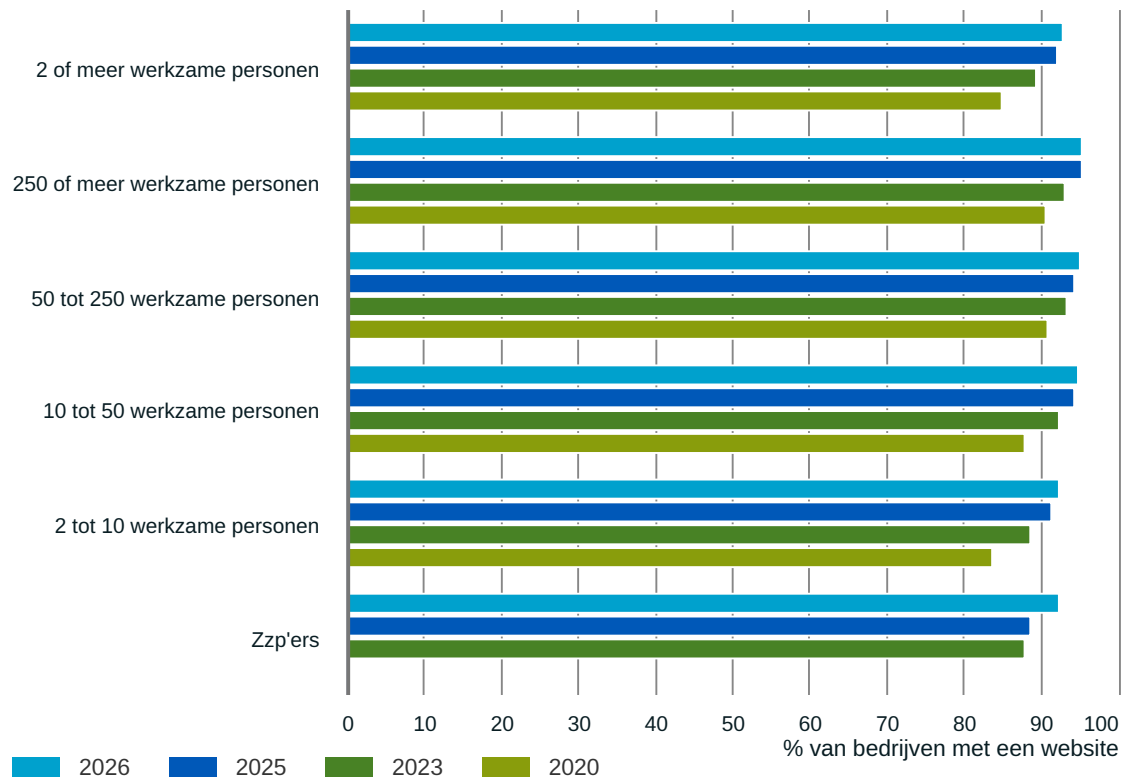
Figuur B.53.: Percentage van bedrijven met een website met geslaagde websitetest 'OCSP stapeling' naar bedrijfsgrootteklasse



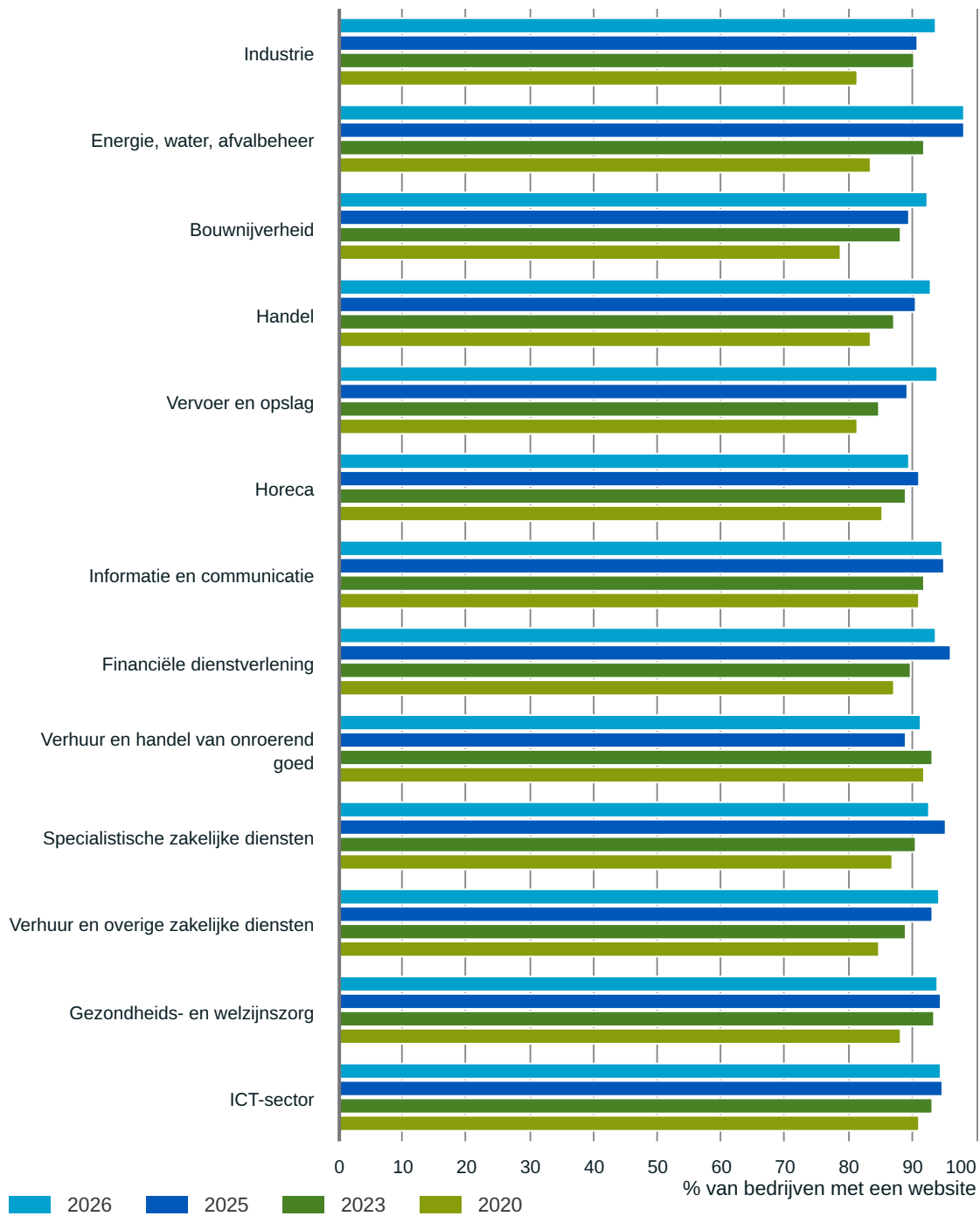
Figuur B.54.: Percentage van bedrijven met een website met geslaagde websitetest 'OCSP stapeling' naar bedrijfstak (2 of meer werkzame personen)



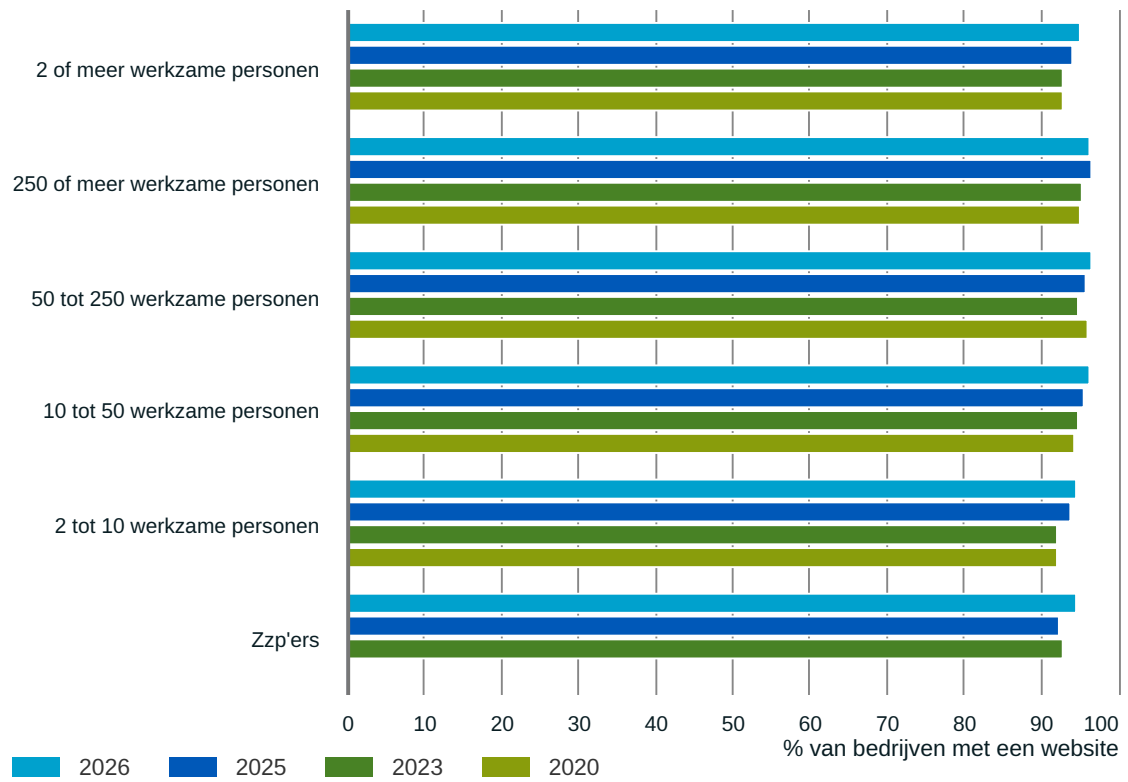
Figuur B.55.: Percentage van bedrijven met een website met geslaagde websitetest 'Vertrouwensketen van certificaat' naar bedrijfsgrootteklasse



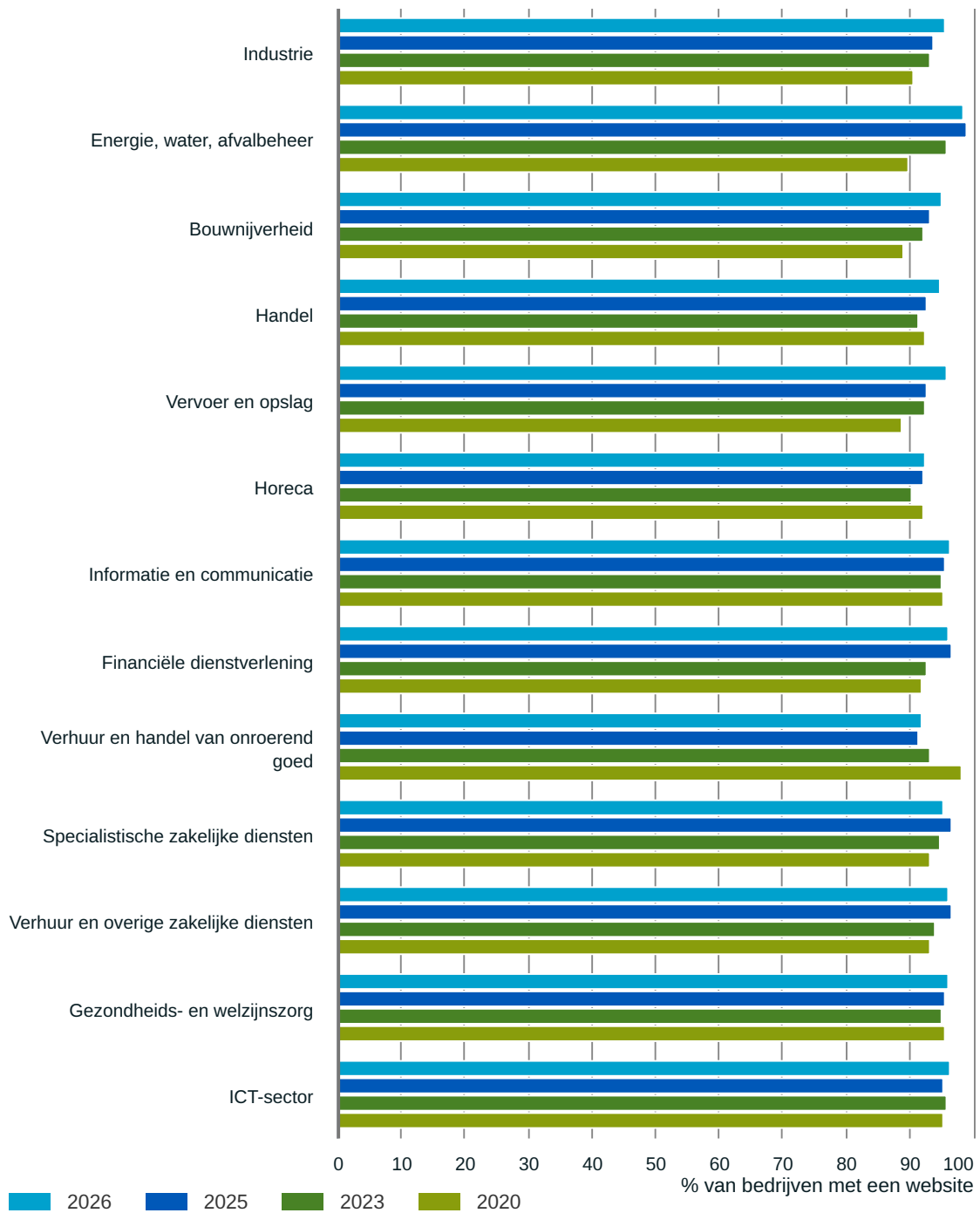
Figuur B.56.: Percentage van bedrijven met een website met geslaagde websitetest 'Vertrouwensketen van certificaat' naar bedrijfstak (2 of meer werkzame personen)



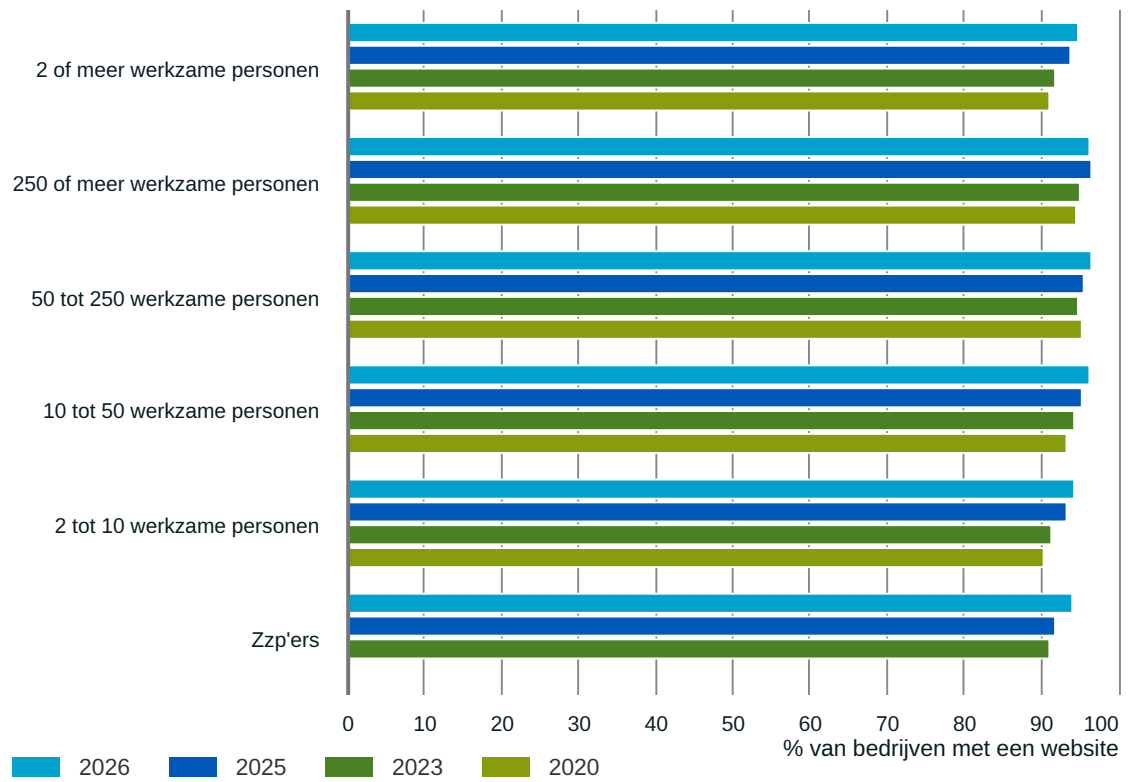
Figuur B.57.: Percentage van bedrijven met een website met geslaagde websitetest 'Publieke sleutel van certificaat' naar bedrijfsgrootteklasse



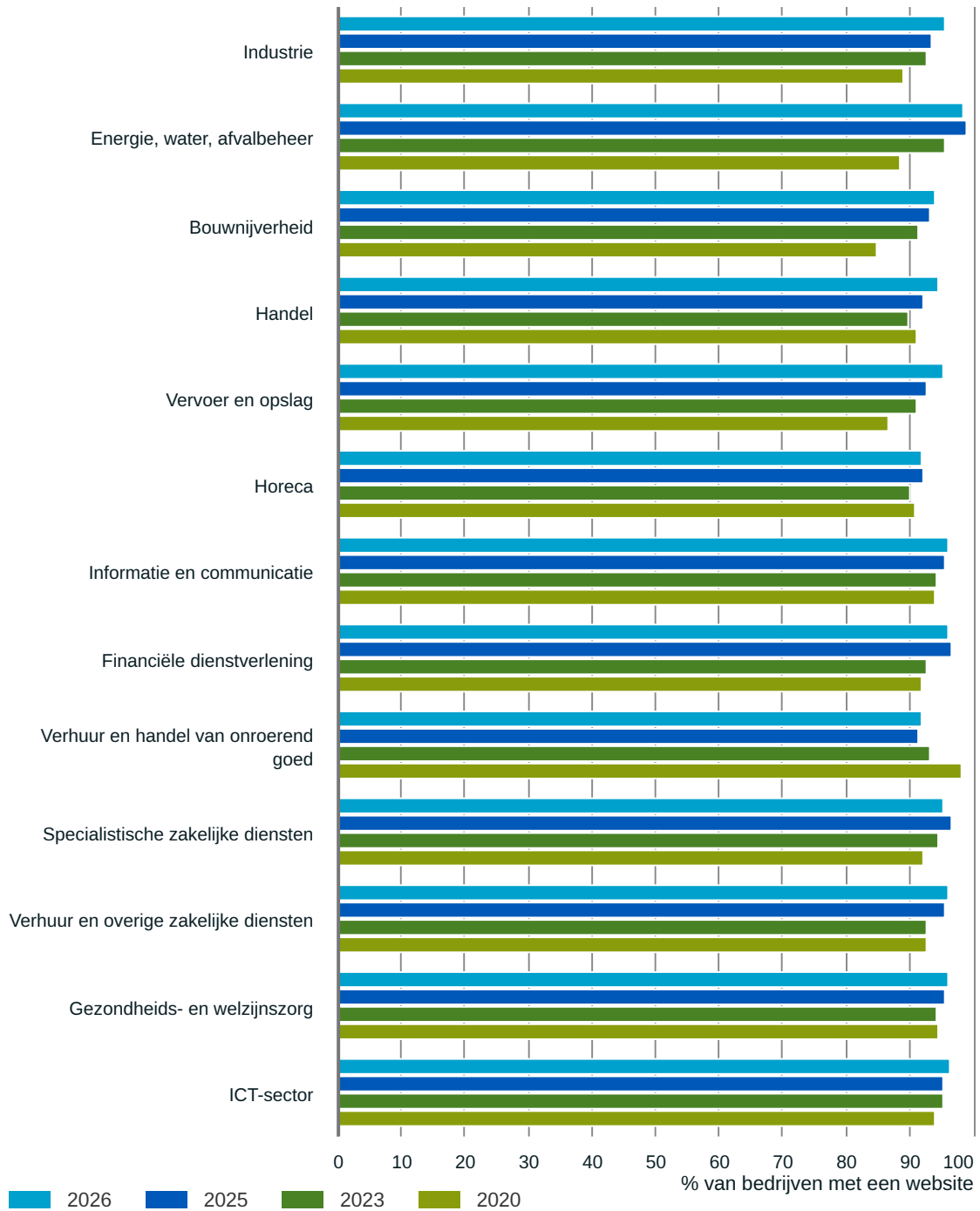
Figuur B.58.: Percentage van bedrijven met een website met geslaagde websitetest 'Publieke sleutel van certificaat' naar bedrijfstak (2 of meer werkzame personen)



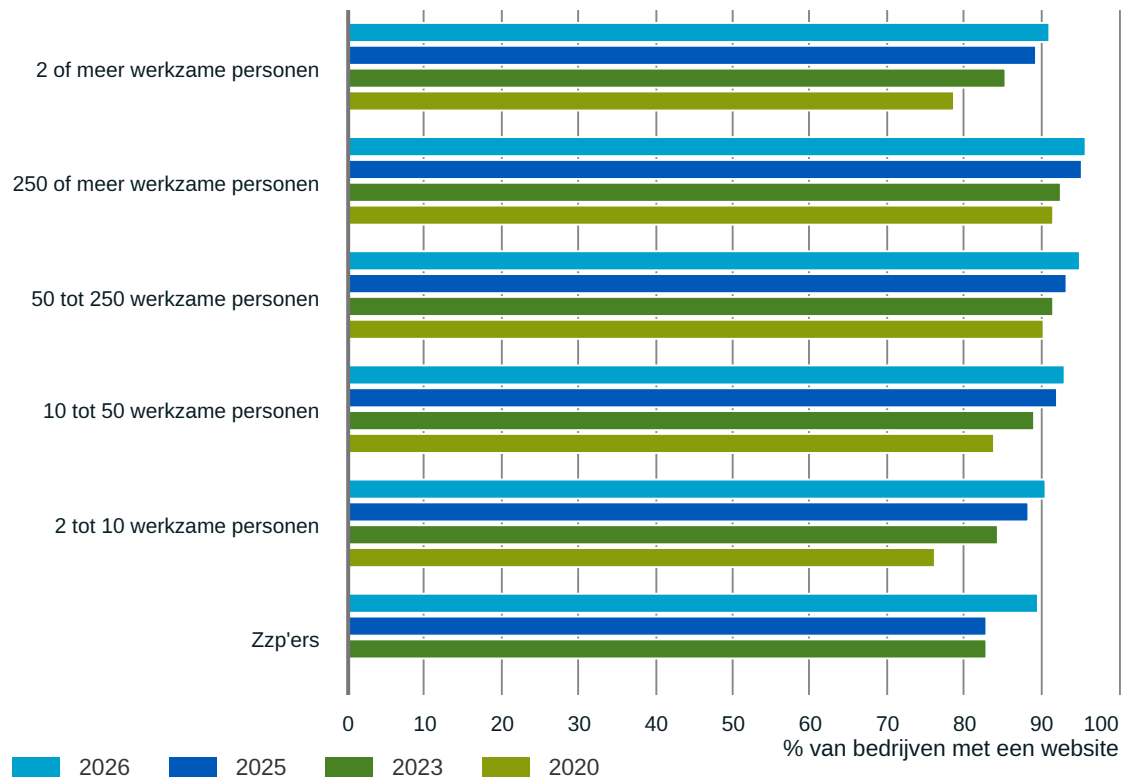
Figuur B.59.: Percentage van bedrijven met een website met geslaagde websitetest 'Handtekening van certificaat' naar bedrijfsgrootteklasse



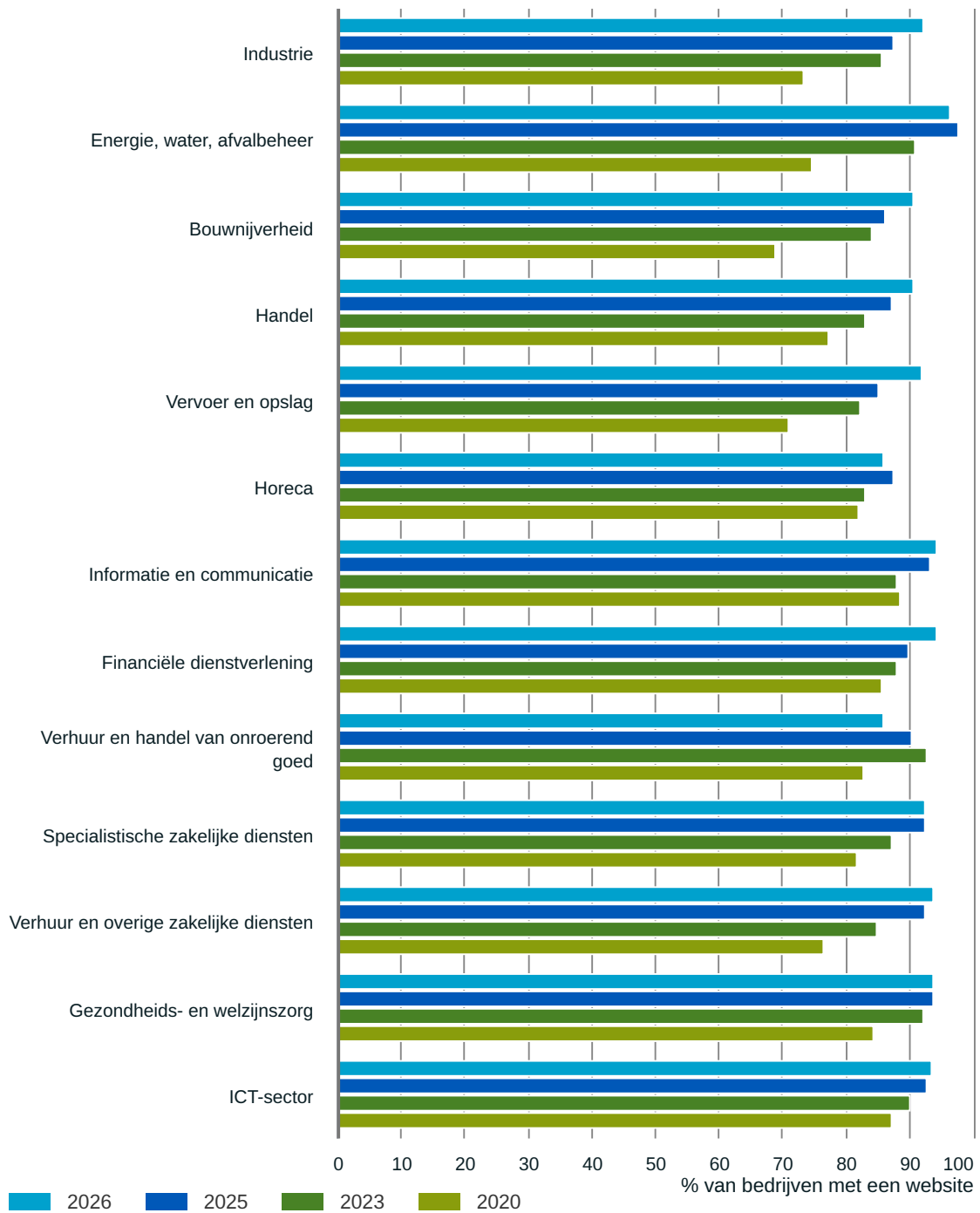
Figuur B.60.: Percentage van bedrijven met een website met geslaagde websitetest 'Handtekening van certificaat' naar bedrijfstak (2 of meer werkzame personen)



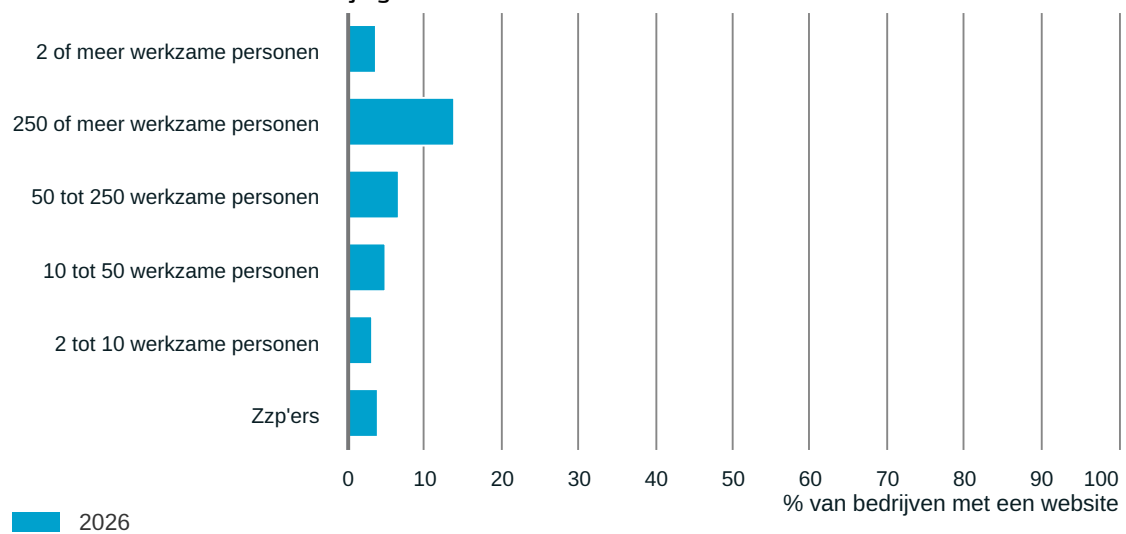
Figuur B.61.: Percentage van bedrijven met een website met geslaagde websitetest 'Domeinnaam op certificaat' naar bedrijfsgrootteklasse



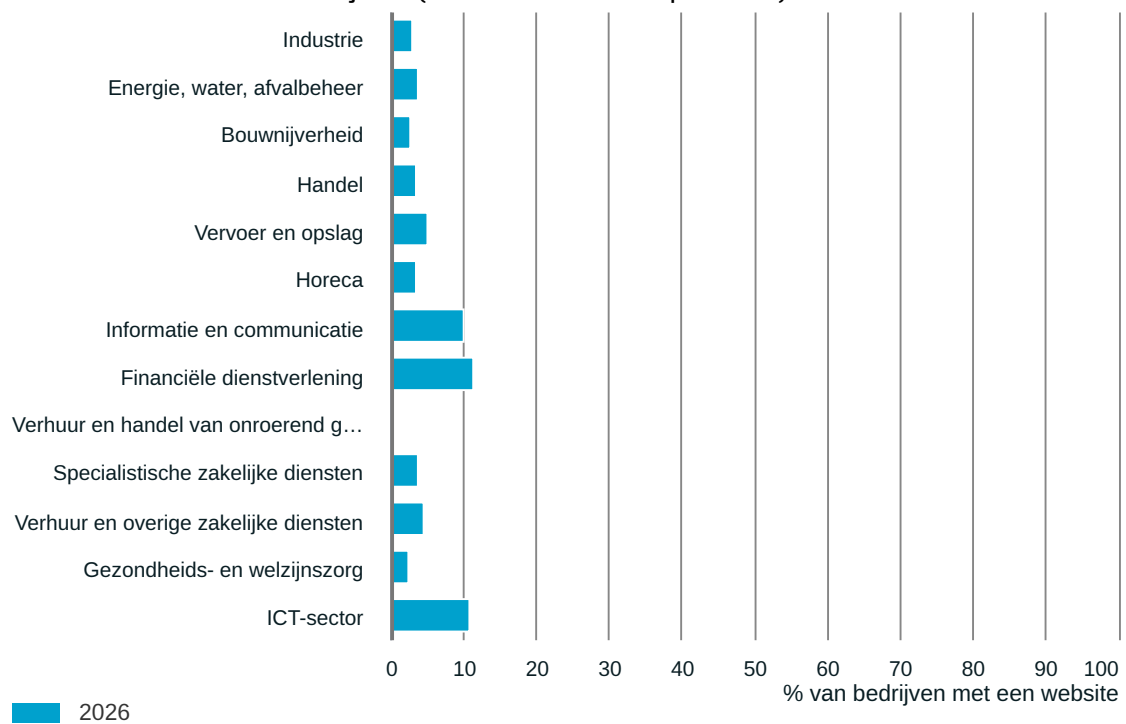
Figuur B.62.: Percentage van bedrijven met een website met geslaagde websitetest 'Domeinnaam op certificaat' naar bedrijfstak (2 of meer werkzame personen)



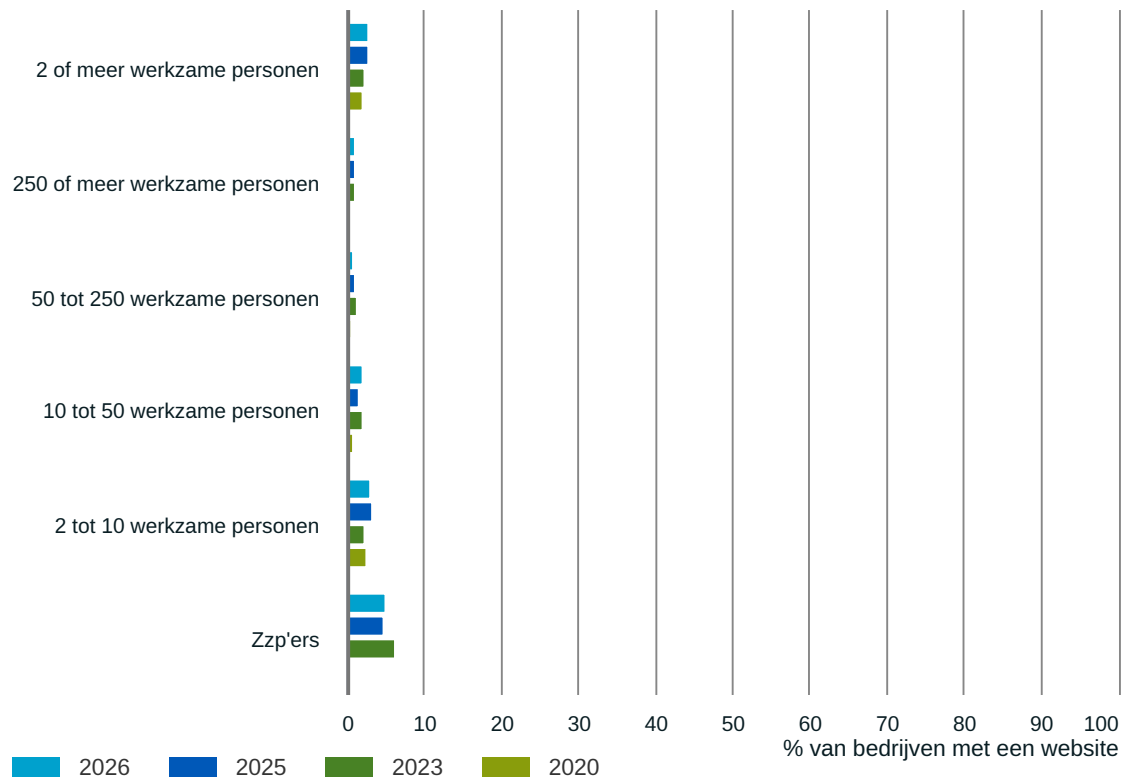
**Figuur B.63.: Percentage van bedrijven met een website met geslaagde websitetest 'CAA voor domein' naar bedrijfsgrootteklasse**



**Figuur B.64.: Percentage van bedrijven met een website met geslaagde websitetest 'CAA voor domein' naar bedrijfstak (2 of meer werkzame personen)**



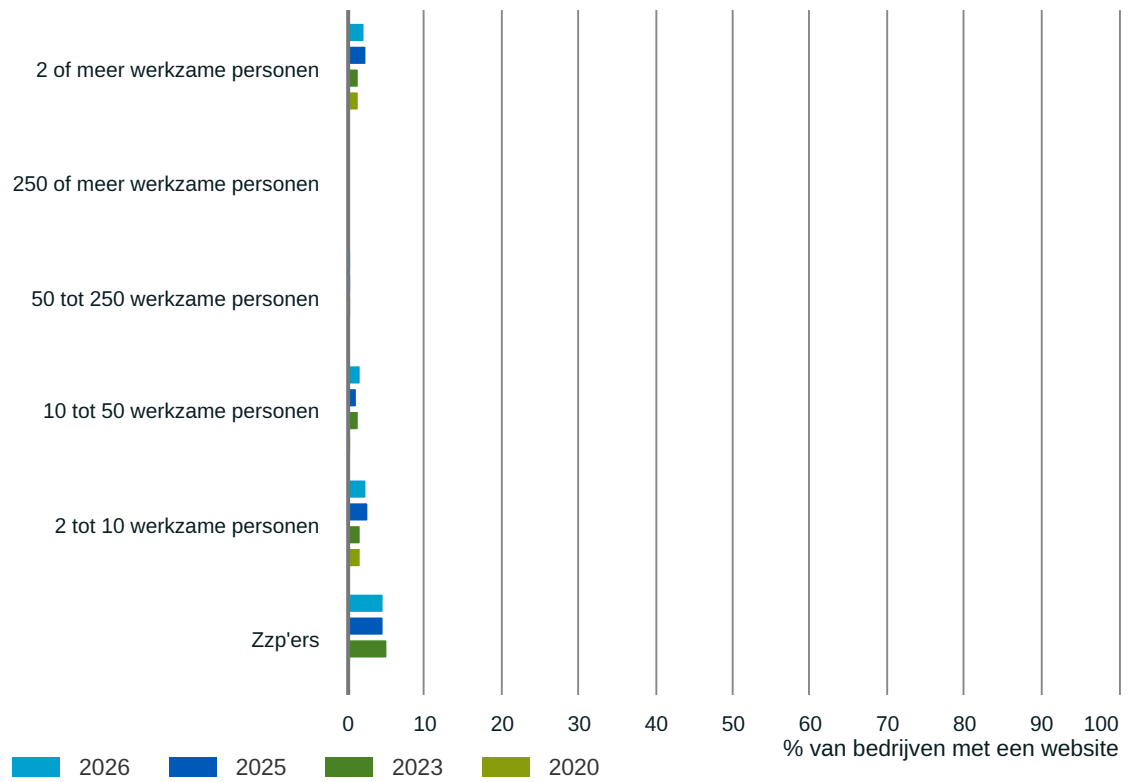
Figuur B.65.: Percentage van bedrijven met een website met geslaagde websitetest 'DANE aanwezig' naar bedrijfsgrootteklasse



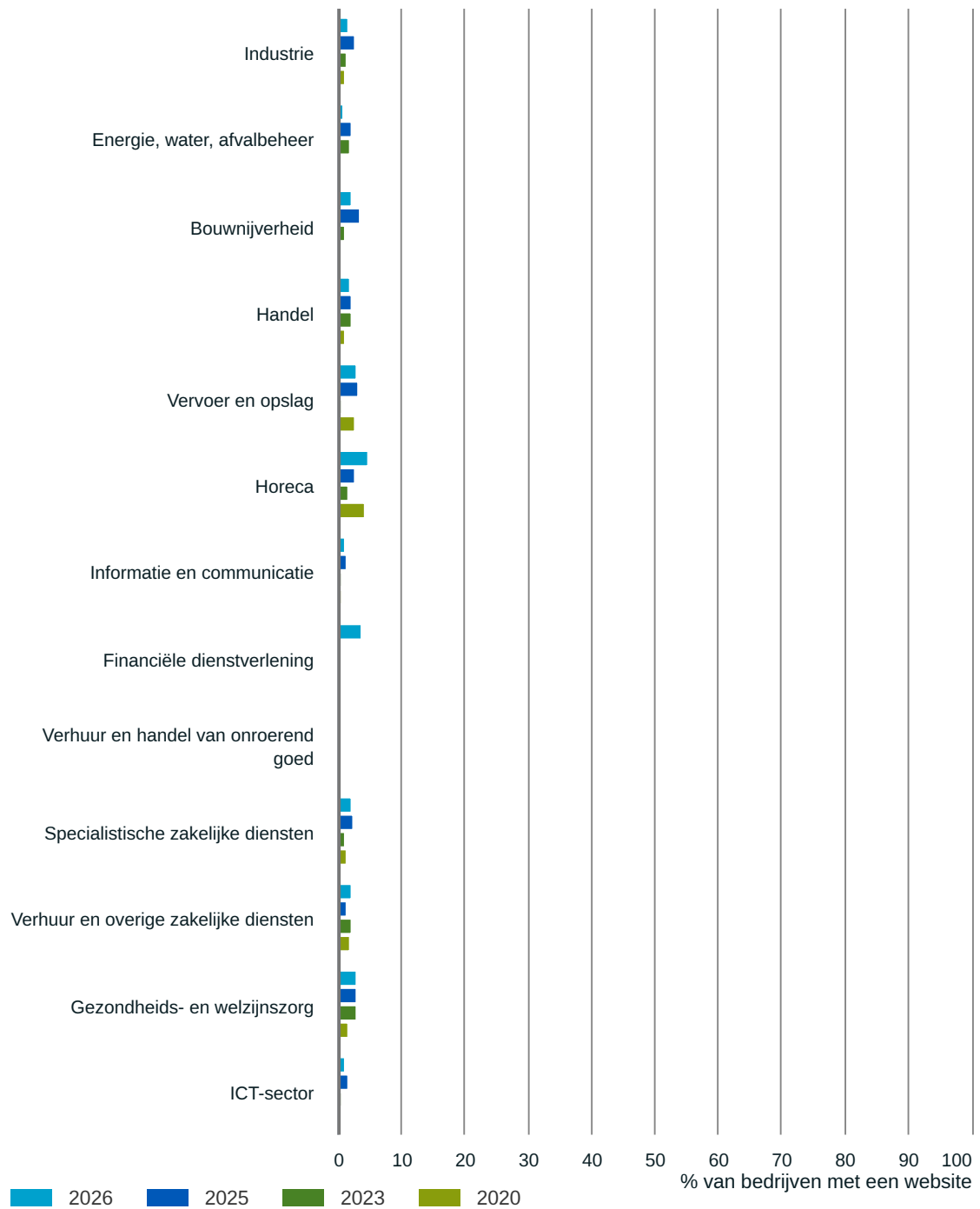
Figuur B.66.: Percentage van bedrijven met een website met geslaagde websitetest 'DANE aanwezig' naar bedrijfstak (2 of meer werkzame personen)



Figuur B.67.: Percentage van bedrijven met een website met geslaagde websitetest 'DANE geldig' naar bedrijfsgrootteklasse

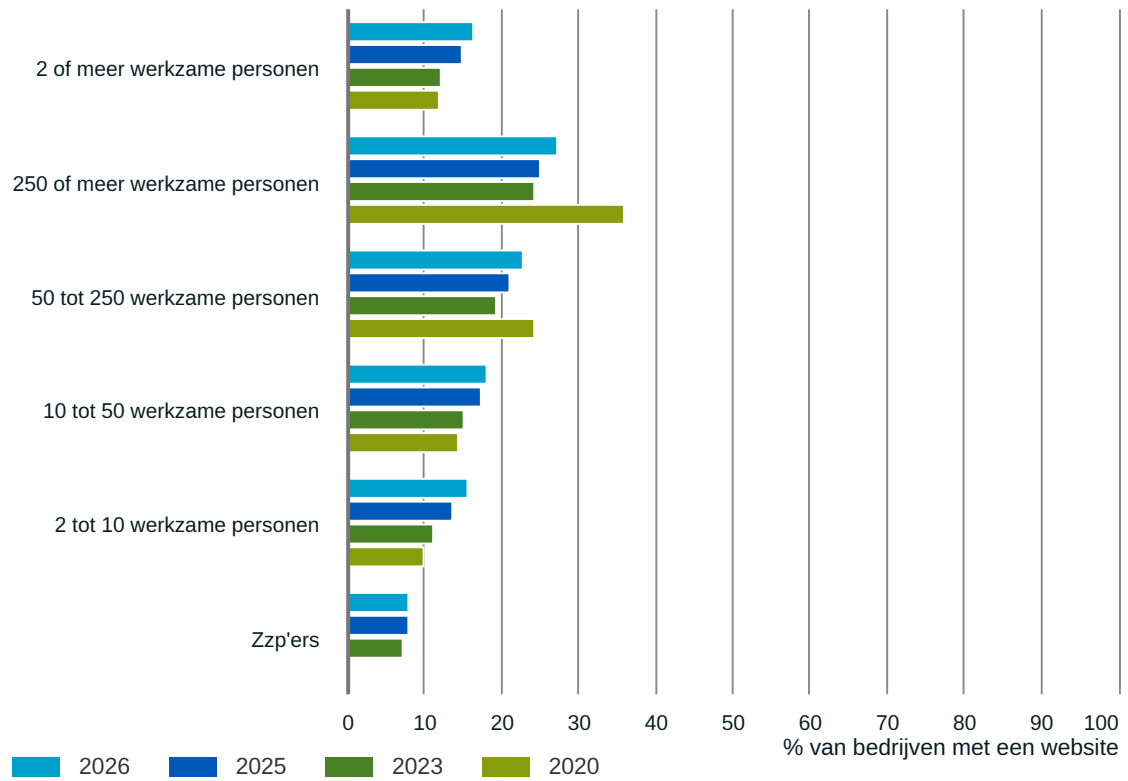


Figuur B.68.: Percentage van bedrijven met een website met geslaagde websitetest 'DANE geldig' naar bedrijfstak (2 of meer werkzame personen)

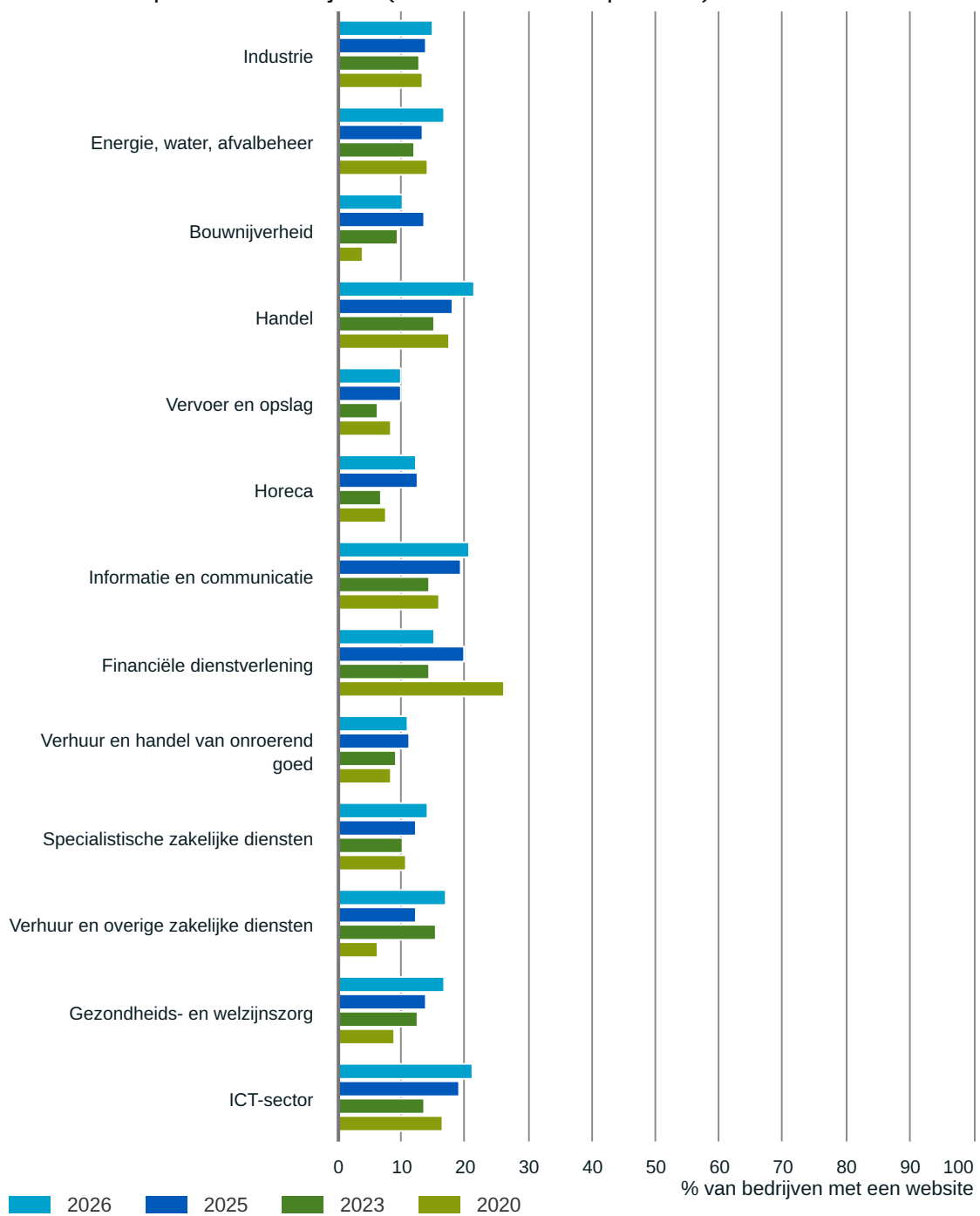


## B.5. Websitescanslagen voor categorie Beveiligingsopties

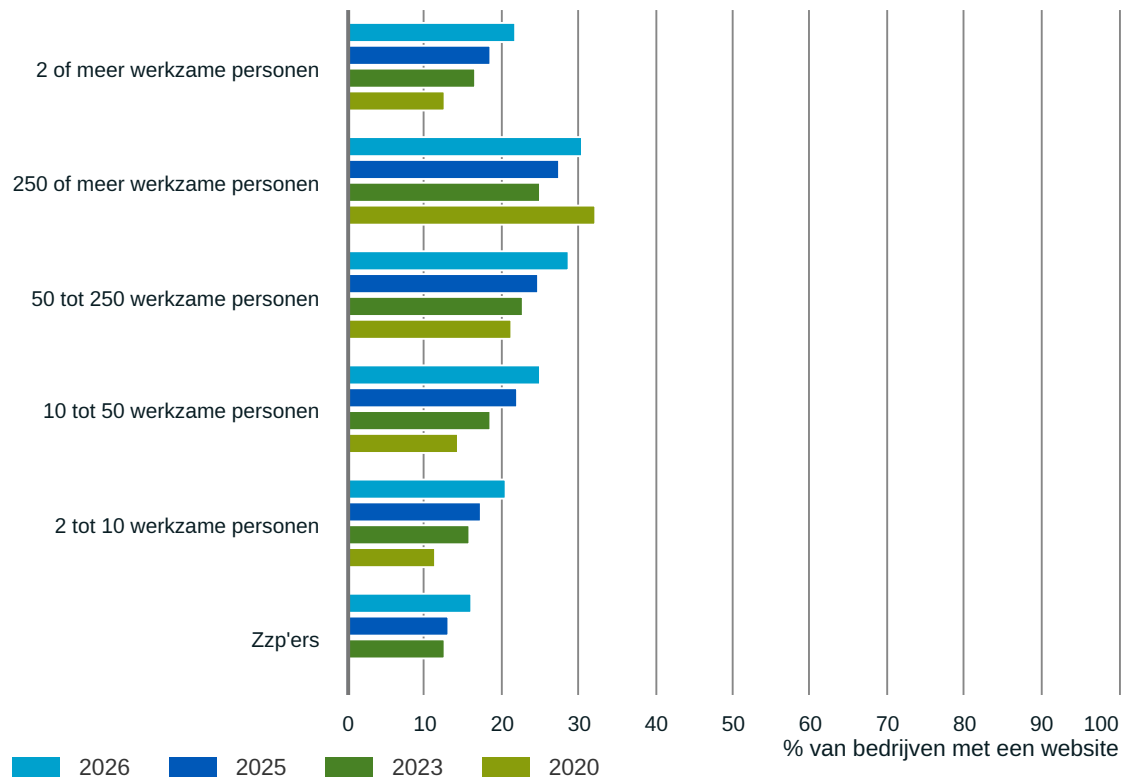
Figuur B.69.: Percentage van bedrijven met een website met geslaagde websitetest 'X-Frame-Options' naar bedrijfsgrootteklasse



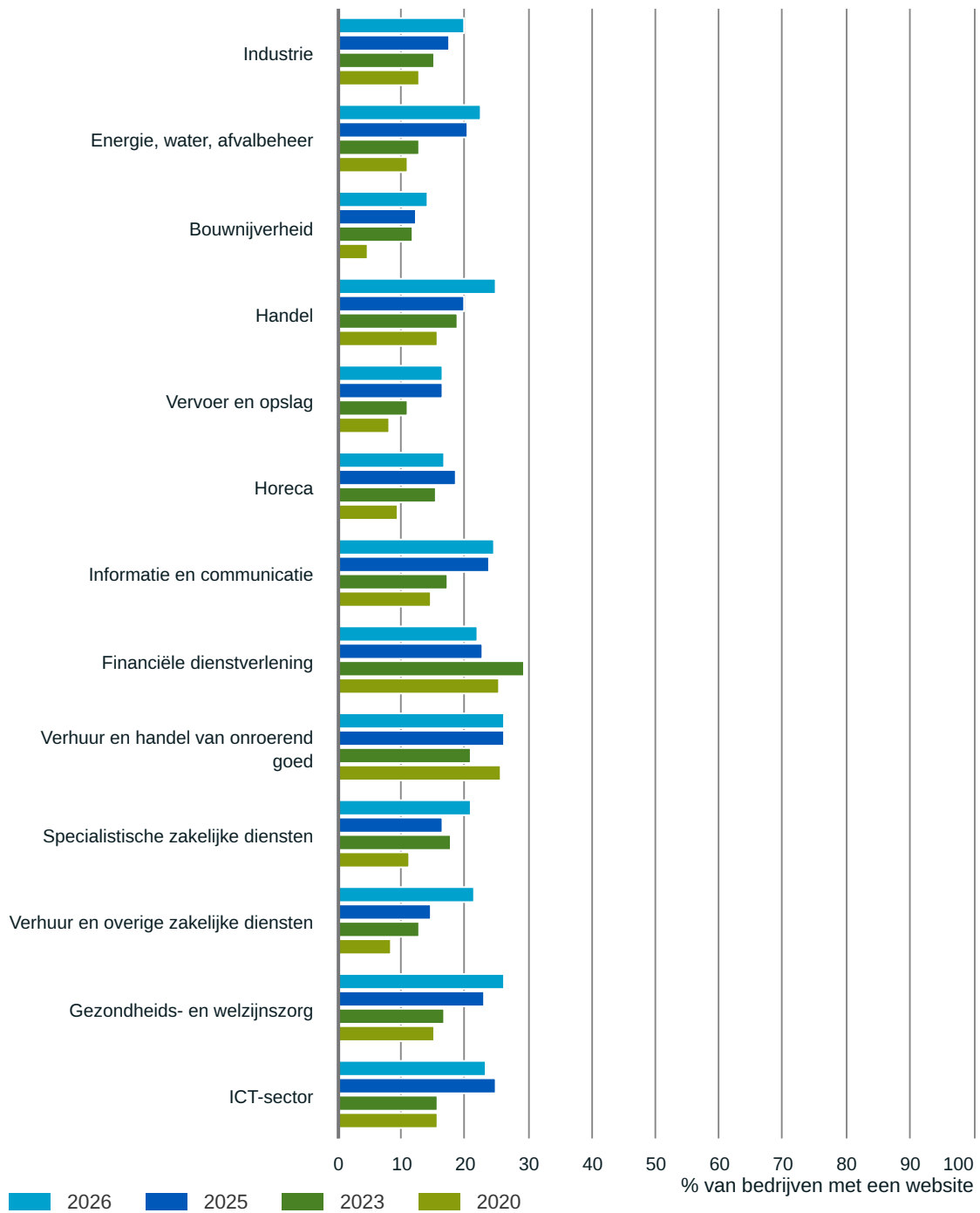
Figuur B.70.: Percentage van bedrijven met een website met geslaagde websitetest 'X-Frame-Options' naar bedrijfstak (2 of meer werkzame personen)



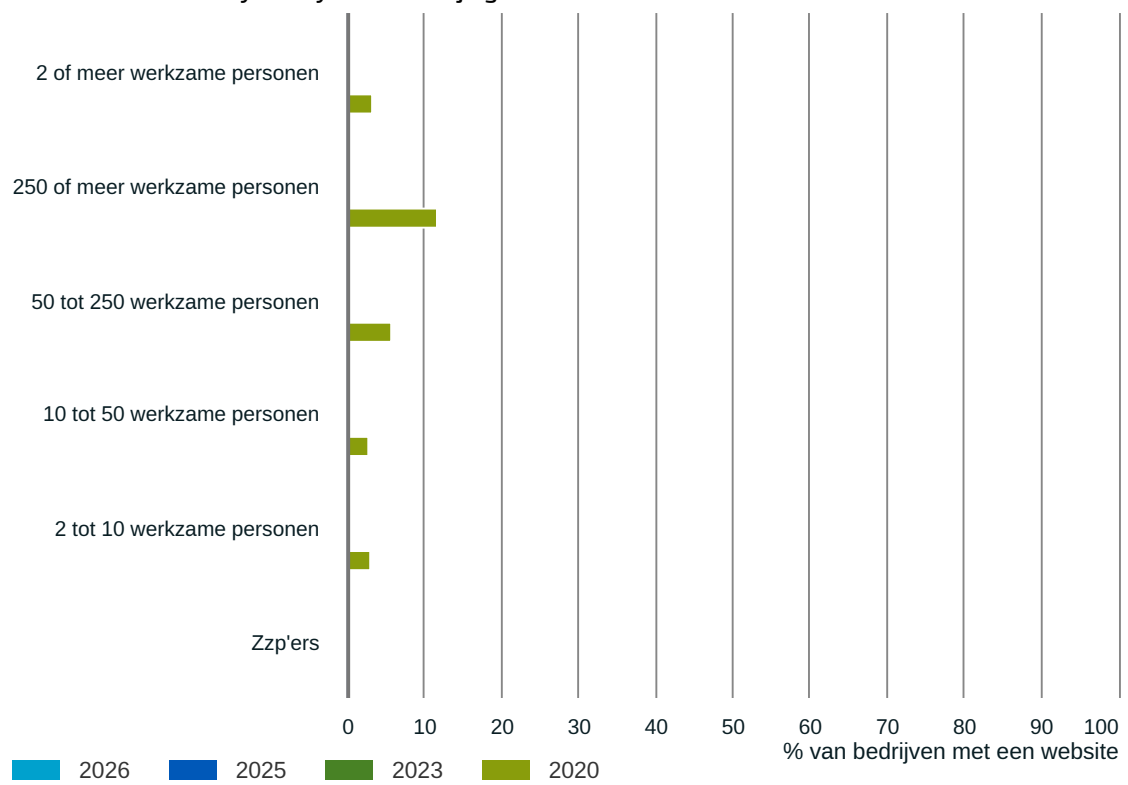
Figuur B.71.: Percentage van bedrijven met een website met geslaagde websitetest 'X-Content-Type-Options' naar bedrijfsgrootteklasse



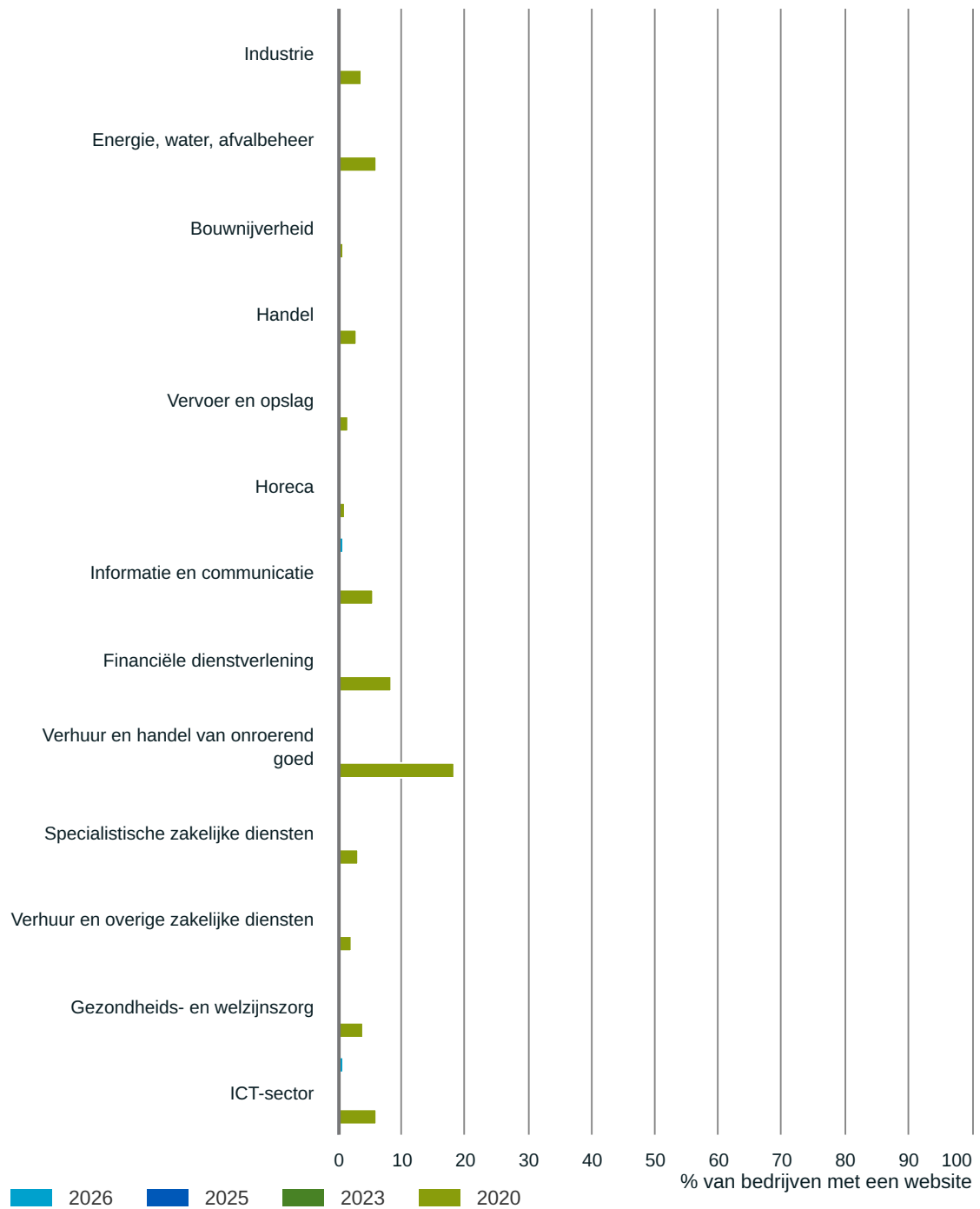
Figuur B.72.: Percentage van bedrijven met een website met geslaagde websitetest 'X-Content-Type-Options' naar bedrijfstak (2 of meer werkzame personen)



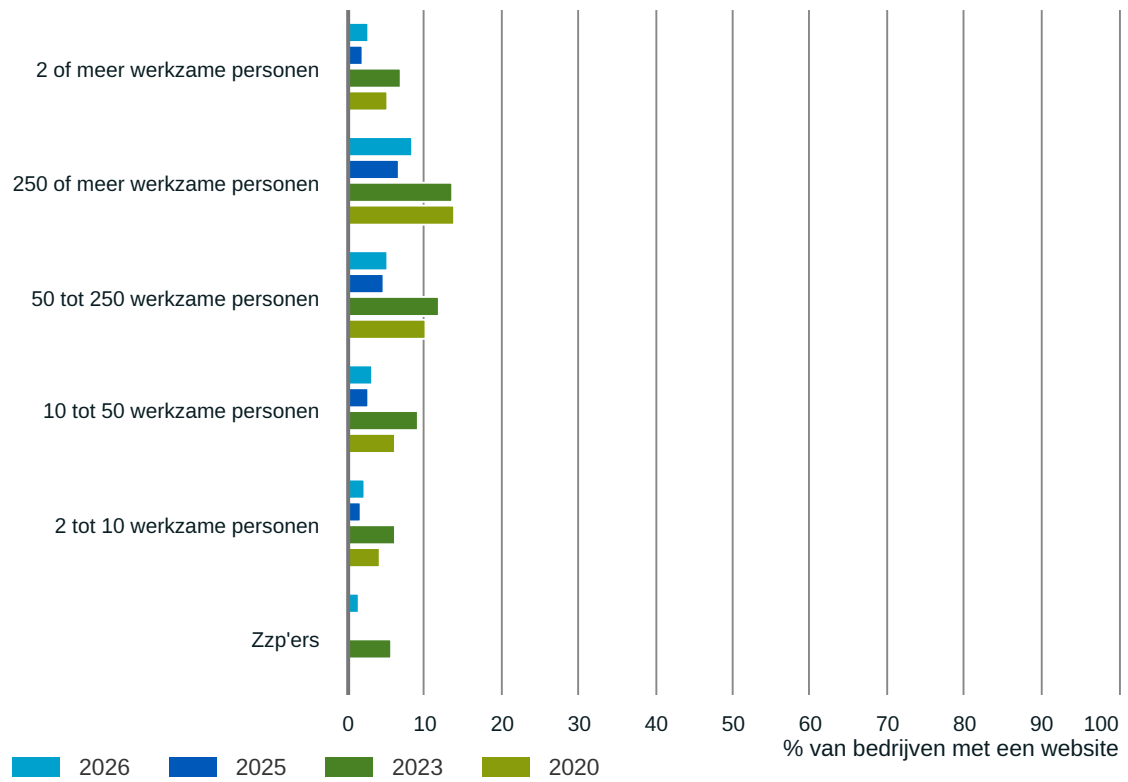
Figuur B.73.: Percentage van bedrijven met een website met geslaagde websitetest 'Content-Security-Policy' naar bedrijfsgrootteklasse



Figuur B.74.: Percentage van bedrijven met een website met geslaagde websitetest 'Content-Security-Policy' naar bedrijfstak (2 of meer werkzame personen)



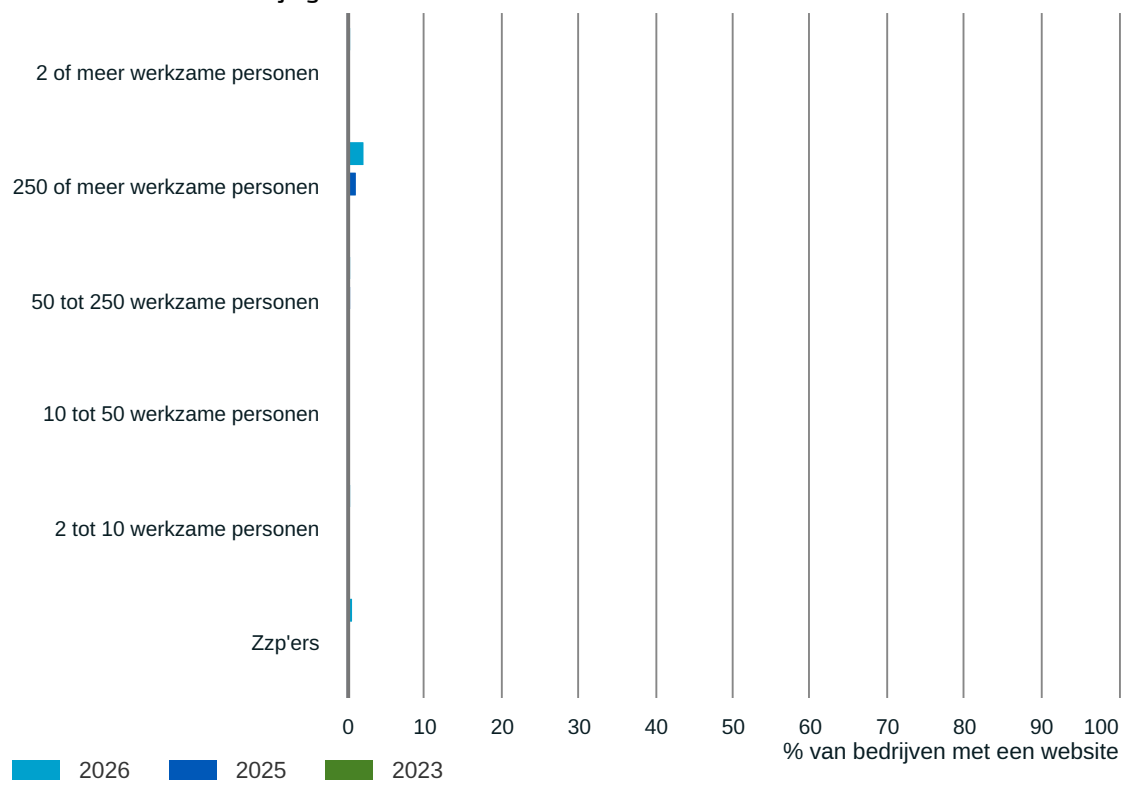
Figuur B.75.: Percentage van bedrijven met een website met geslaagde websitetest 'Referrer-Policy' naar bedrijfsgrootteklasse



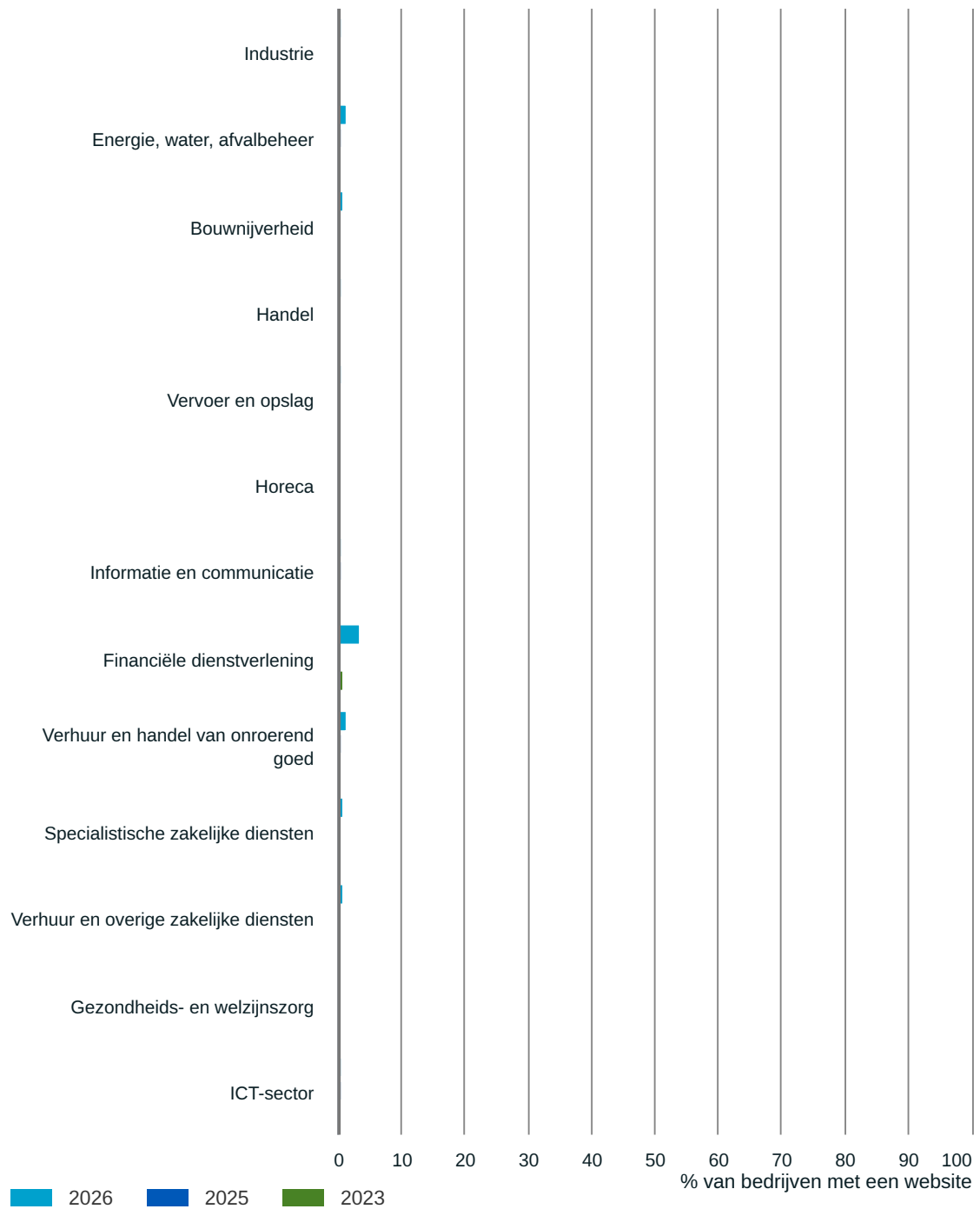
Figuur B.76.: Percentage van bedrijven met een website met geslaagde websitetest 'Referrer-Policy' naar bedrijfstak (2 of meer werkzame personen)



Figuur B.77.: Percentage van bedrijven met een website met geslaagde websitetest 'security.txt' naar bedrijfsgrootteklasse

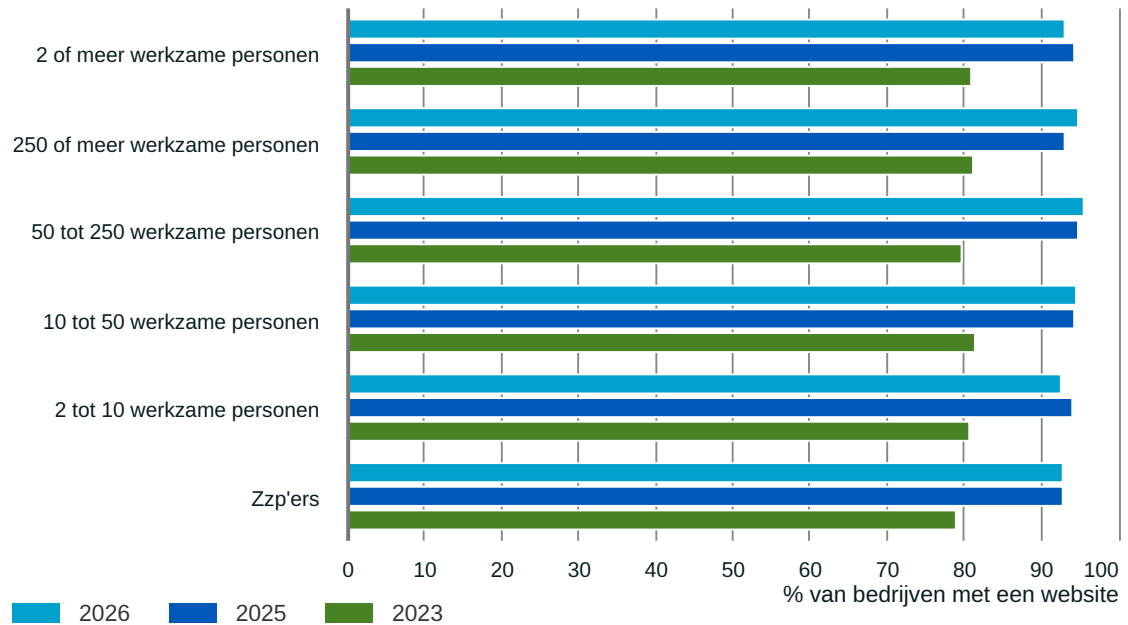


Figuur B.78.: Percentage van bedrijven met een website met geslaagde websitetest 'security.txt' naar bedrijfstak (2 of meer werkzame personen)

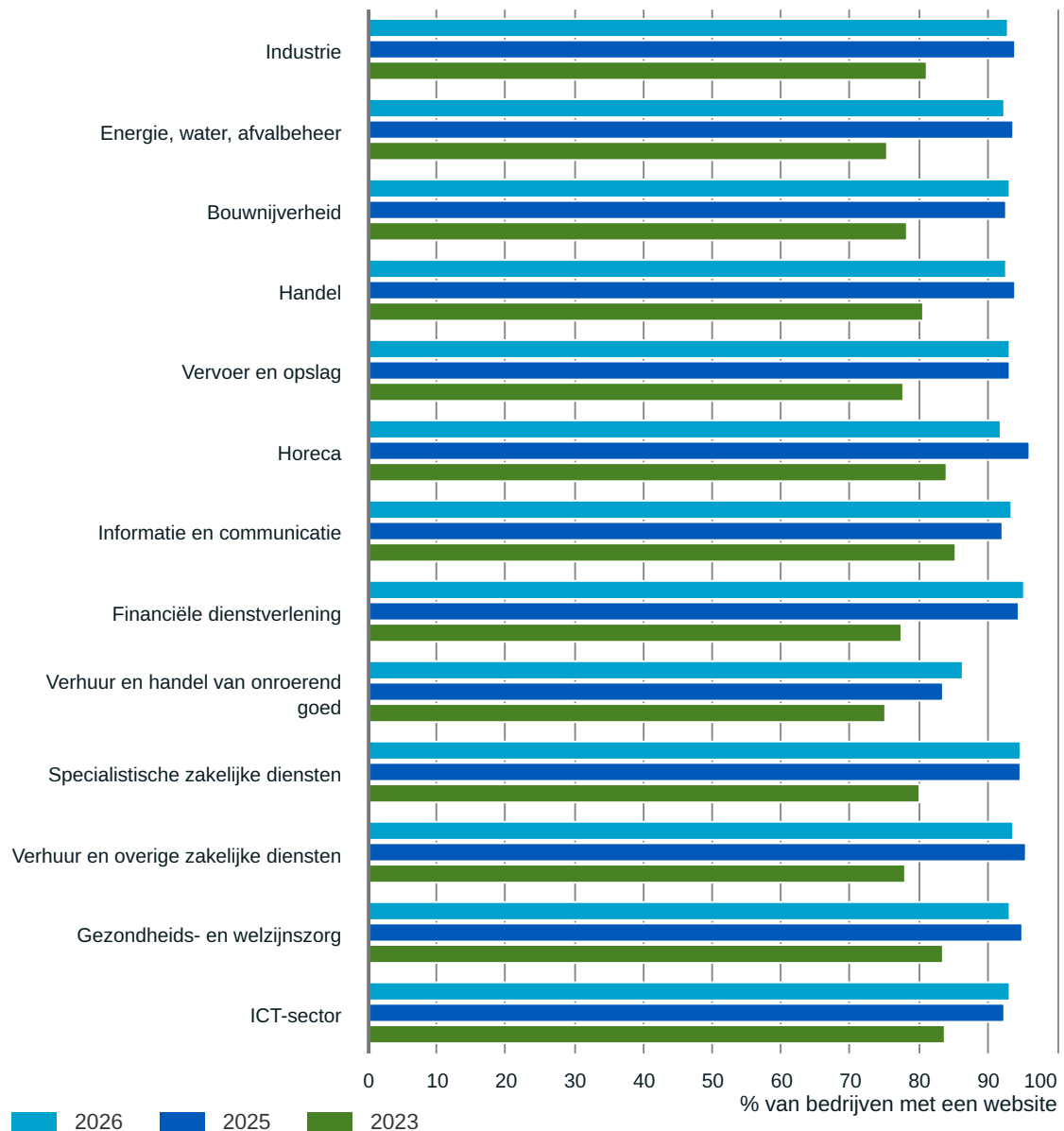


## B.6. Websitescanuitslagen voor categorie RPKI

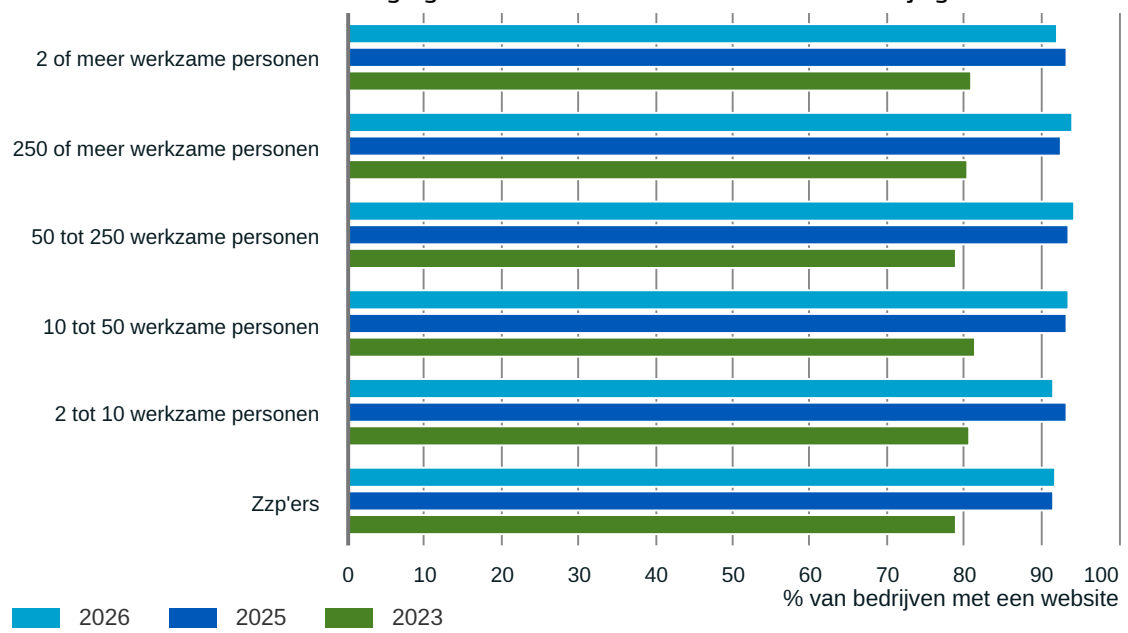
Figuur B.79.: Percentage van bedrijven met een website met geslaagde websitetest 'Aanwezigheid van Route Origin Authorisation voor nameserver van domein' naar bedrijfsgrootteklasse



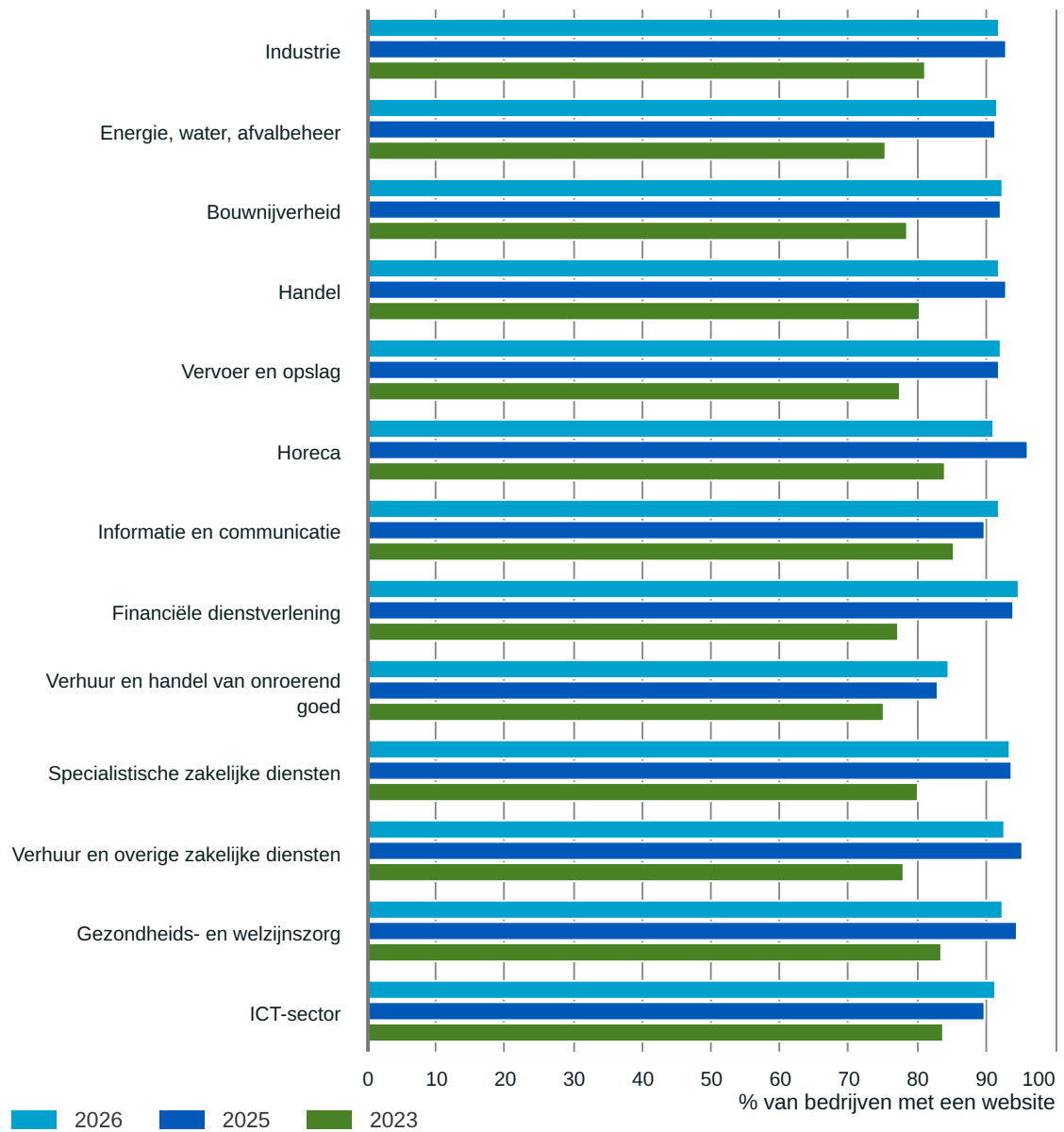
Figuur B.80.: Percentage van bedrijven met een website met geslaagde websitetest 'Aanwezigheid van Route Origin Authorisation voor nameserver van domein' naar bedrijfstak (2 of meer werkzame personen)



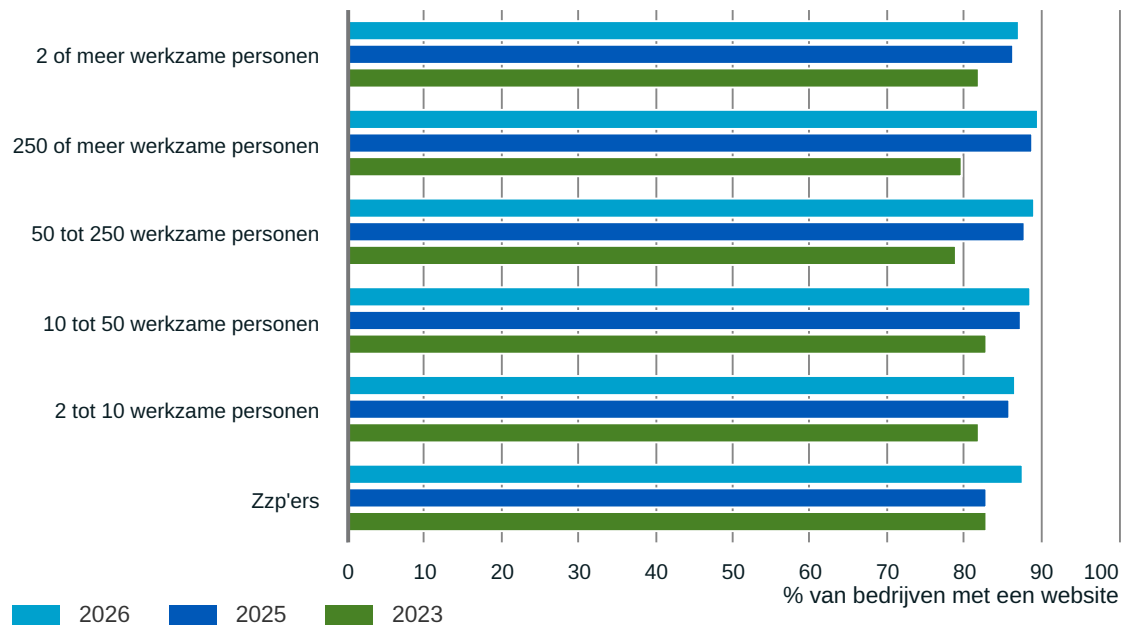
Figuur B.81.: Percentage van bedrijven met een website met geslaagde websitetest 'Geldigheid van route-aankondiging voor nameserver van domein' naar bedrijfsgrootteklasse



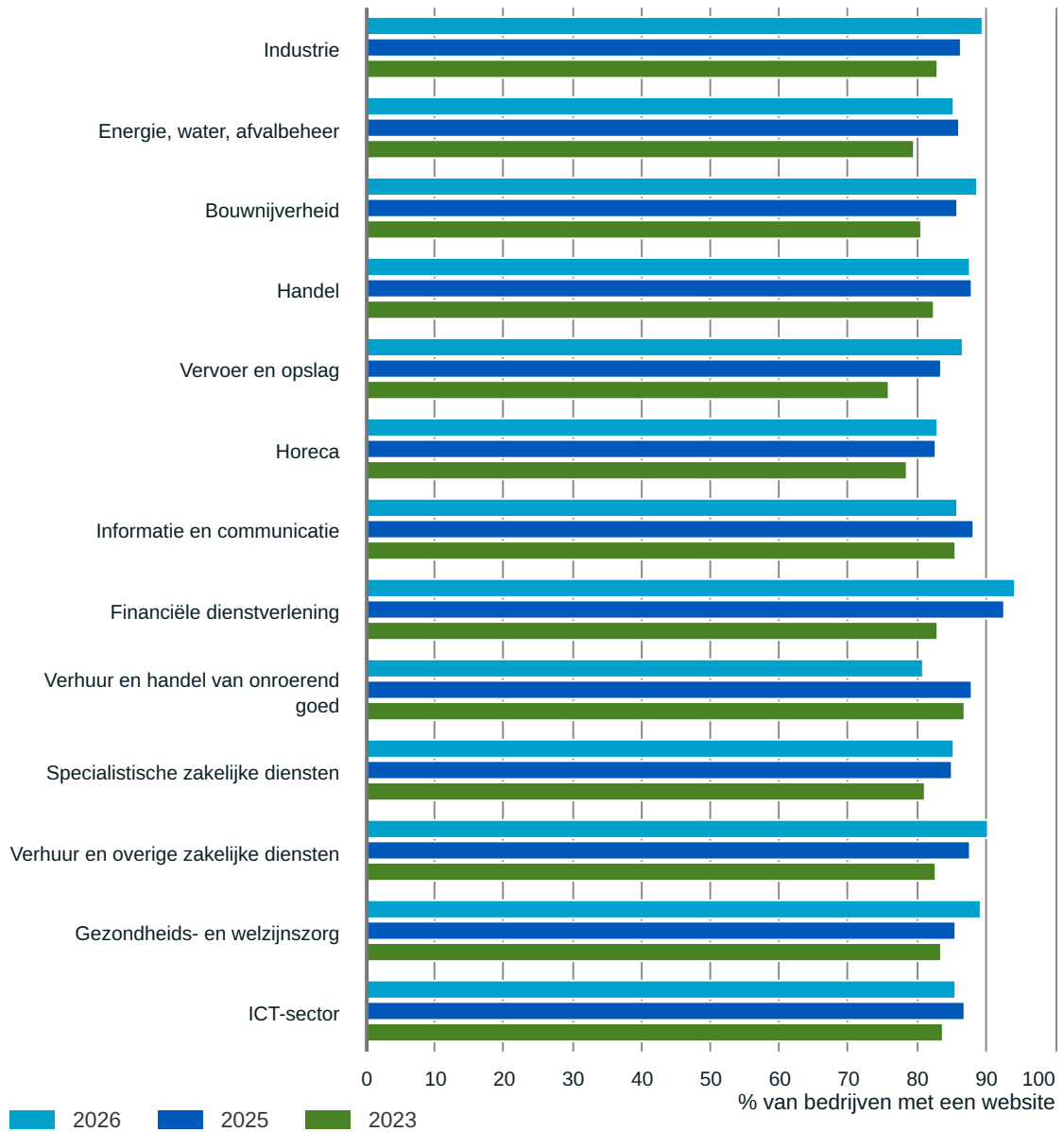
Figuur B.82.: Percentage van bedrijven met een website met geslaagde websitetest 'Geldigheid van route-aankondiging voor nameserver van domein' naar bedrijfstak (2 of meer werkzame personen)



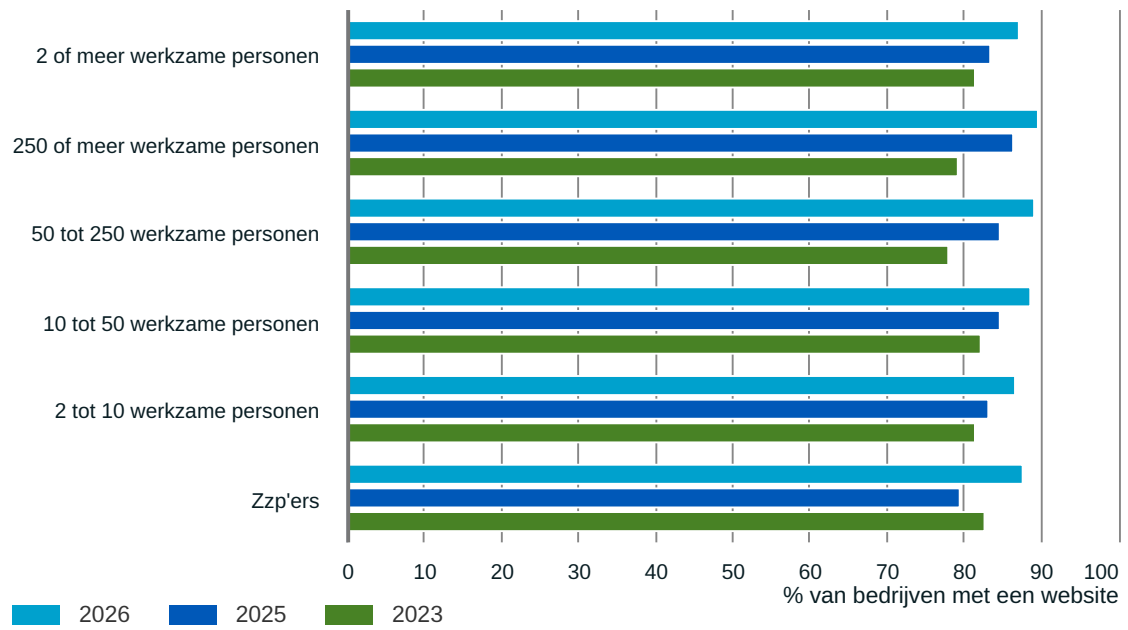
Figuur B.83.: Percentage van bedrijven met een website met geslaagde websitetest 'Aanwezigheid van Route Origin Authorisation voor webserver' naar bedrijfsgrootteklasse



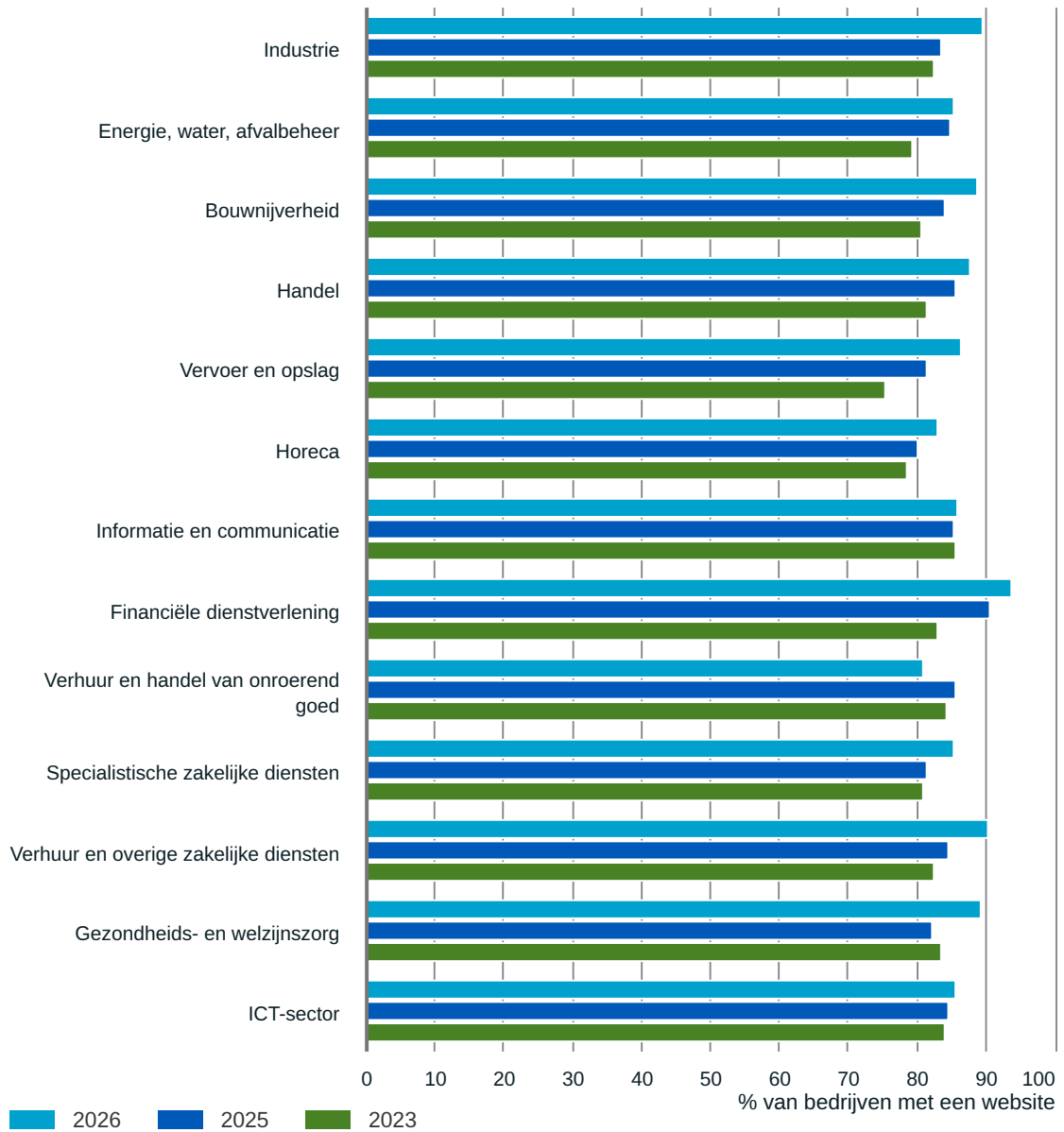
Figuur B.84.: Percentage van bedrijven met een website met geslaagde websitetest 'Aanwezigheid van Route Origin Authorisation voor webserver' naar bedrijfstak (2 of meer werkzame personen)



Figuur B.85.: Percentage van bedrijven met een website met geslaagde websitetest 'Geldigheid van route-aankondiging voor webserver' naar bedrijfsgrootteklasse

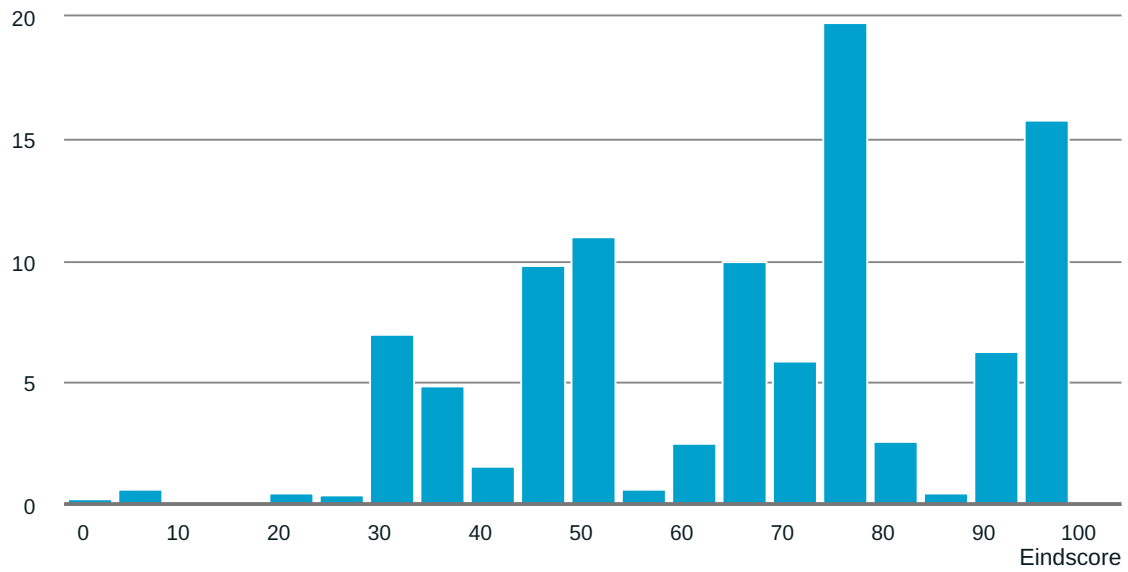


Figuur B.86.: Percentage van bedrijven met een website met geslaagde websitetest 'Geldigheid van route-aankondiging voor webserver' naar bedrijfstak (2 of meer werkzame personen)

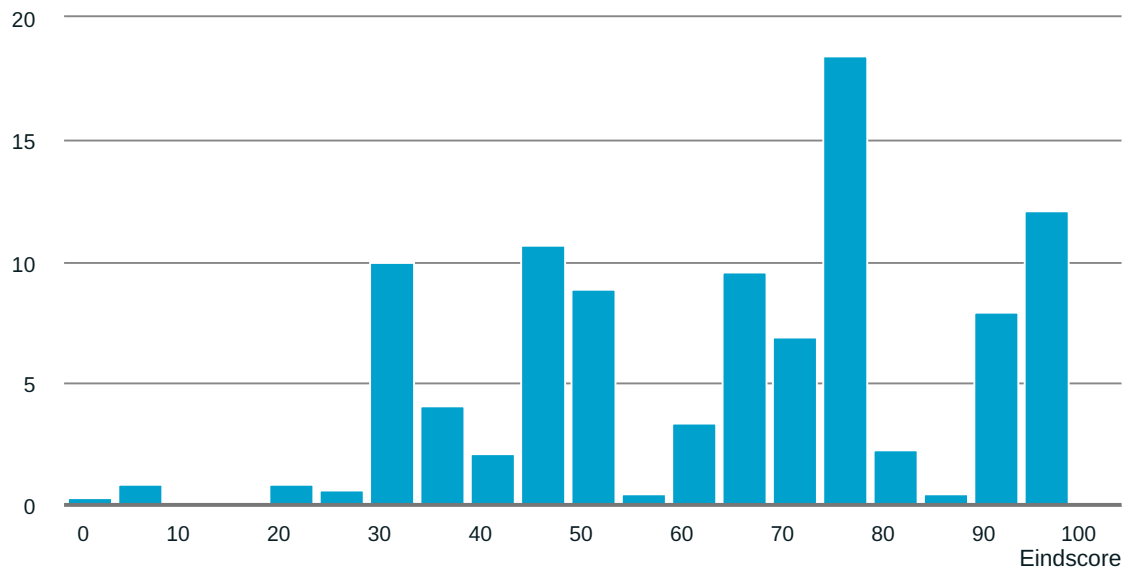


## B.7. Verdeling eindscores websitescan

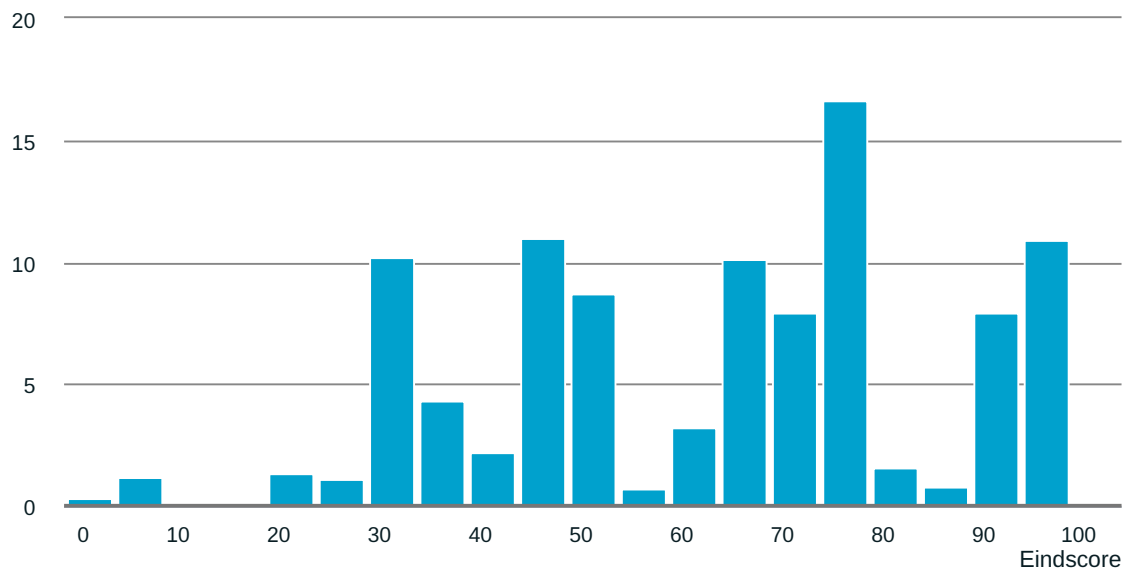
Figuur B.87.: Verdeling eindscores websitescan voor bedrijven met 2 of meer werkzame personen, 2025



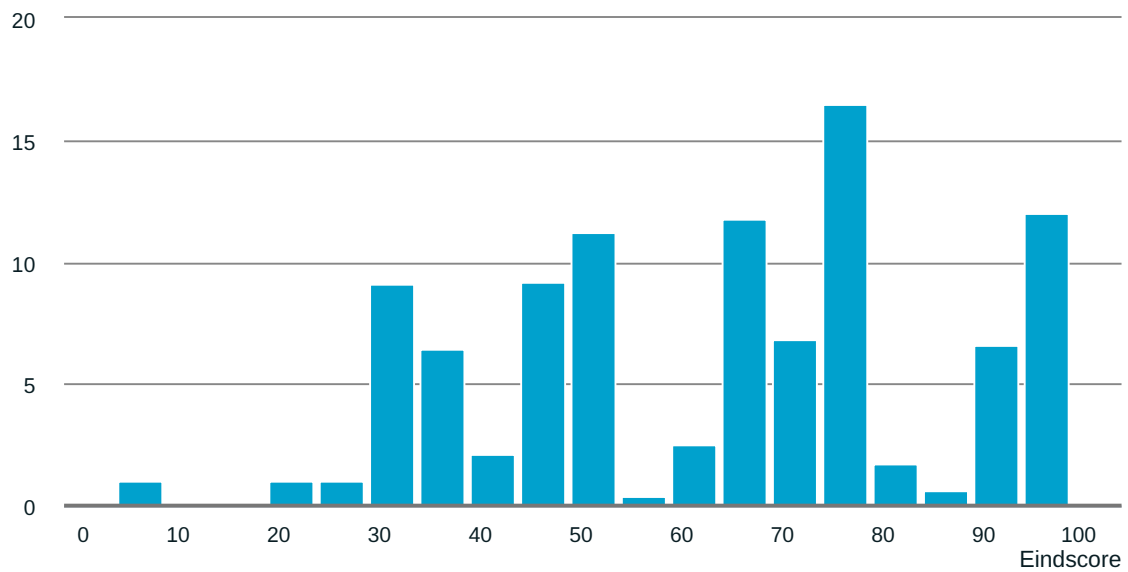
Figuur B.88.: Verdeling eindscores websitescan voor bedrijven met 2 of meer werkzame personen, 2024



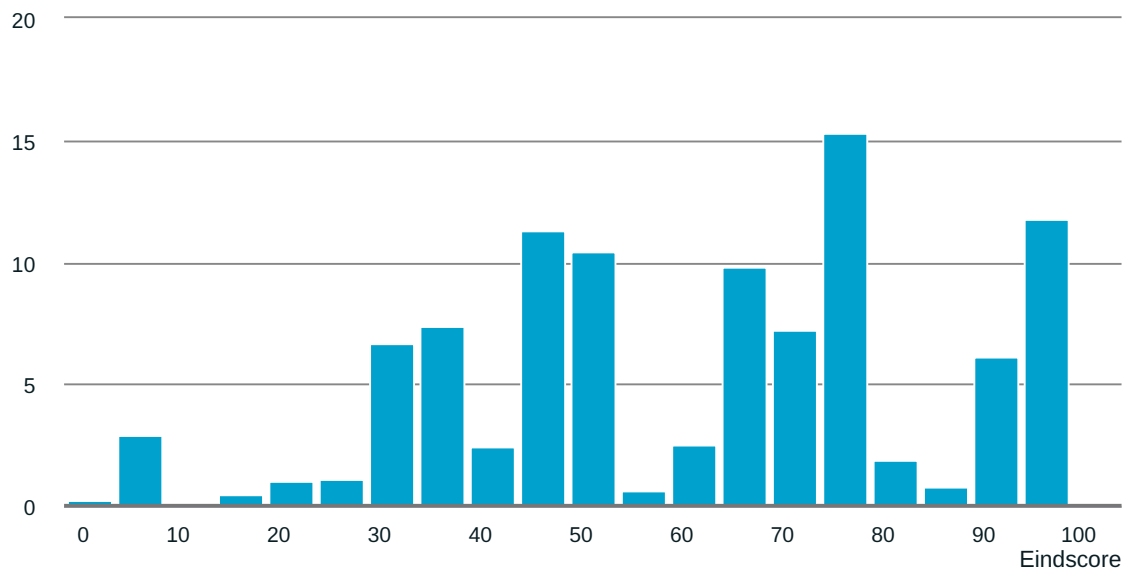
Figuur B.89.: Verdeling eindscores websitescan voor bedrijven met 2 of meer werkzame personen, 2023



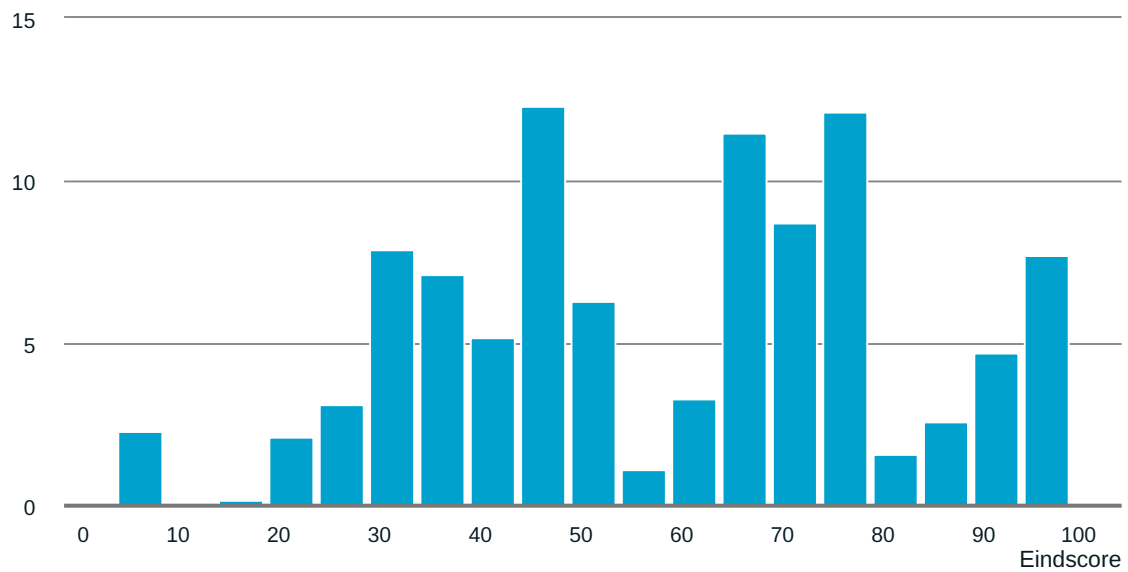
Figuur B.90.: Verdeling eindscores websitescan voor bedrijven met 2 of meer werkzame personen, 2022



Figuur B.91.: Verdeling eindscores websitescan voor bedrijven met 2 of meer werkzame personen, 2021



Figuur B.92.: Verdeling eindscores websitescan voor bedrijven met 2 of meer werkzame personen, 2020

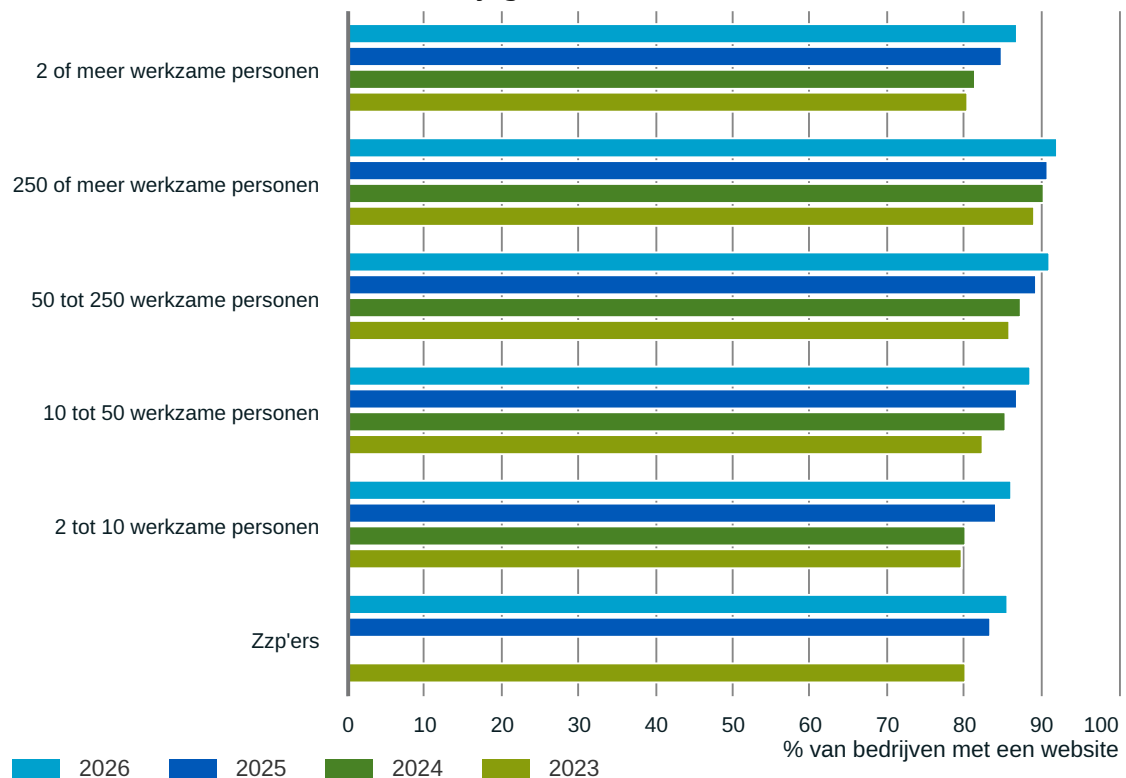


## C. Alle e-mailscanuitslagen

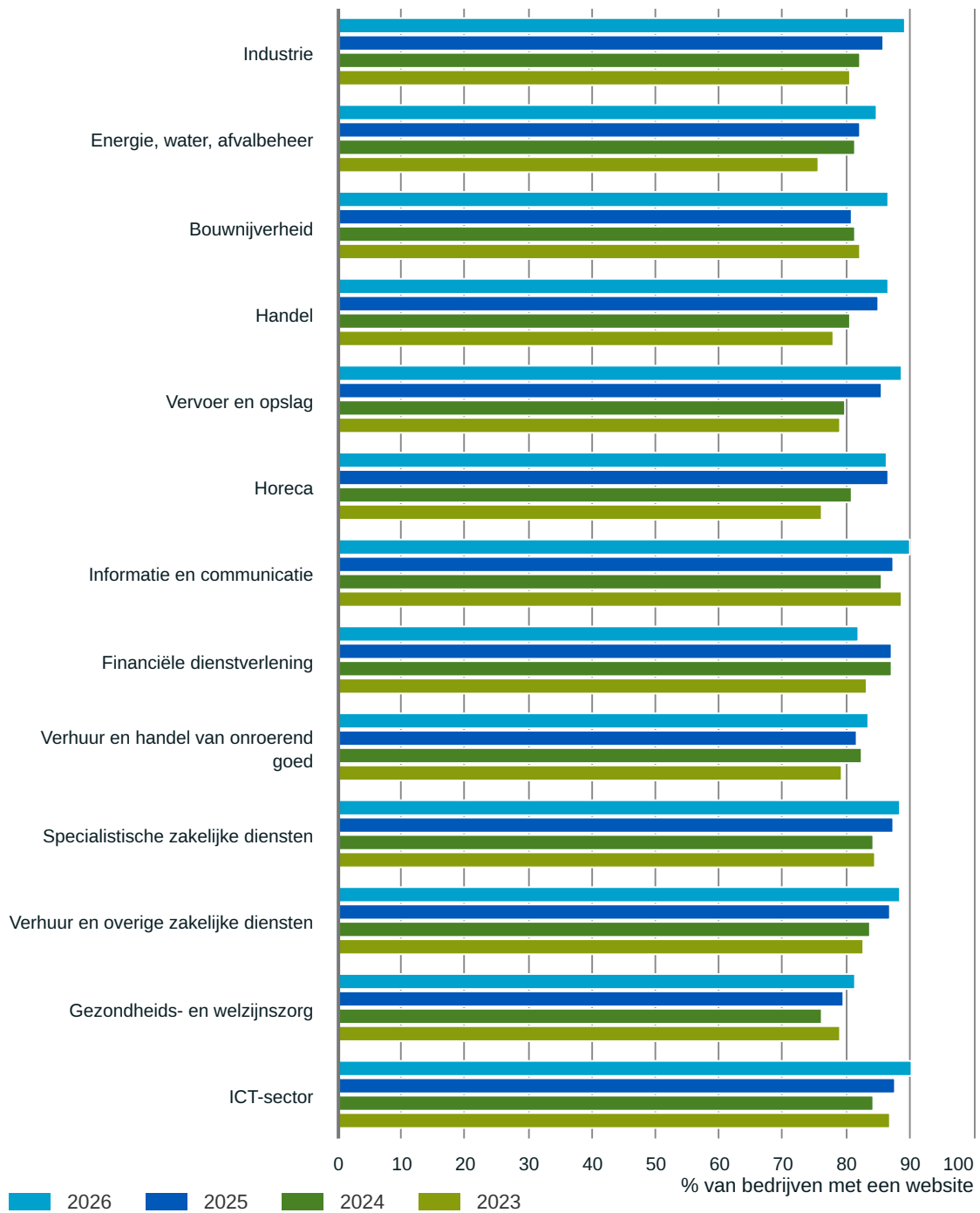
In deze bijlage worden de uitslagen van de e-mailscans weergegeven voor alle jaren. De resultaten voor alle subtesten worden gegeven in: Paragraaf C.1 voor de categorie IPv6, Paragraaf C.2 voor de categorie DNSSEC, Paragraaf C.4 voor de categorie Beveiligd e-mailtransport (STARTTLS en DANE), Paragraaf C.3 voor de categorie Authenticiteit, en Paragraaf C.5 voor de categorie RPKI. Zie Paragraaf A.3 voor een korte uitleg per subtest. Tot slot wordt de verdeling van de eindscores getoond voor alle jaren in Paragraaf C.6.

### C.1. E-mailscanuitslagen voor categorie IPv6

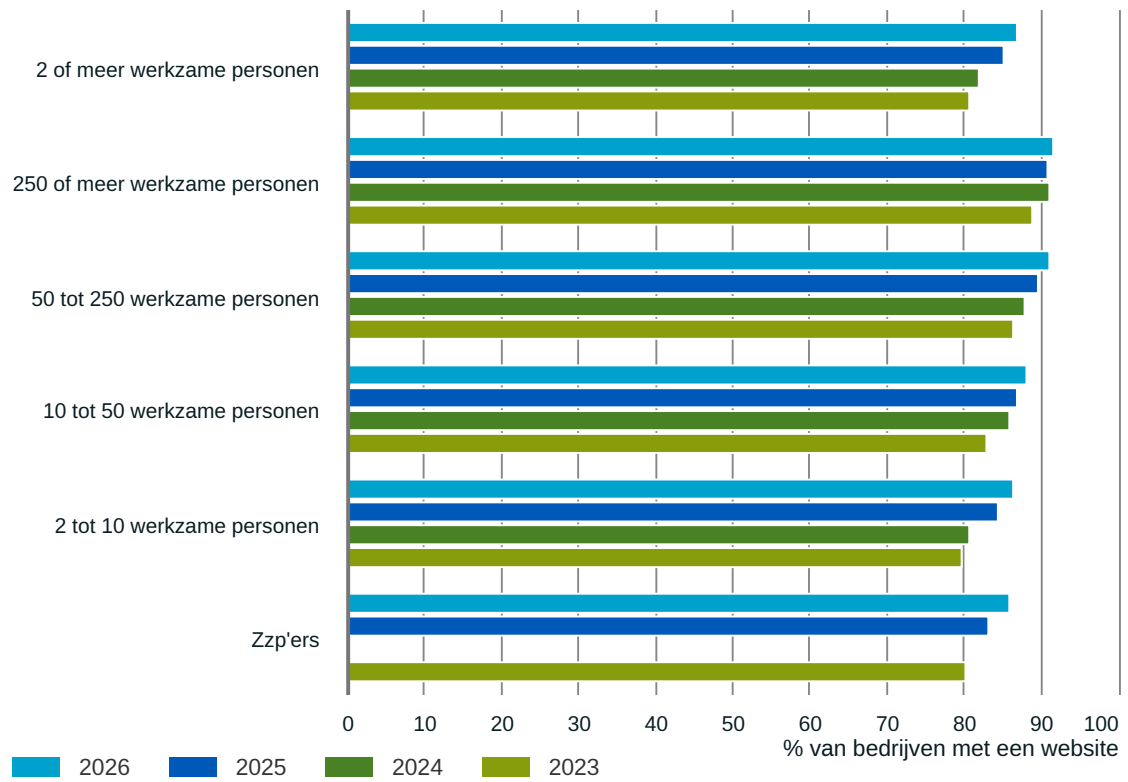
Figuur C.1.: Percentage van bedrijven met een website met geslaagde e-mailtest 'IPv6-adressen voor nameservers' naar bedrijfsgrootteklasse



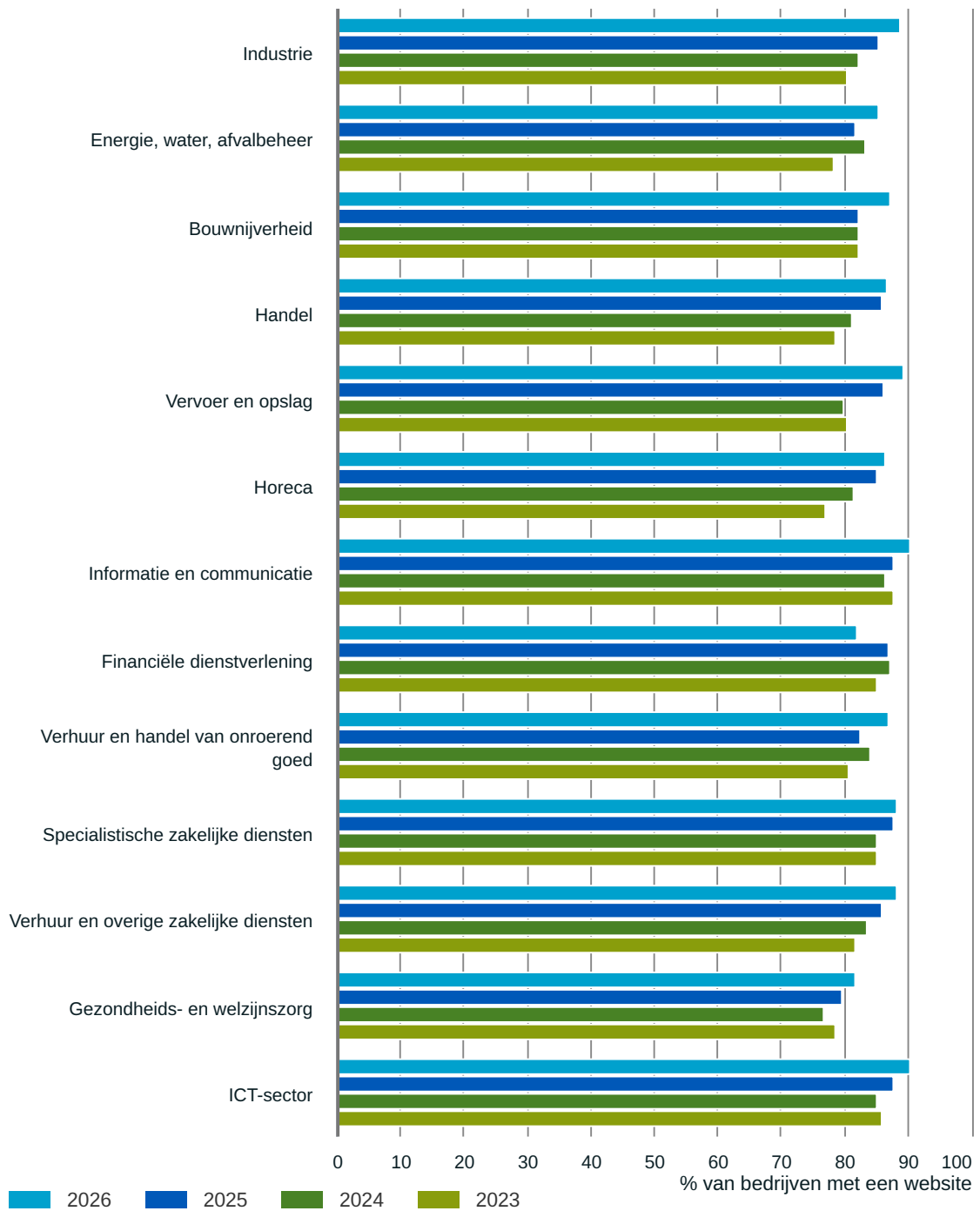
Figuur C.2.: Percentage van bedrijven met een website met geslaagde e-mailtest 'IPv6-adressen voor nameservers' naar bedrijfstak (2 of meer werkzame personen)



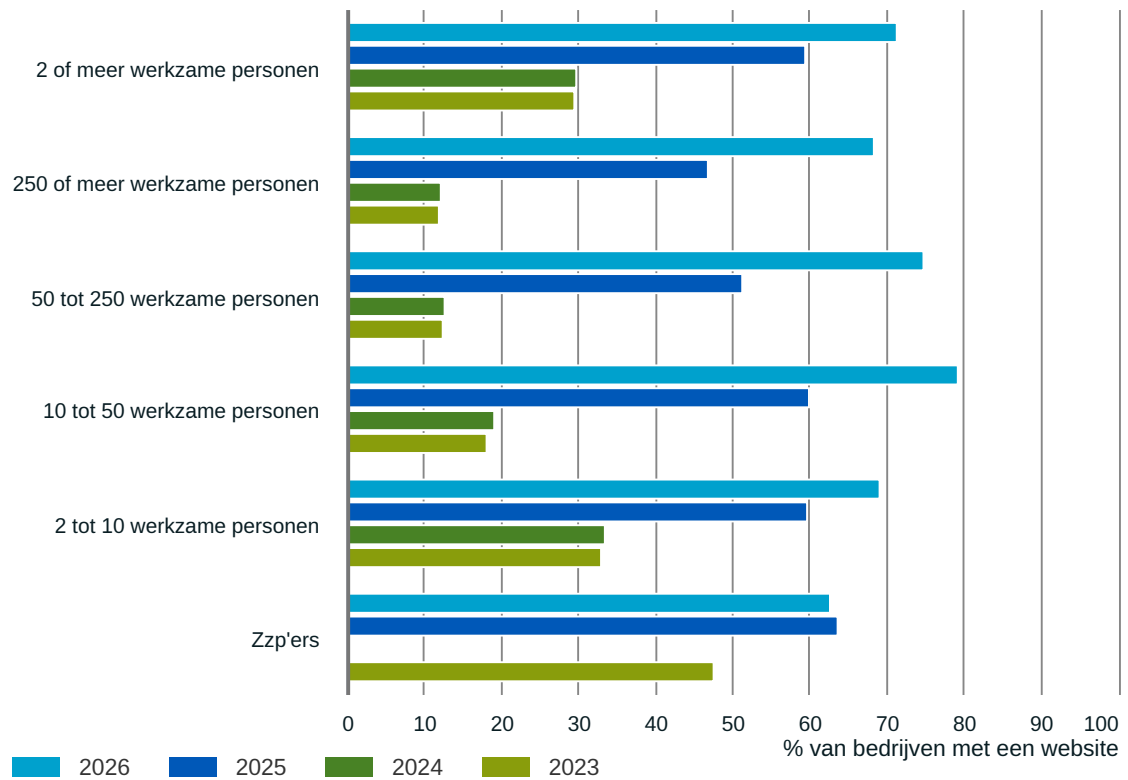
Figuur C.3.: Percentage van bedrijven met een website met geslaagde e-mailtest 'IPv6-bereikbaarheid voor nameservers' naar bedrijfsgrootteklasse



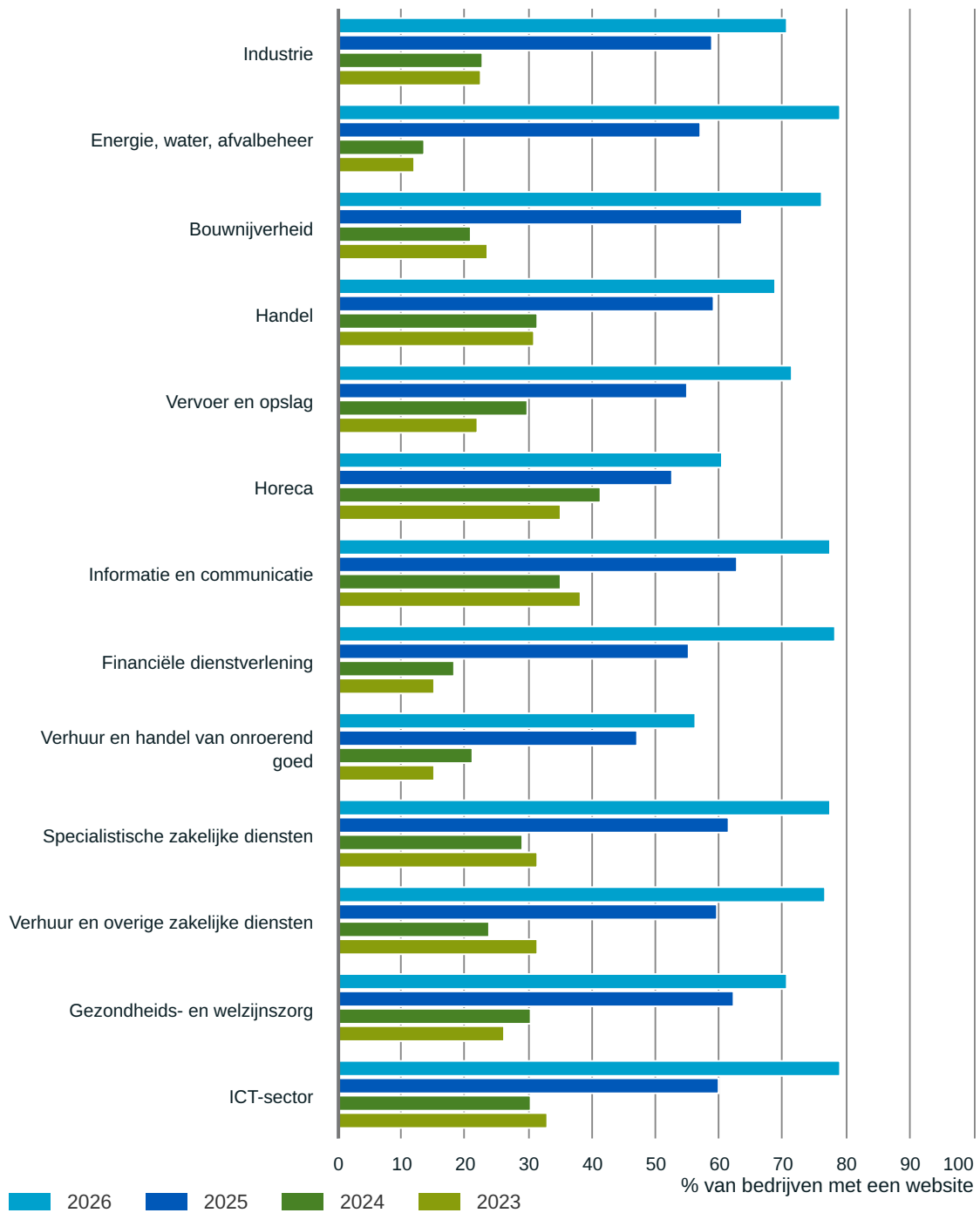
Figuur C.4.: Percentage van bedrijven met een website met geslaagde e-mailtest 'IPv6-bereikbaarheid voor nameservers' naar bedrijfstak (2 of meer werkzame personen)



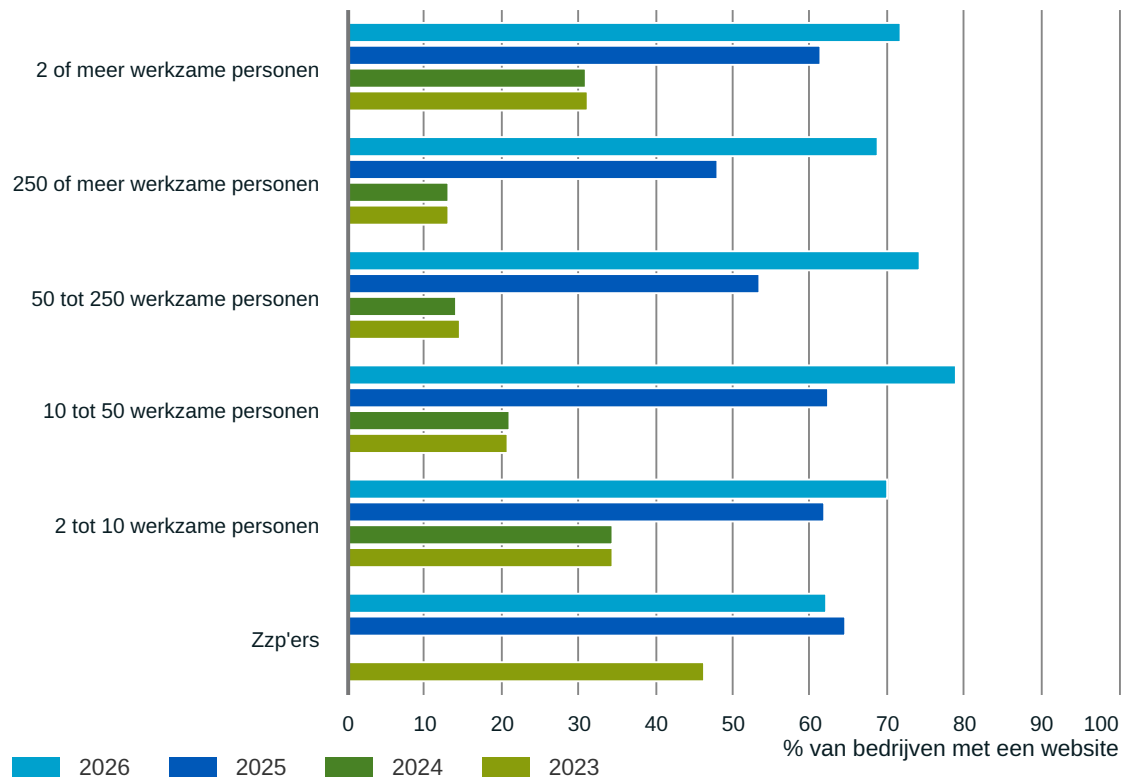
Figuur C.5.: Percentage van bedrijven met een website met geslaagde e-mailtest 'IPv6-adressen voor mailservers' naar bedrijfsgrootteklasse



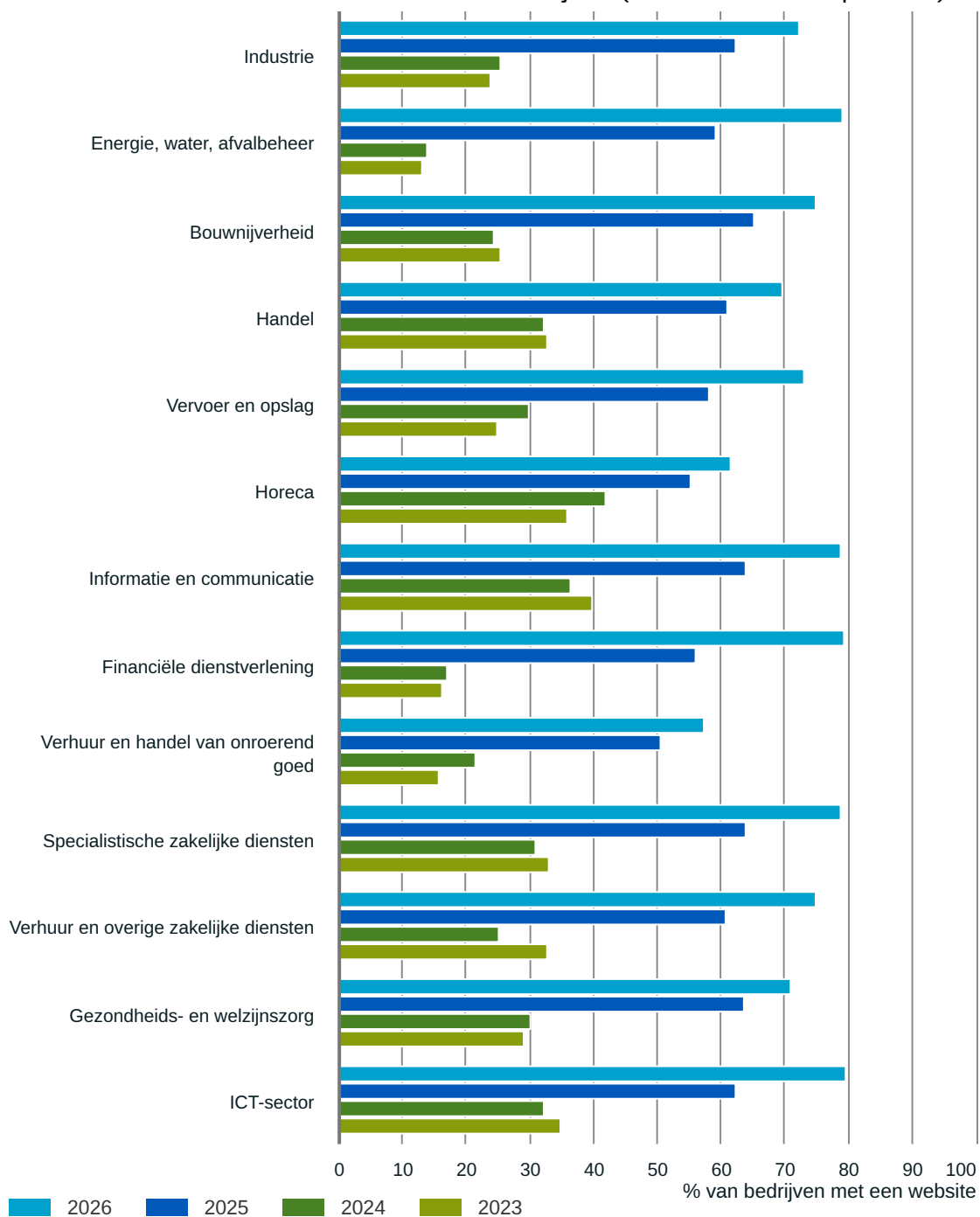
Figuur C.6.: Percentage van bedrijven met een website met geslaagde e-mailtest 'IPv6-adressen voor mailservers' naar bedrijfstak (2 of meer werkzame personen)



Figuur C.7.: Percentage van bedrijven met een website met geslaagde e-mailtest 'IPv6-bereikbaarheid voor mailservers' naar bedrijfsgrootteklasse

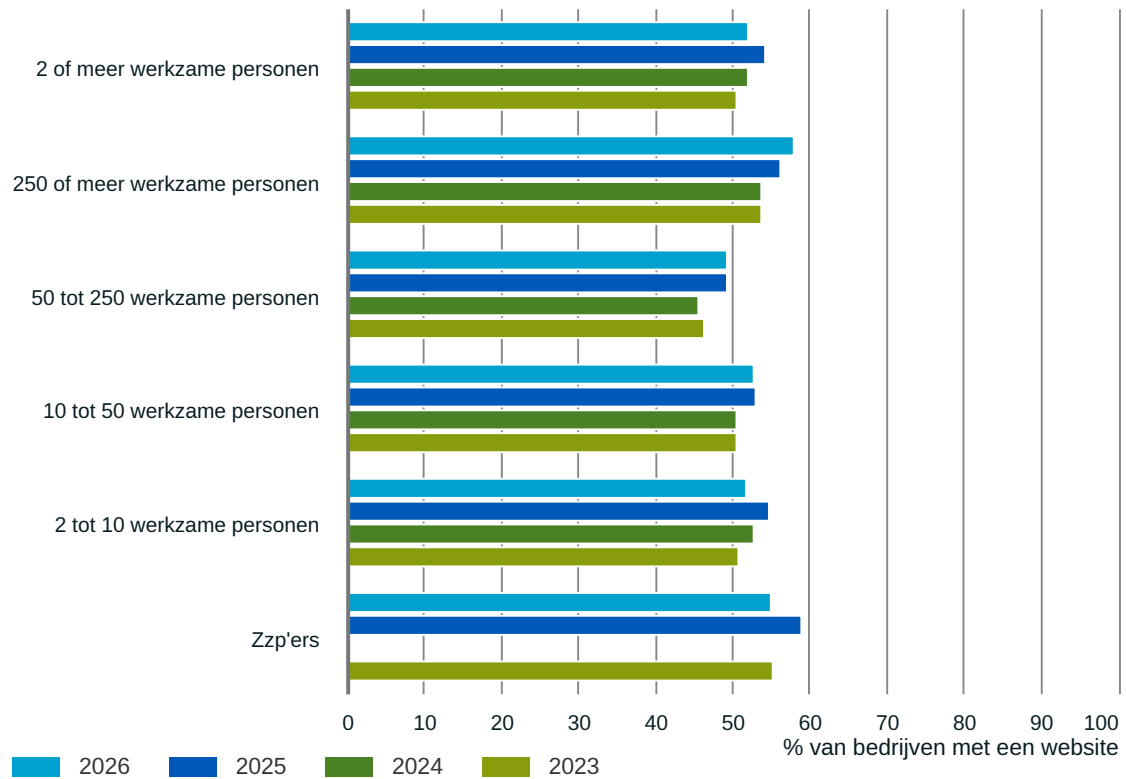


Figuur C.8.: Percentage van bedrijven met een website met geslaagde e-mailtest 'IPv6-bereikbaarheid voor mailservers' naar bedrijfstak (2 of meer werkzame personen)

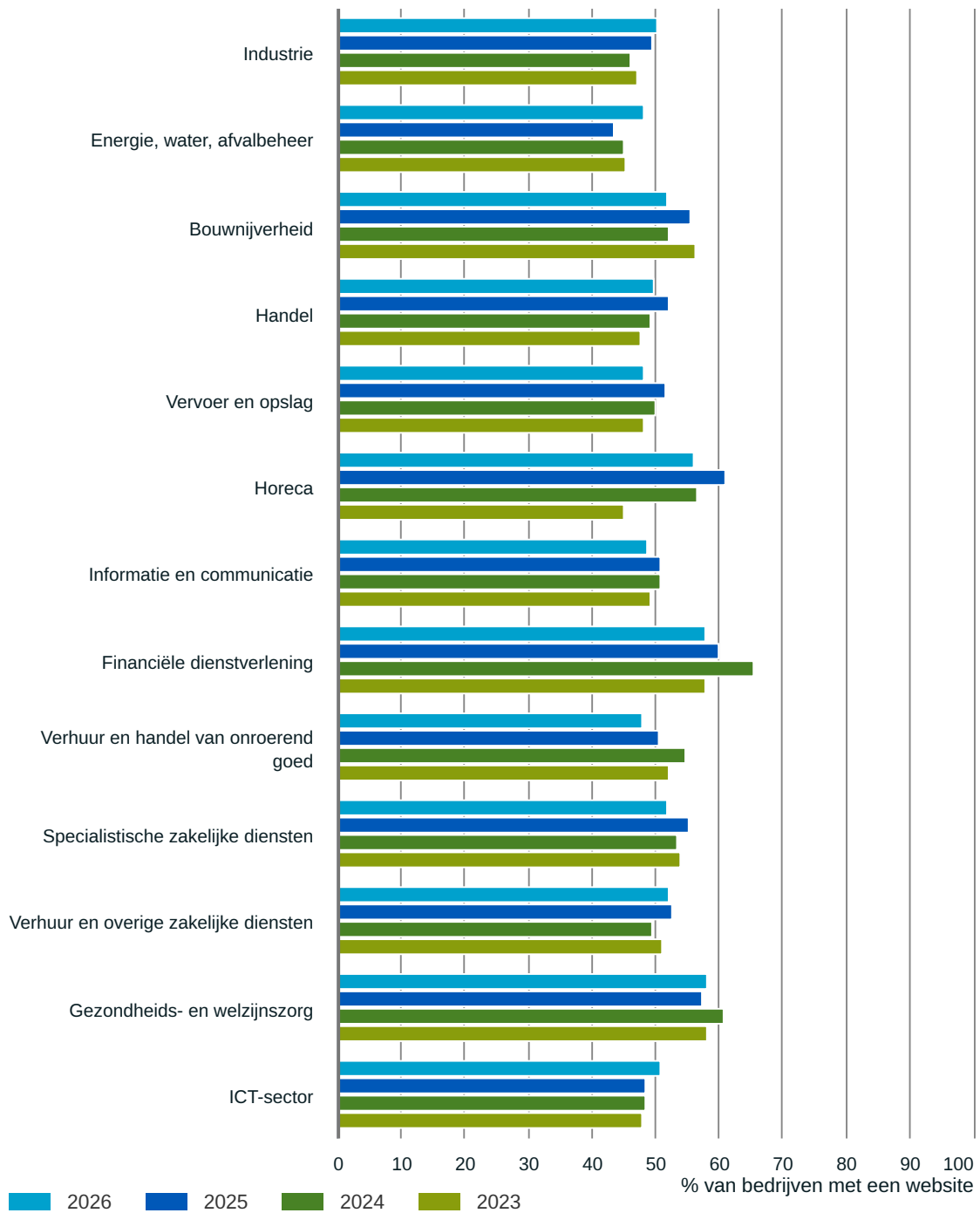


## C.2. E-mailscanuitslagen voor categorie DNSSEC

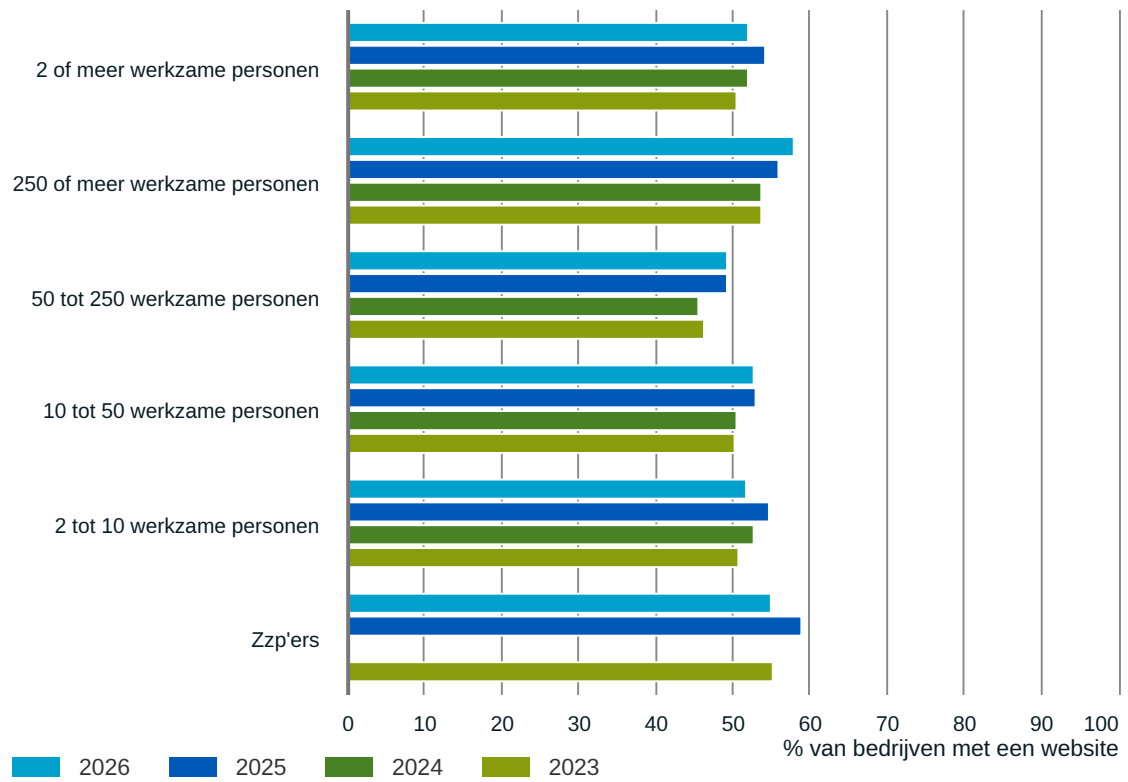
Figuur C.9.: Percentage van bedrijven met een website met geslaagde e-mailtest 'DNSSEC aanwezig voor het e-mailadresdomein' naar bedrijfsgrootteklasse



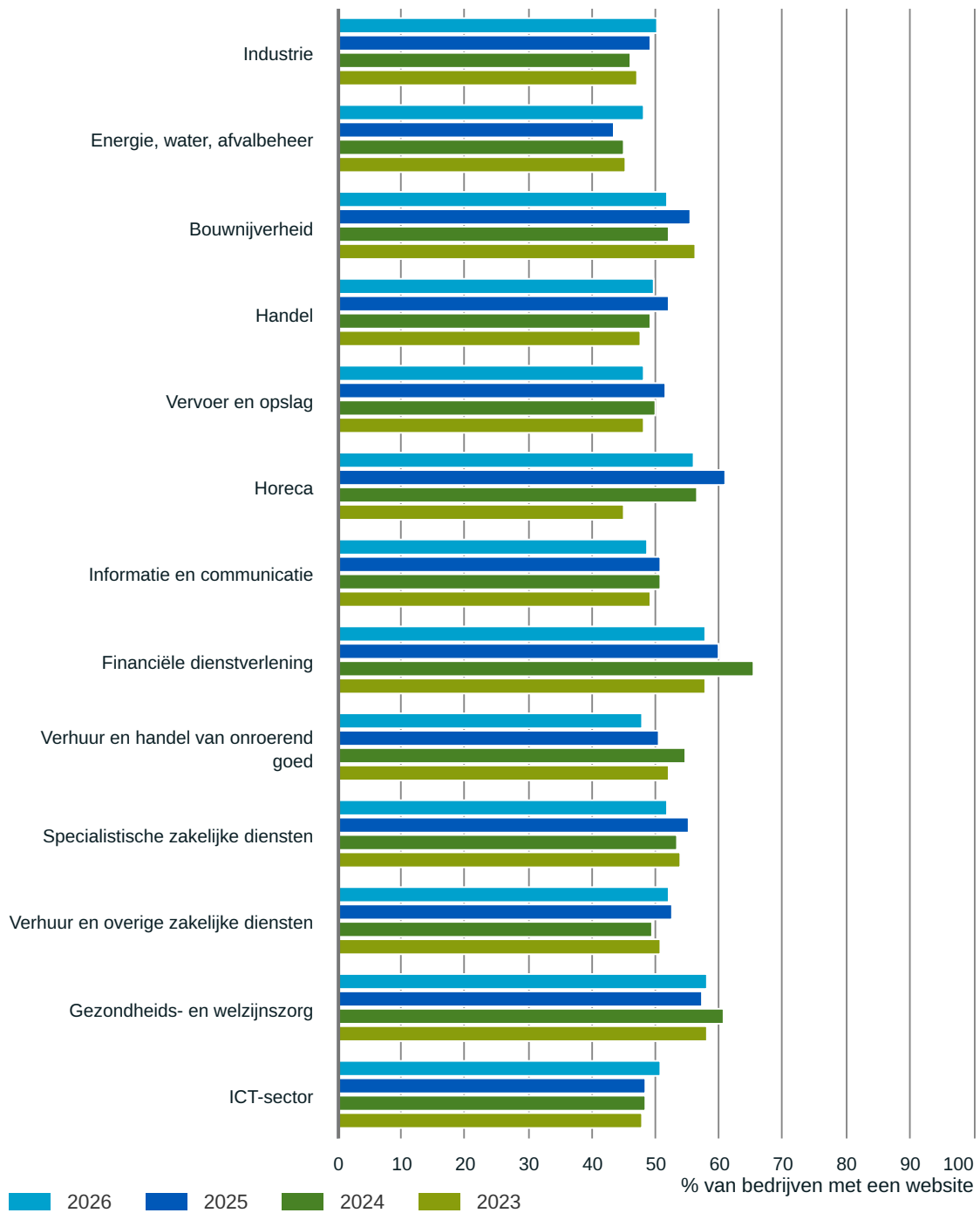
Figuur C.10.: Percentage van bedrijven met een website met geslaagde e-mailtest 'DNSSEC aanwezig voor het e-mailadresdomein' naar bedrijfstak (2 of meer werkzame personen)



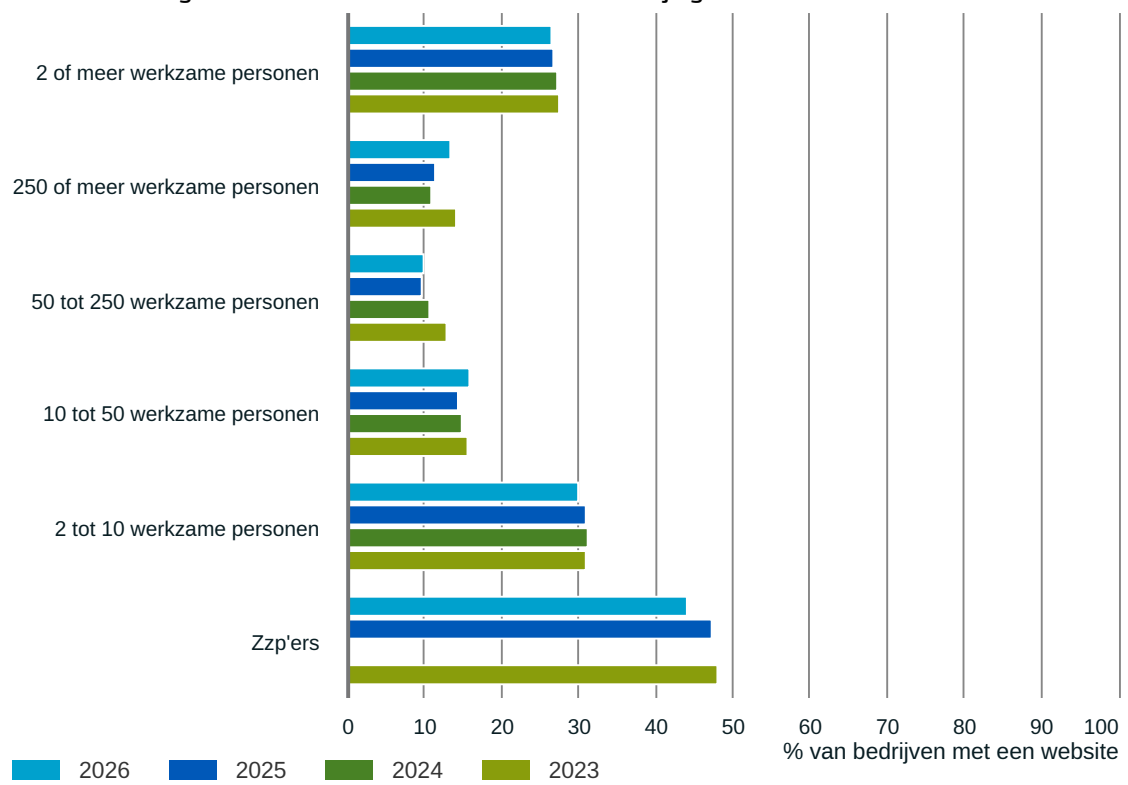
**Figuur C.11.: Percentage van bedrijven met een website met geslaagde e-mailtest 'DNSSEC geldig voor het e-mailadresdomein' naar bedrijfsgrootteklasse**



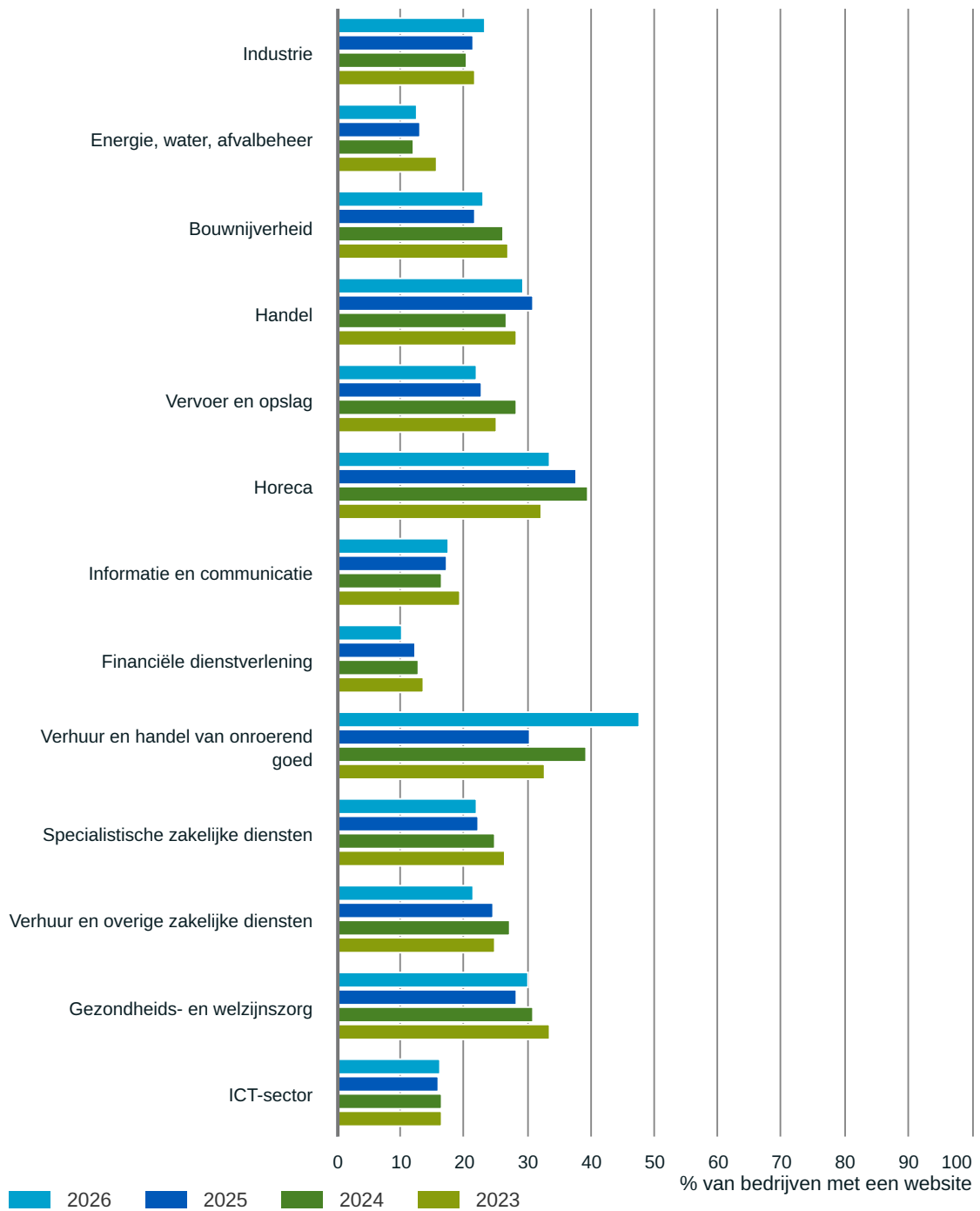
Figuur C.12.: Percentage van bedrijven met een website met geslaagde e-mailtest 'DNSSEC geldig voor het e-mailadresdomein' naar bedrijfstak (2 of meer werkzame personen)



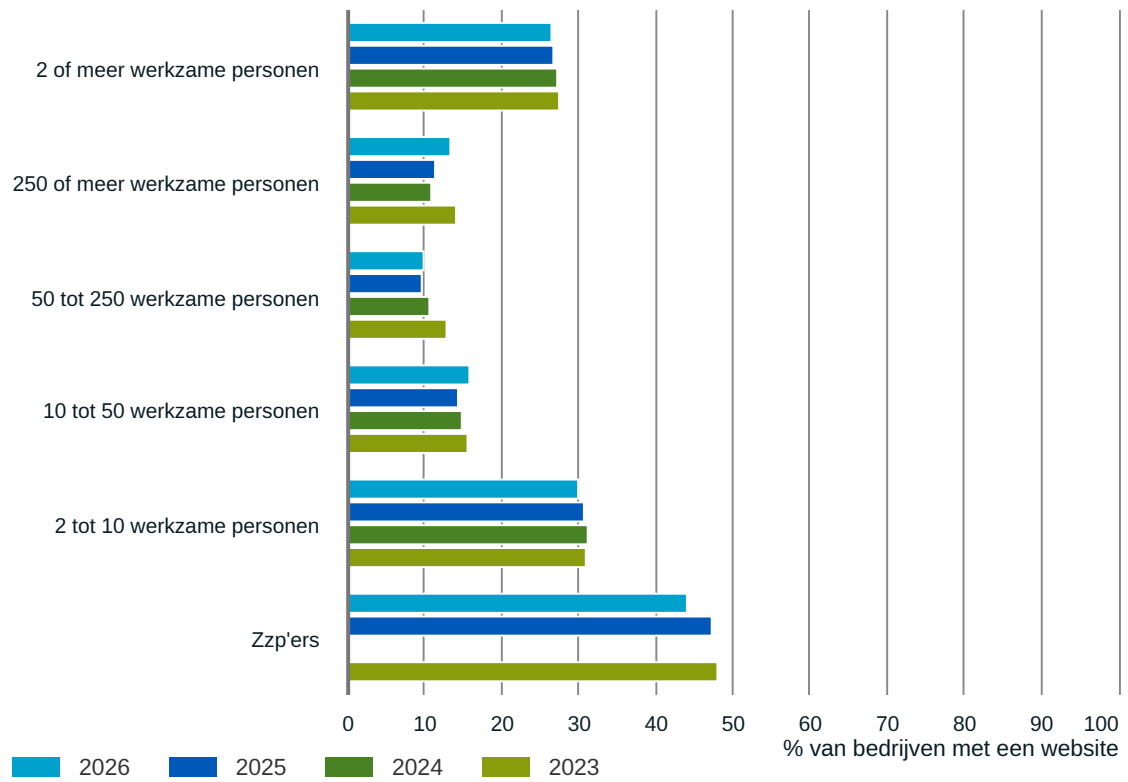
Figuur C.13.: Percentage van bedrijven met een website met geslaagde e-mailtest 'DNSSEC aanwezig voor het e-mailserverdomein' naar bedrijfsgrootteklasse



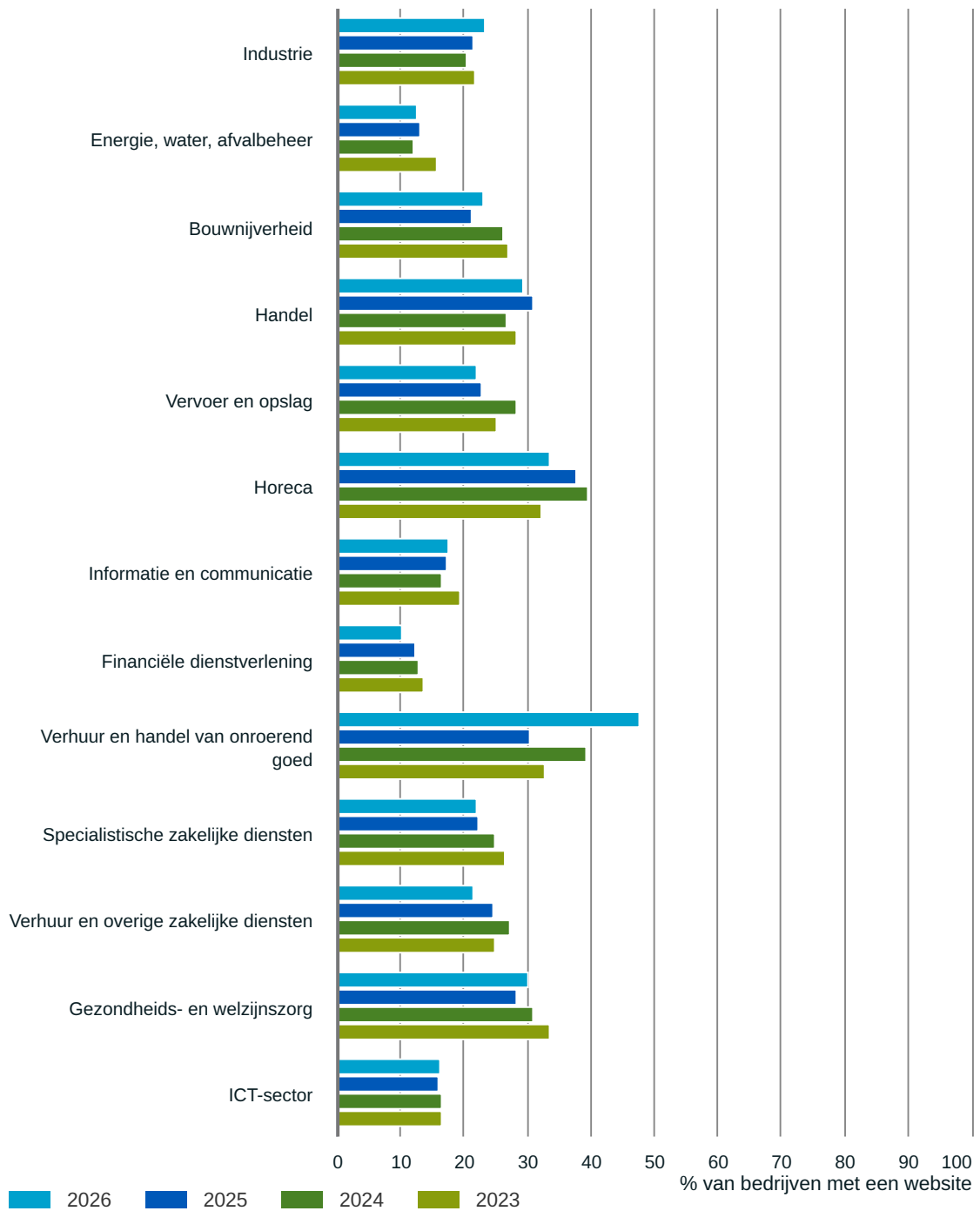
Figuur C.14.: Percentage van bedrijven met een website met geslaagde e-mailtest 'DNSSEC aanwezig voor het e-mailserverdomein' naar bedrijfstak (2 of meer werkzame personen)



Figuur C.15.: Percentage van bedrijven met een website met geslaagde e-mailtest 'DNSSEC geldig voor het e-mailserverdomein' naar bedrijfsgrootteklasse

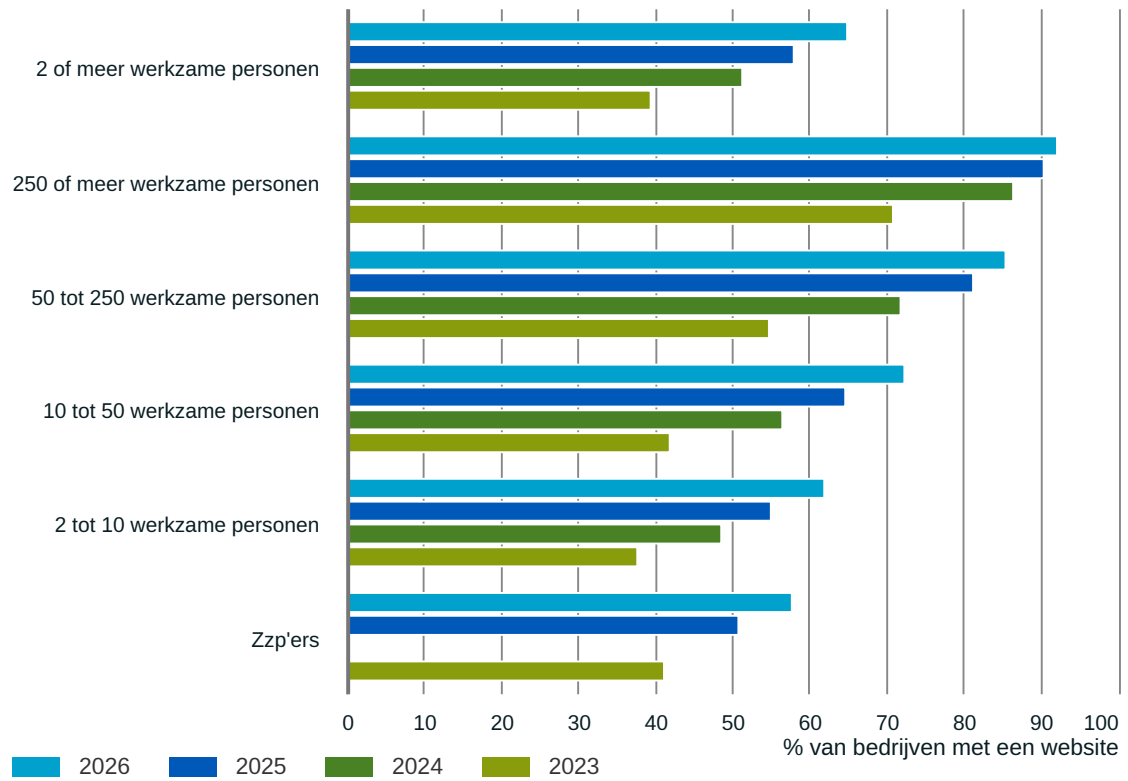


Figuur C.16.: Percentage van bedrijven met een website met geslaagde e-mailtest 'DNSSEC geldig voor het e-mailserverdomein' naar bedrijfstak (2 of meer werkzame personen)

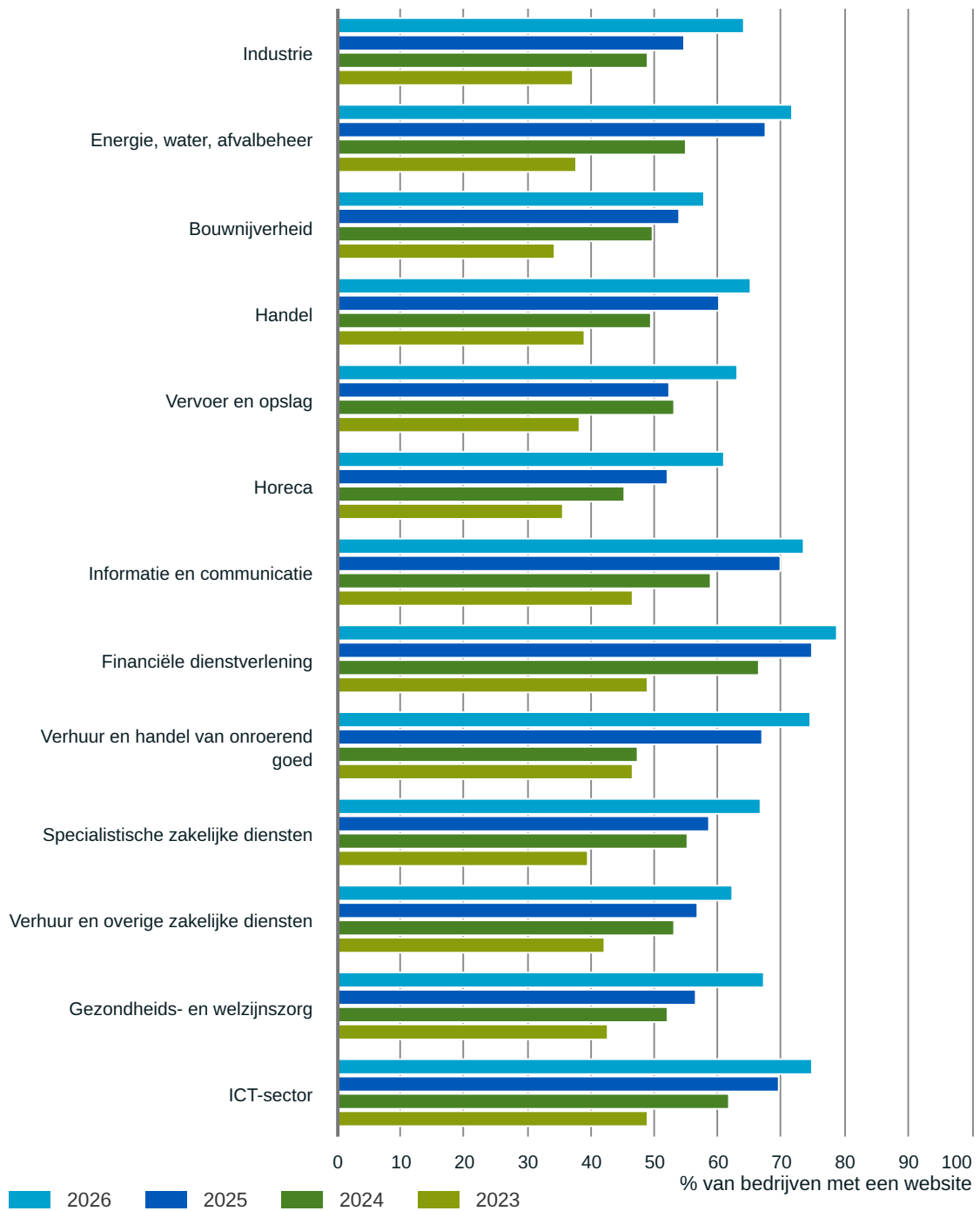


### C.3. E-mailscanuitslagen voor categorie Authenticiteit

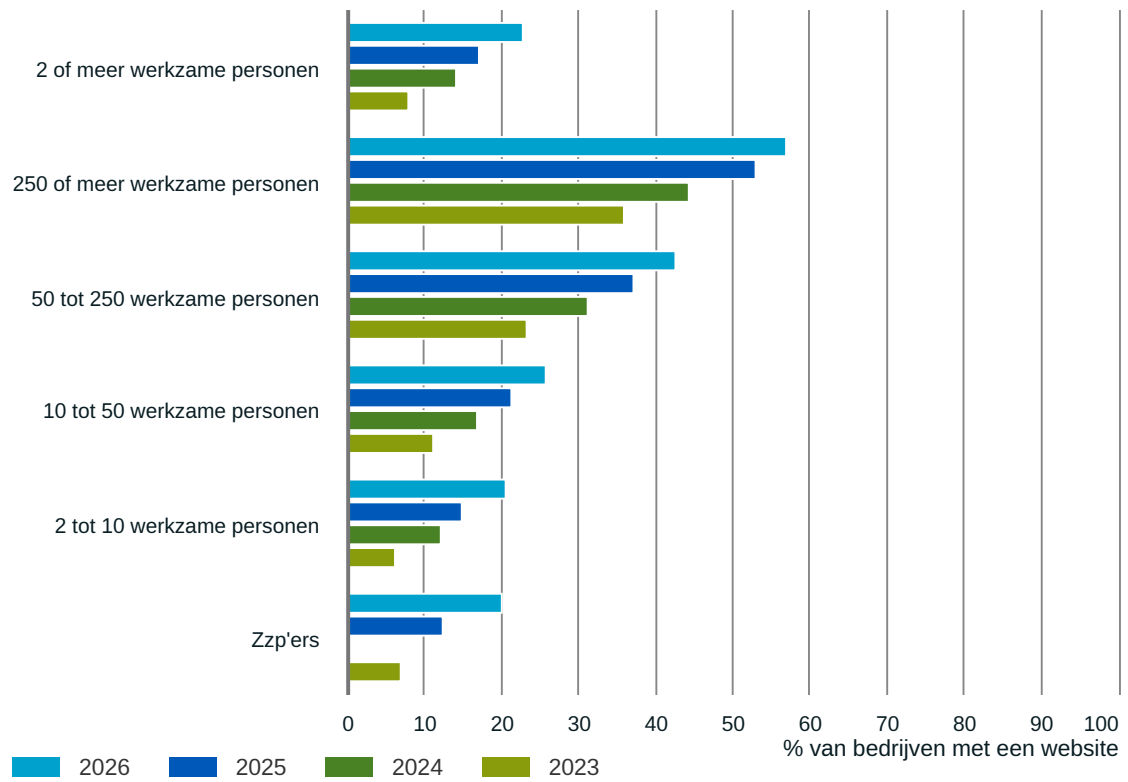
Figuur C.17.: Percentage van bedrijven met een website met geslaagde e-mailtest 'DMARC aanwezigheid' naar bedrijfsgrootteklasse



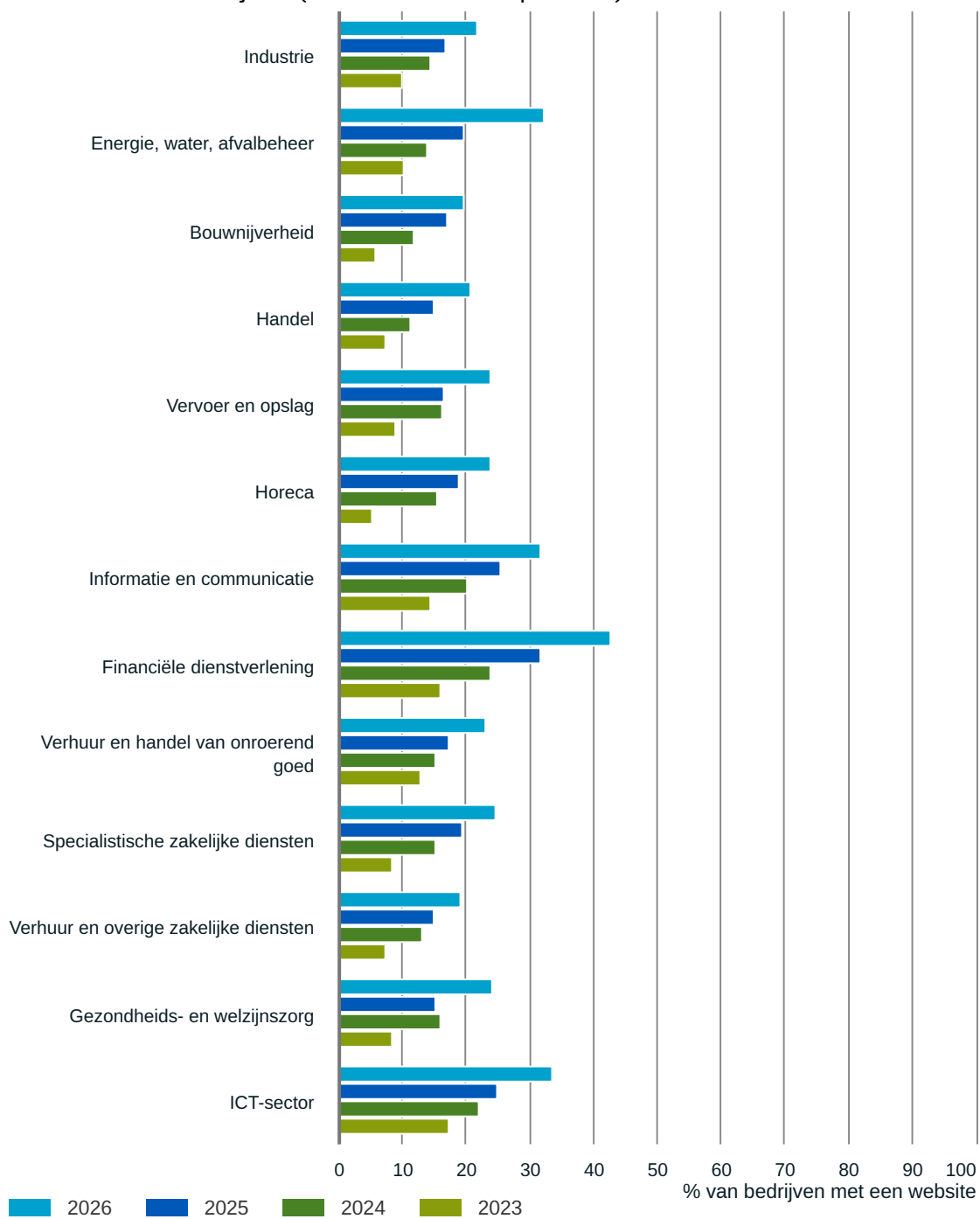
Figuur C.18.: Percentage van bedrijven met een website met geslaagde e-mailtest 'DMARC aanwezigheid' naar bedrijfstak (2 of meer werkzame personen)



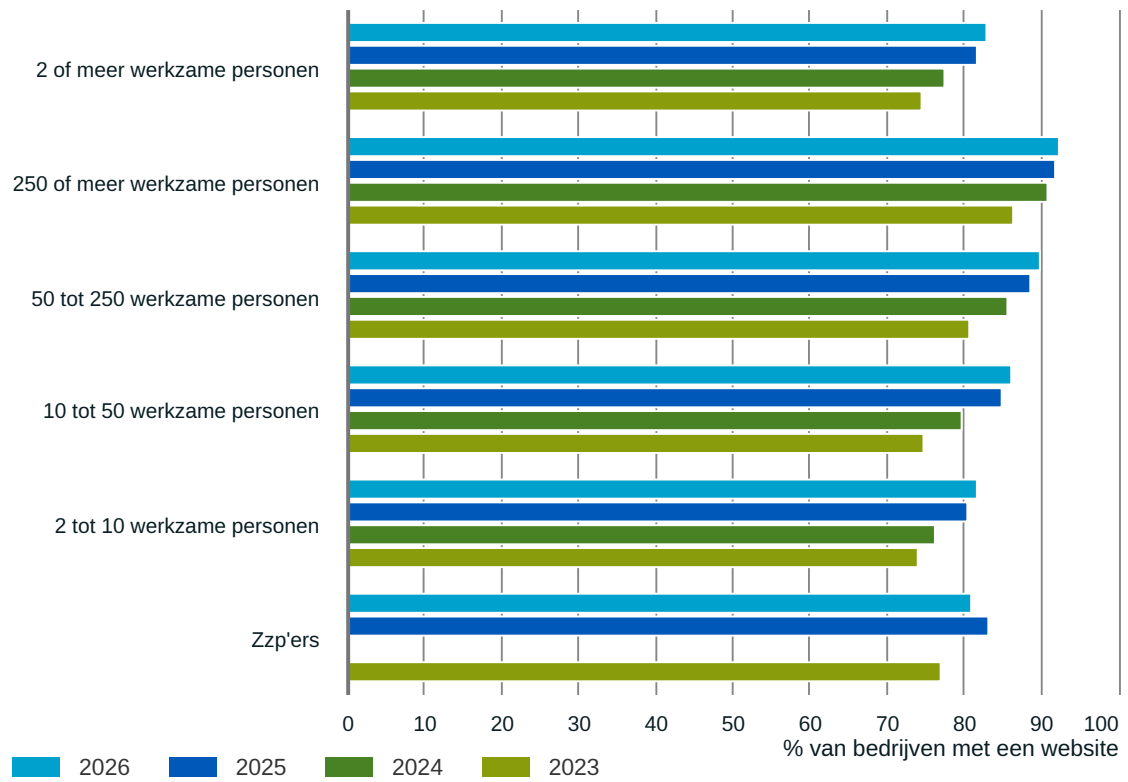
Figuur C.19.: Percentage van bedrijven met een website met geslaagde e-mailtest 'DMARC policy' naar bedrijfsgrootteklasse



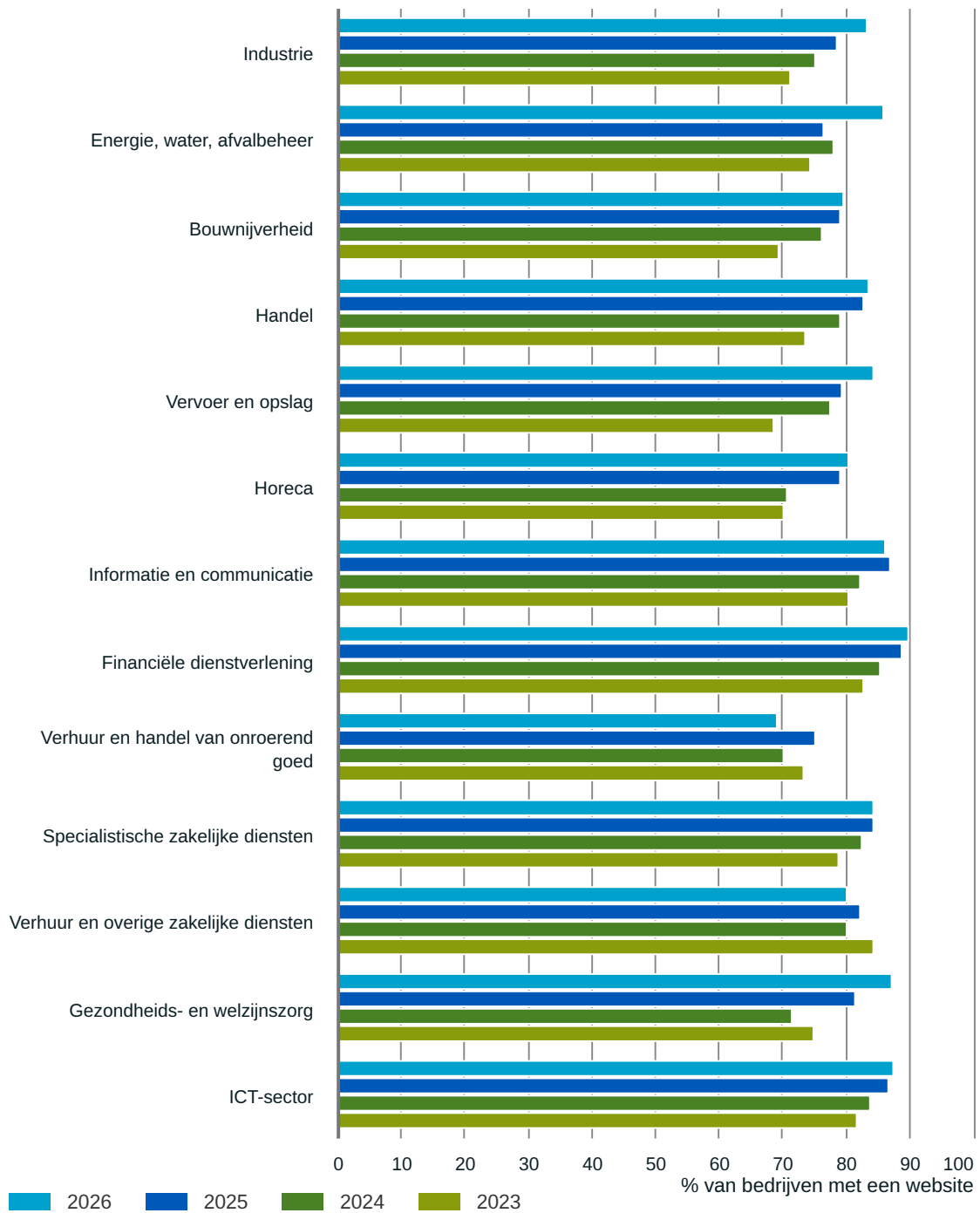
Figuur C.20.: Percentage van bedrijven met een website met geslaagde e-mailtest 'DMARC policy' naar bedrijfstak (2 of meer werkzame personen)



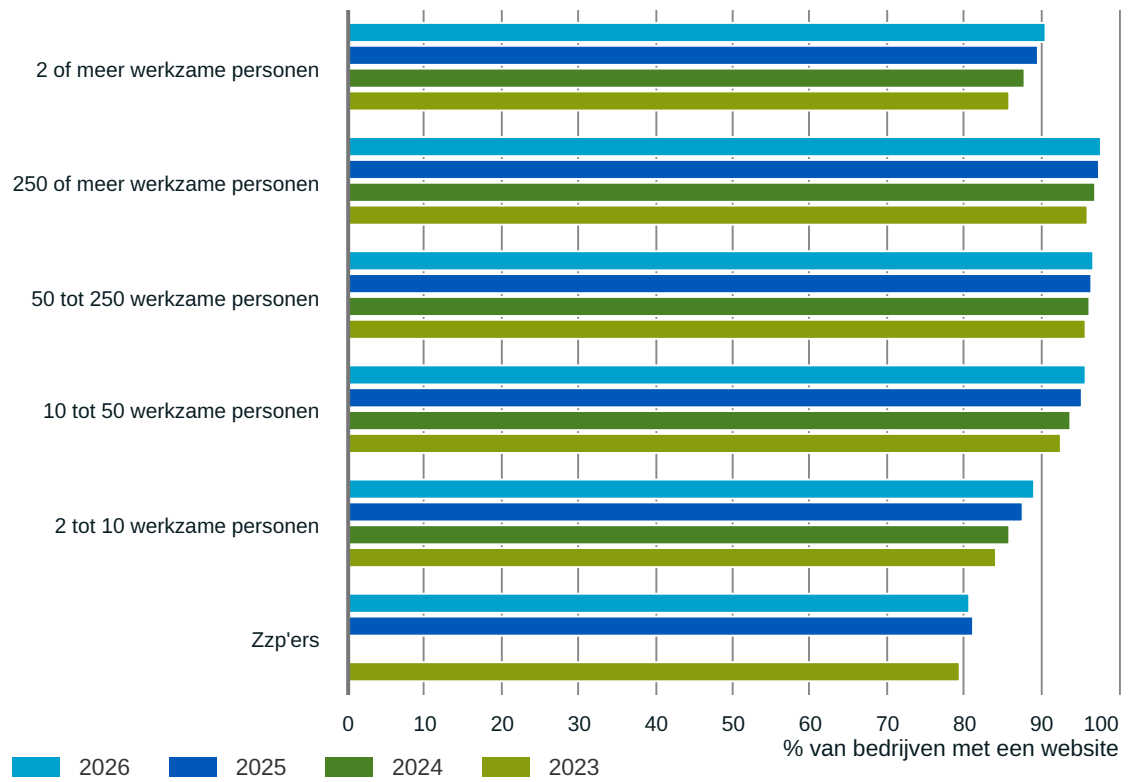
Figuur C.21.: Percentage van bedrijven met een website met geslaagde e-mailtest 'DKIM aanwezigheid' naar bedrijfsgrootteklasse



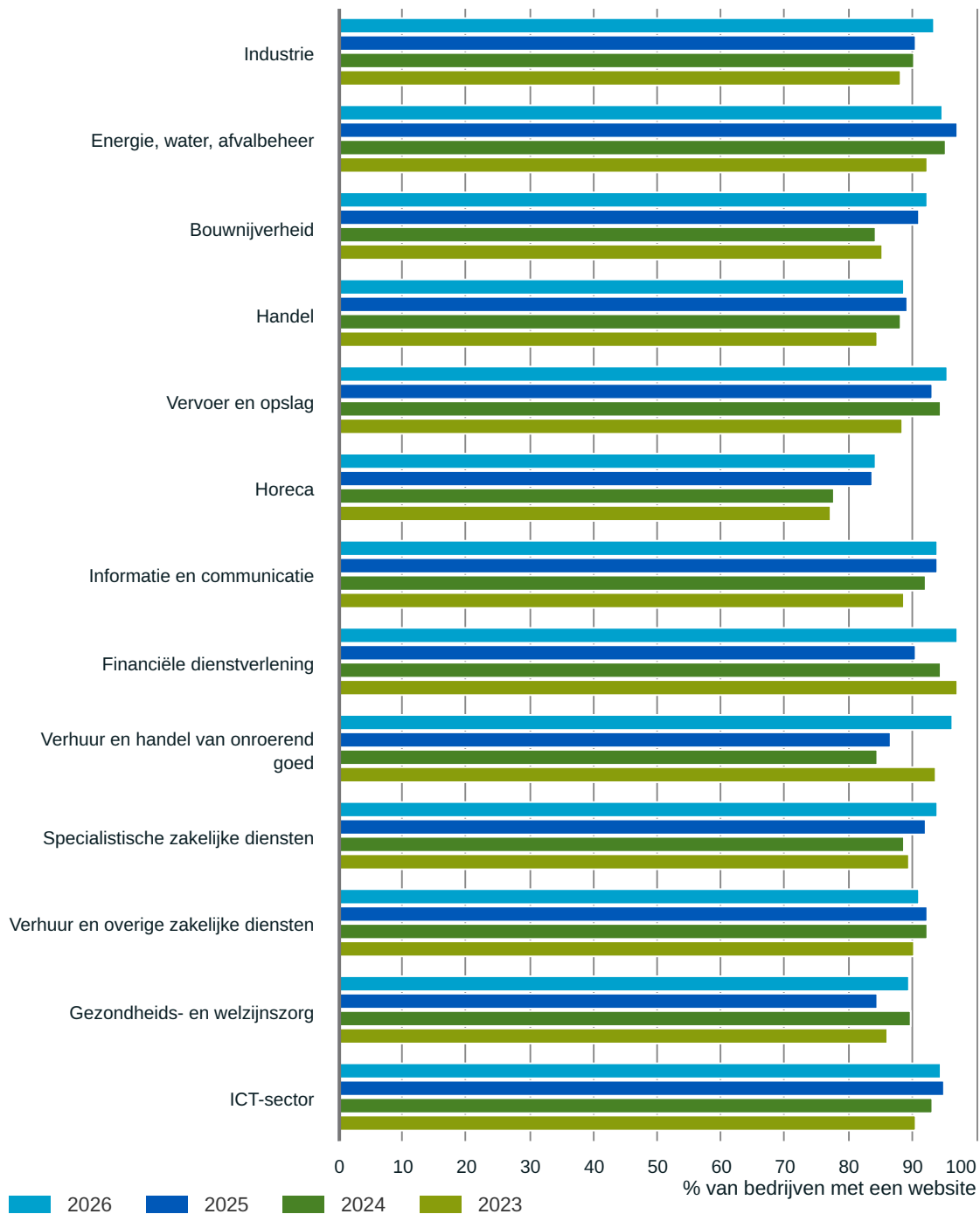
Figuur C.22.: Percentage van bedrijven met een website met geslaagde e-mailtest 'DKIM aanwezigheid' naar bedrijfstak (2 of meer werkzame personen)



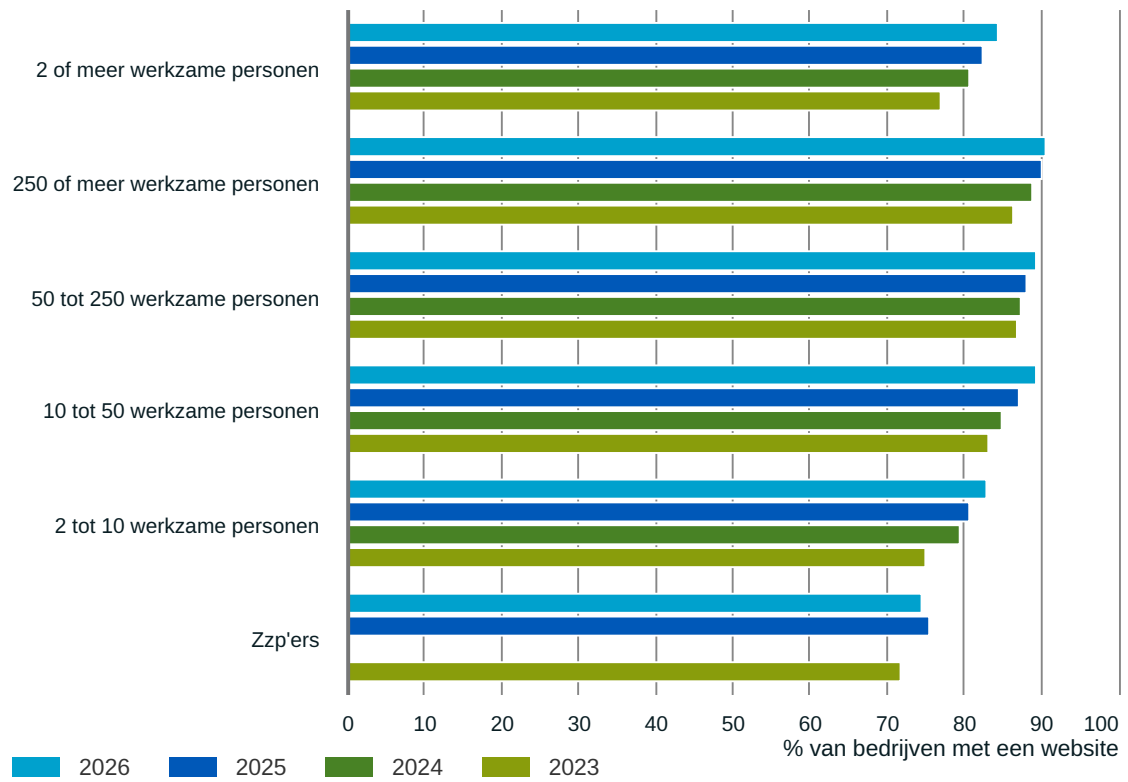
Figuur C.23.: Percentage van bedrijven met een website met geslaagde e-mailtest 'SPF aanwezigheid' naar bedrijfsgrootteklasse



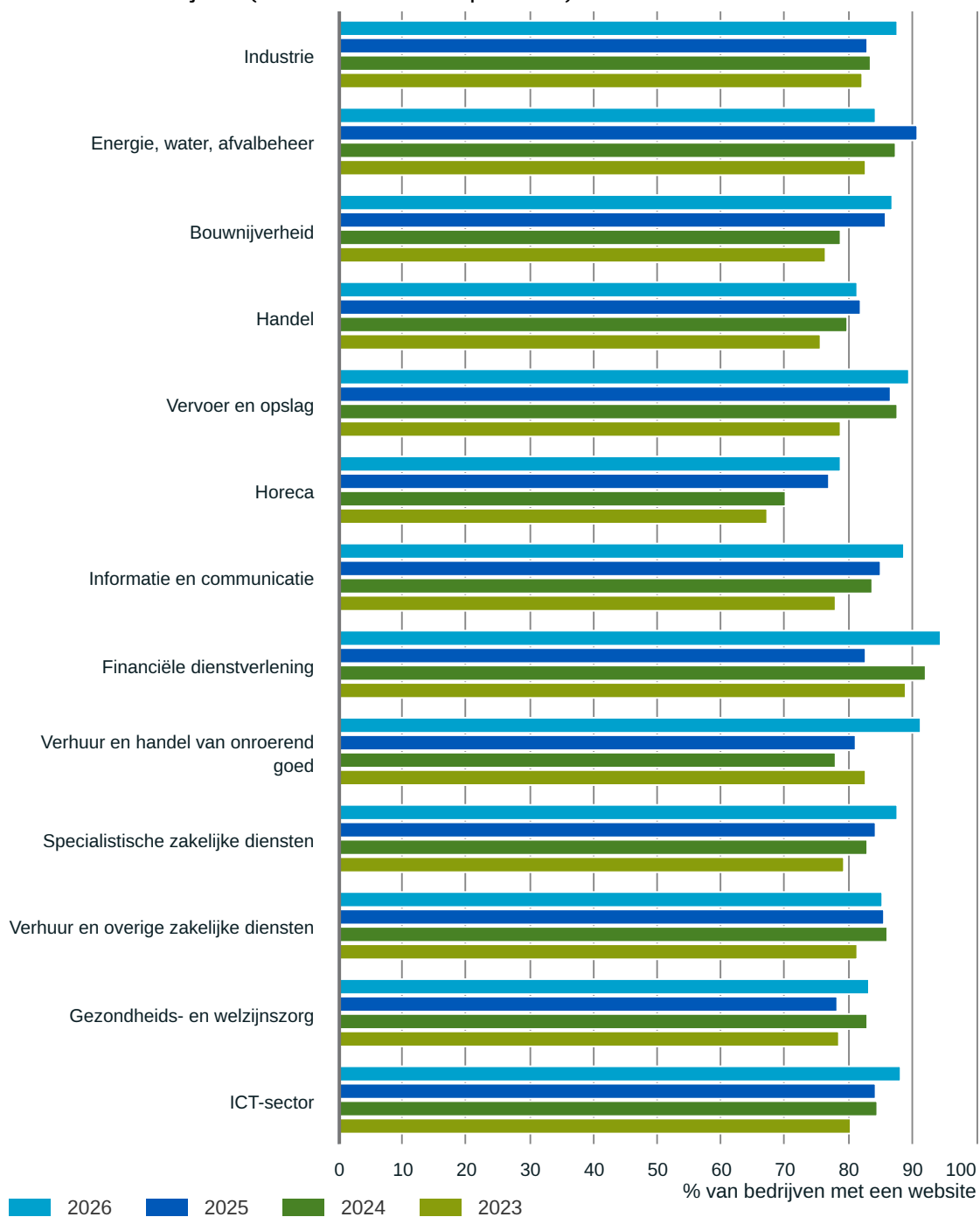
Figuur C.24.: Percentage van bedrijven met een website met geslaagde e-mailtest 'SPF aanwezigheid' naar bedrijfstak (2 of meer werkzame personen)



Figuur C.25.: Percentage van bedrijven met een website met geslaagde e-mailtest 'SPF policy' naar bedrijfsgrootteklasse

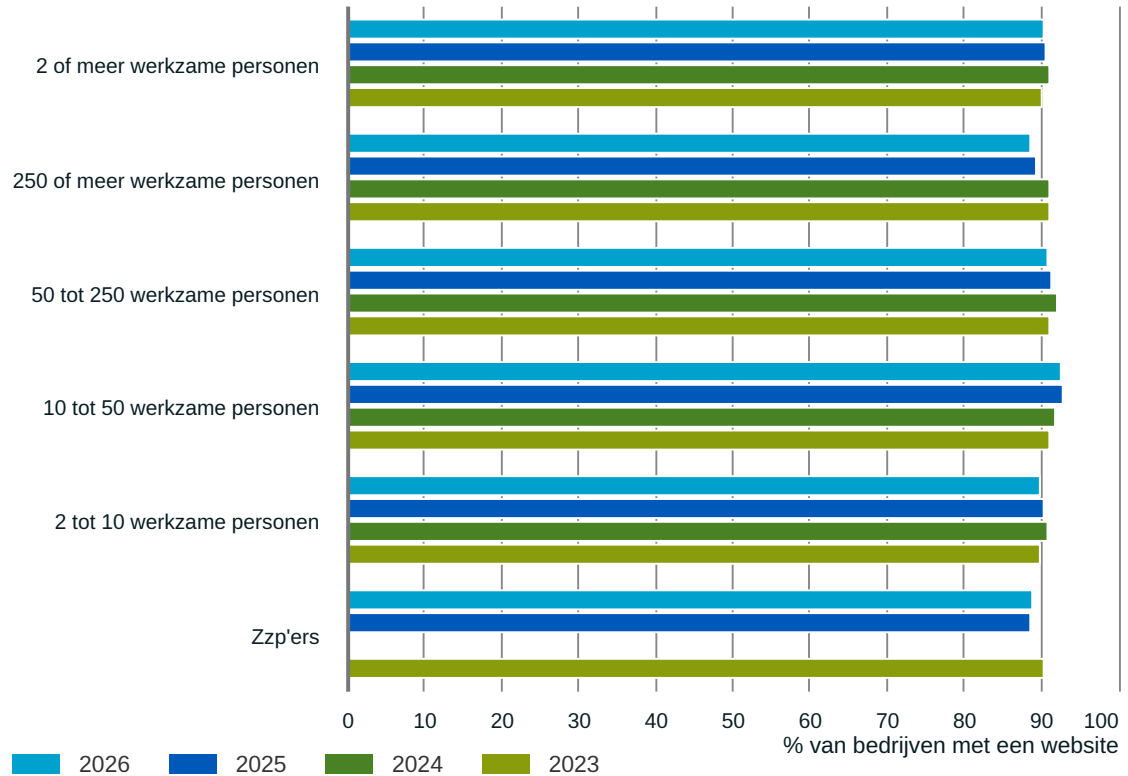


Figuur C.26.: Percentage van bedrijven met een website met geslaagde e-mailtest 'SPF policy' naar bedrijfstak (2 of meer werkzame personen)

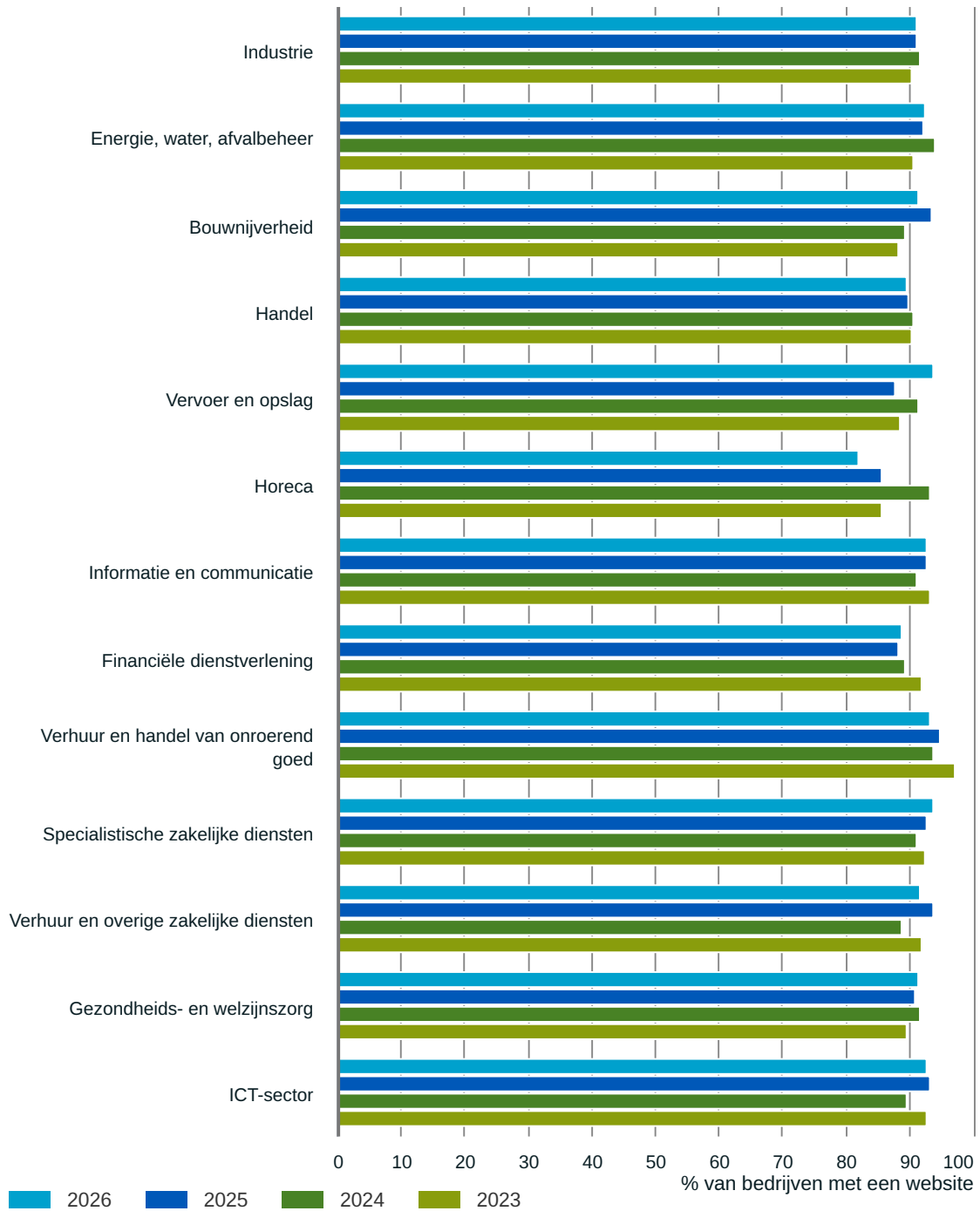


## C.4. E-mailscanuitslagen voor categorie Beveiligd e-mailtransport (STARTTLS en DANE)

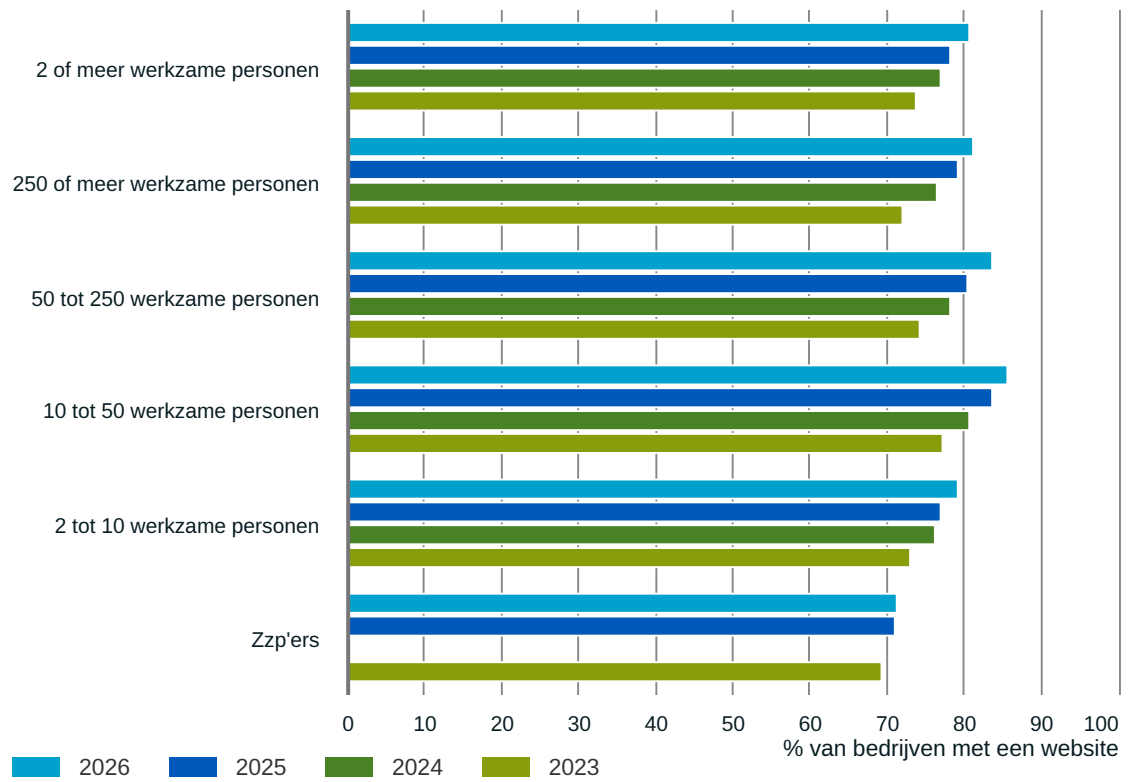
Figuur C.27.: Percentage van bedrijven met een website met geslaagde e-mailtest 'STARTTLS beschikbaar' naar bedrijfsgrootteklasse



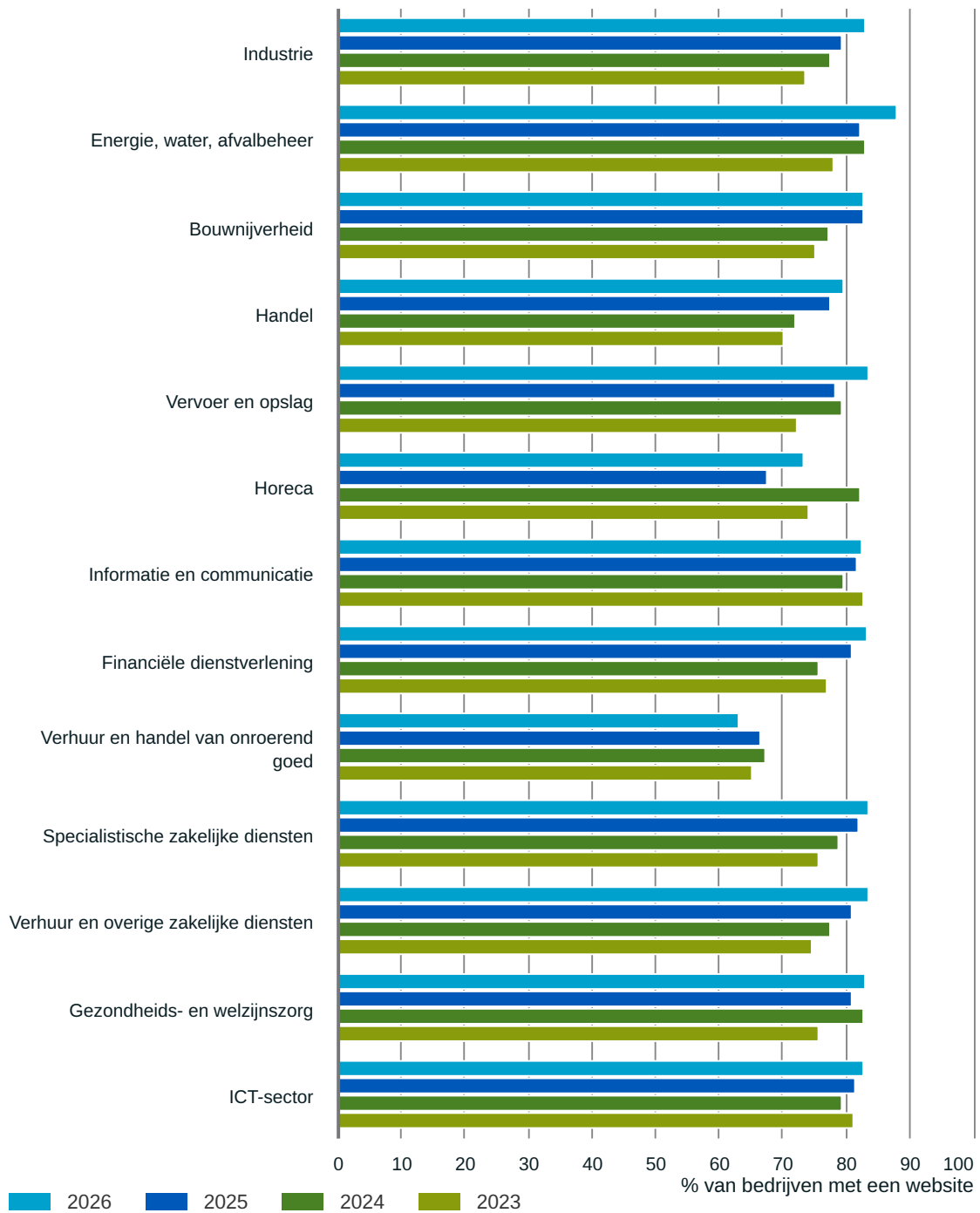
Figuur C.28.: Percentage van bedrijven met een website met geslaagde e-mailtest 'STARTTLS beschikbaar' naar bedrijfstak (2 of meer werkzame personen)



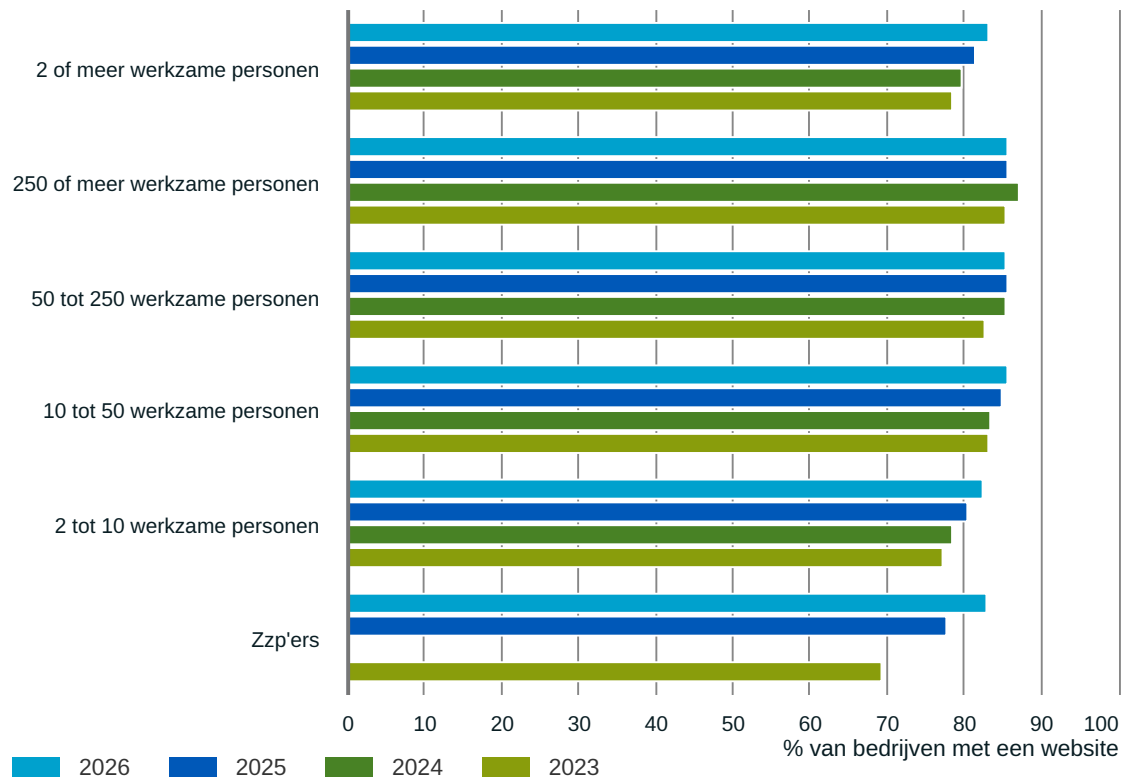
Figuur C.29.: Percentage van bedrijven met een website met geslaagde e-mailtest 'Sleuteluitwisselingsparameters' naar bedrijfsgrootteklasse



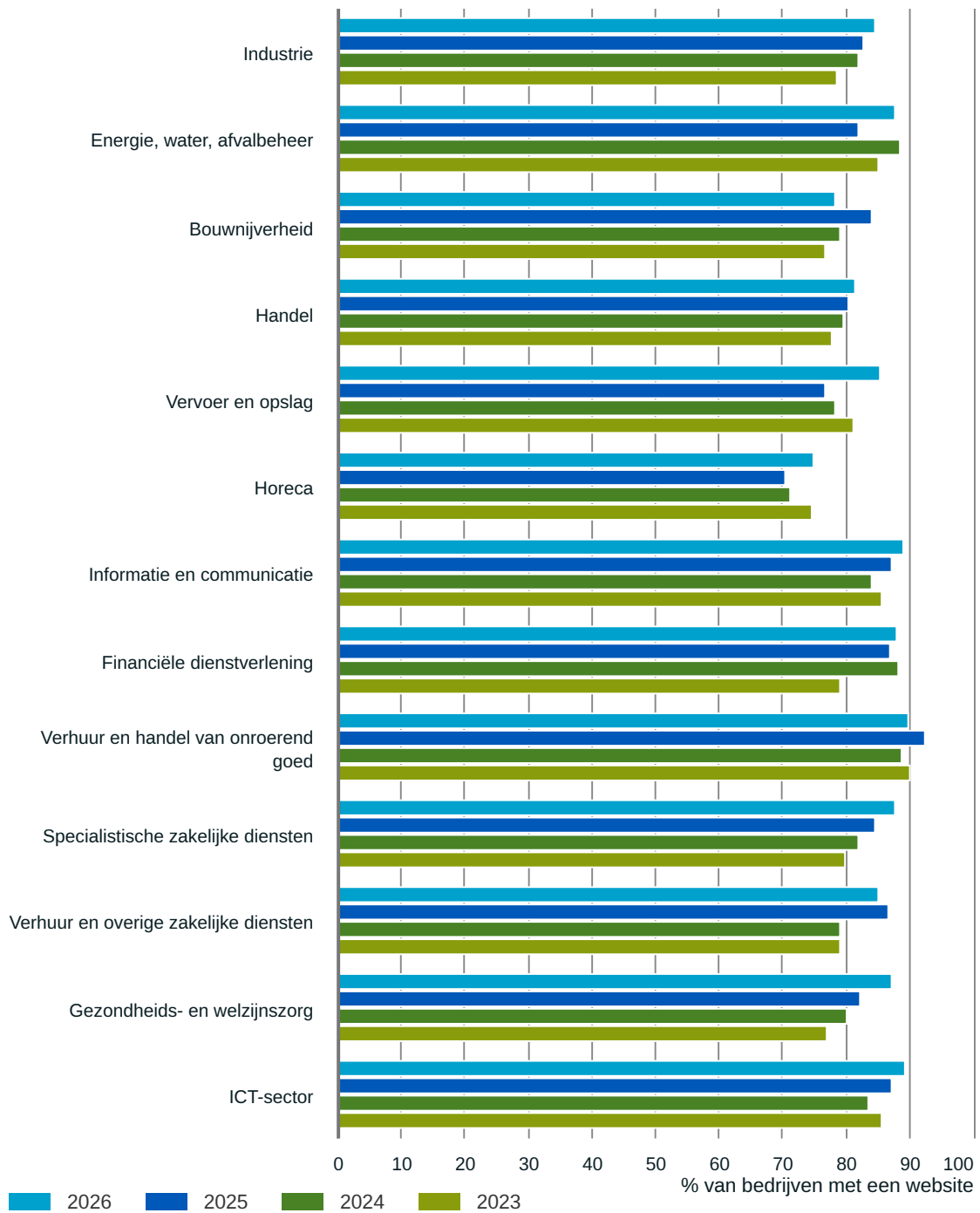
Figuur C.30.: Percentage van bedrijven met een website met geslaagde e-mailtest 'Sleuteluitwisselingsparameters' naar bedrijfstak (2 of meer werkzame personen)



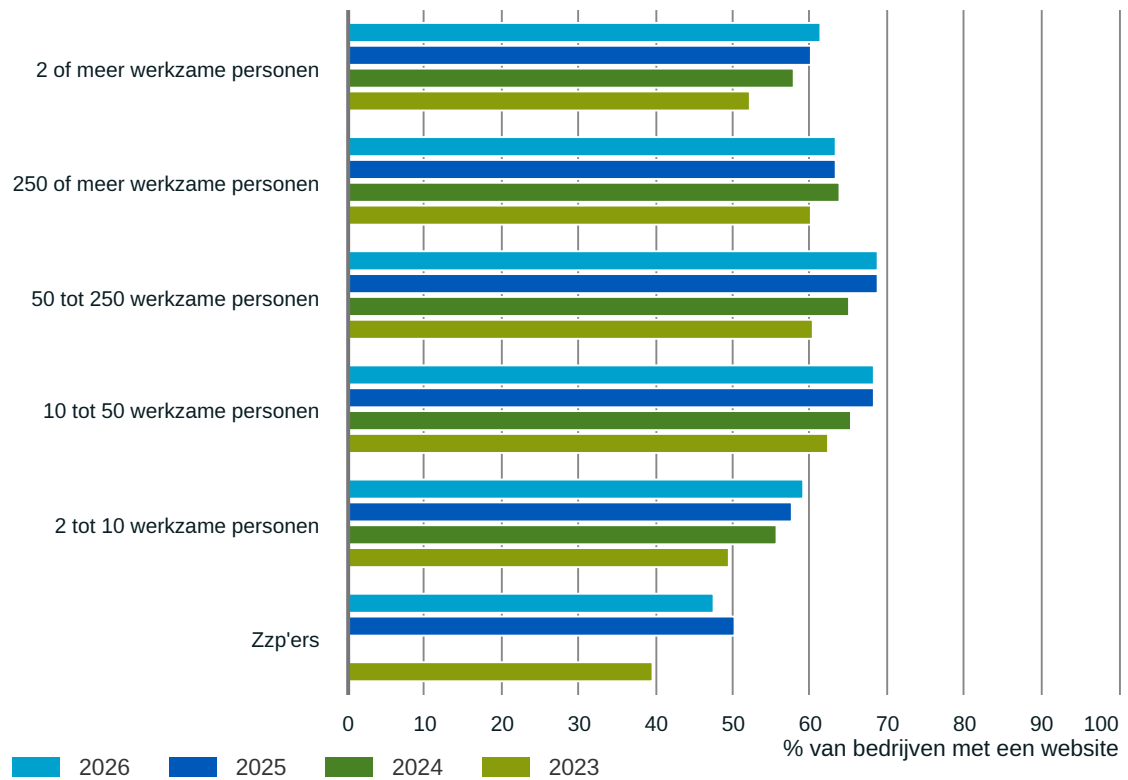
Figuur C.31.: Percentage van bedrijven met een website met geslaagde e-mailtest 'Hashfunctie voor sleuteluitwisseling' naar bedrijfsgrootteklasse



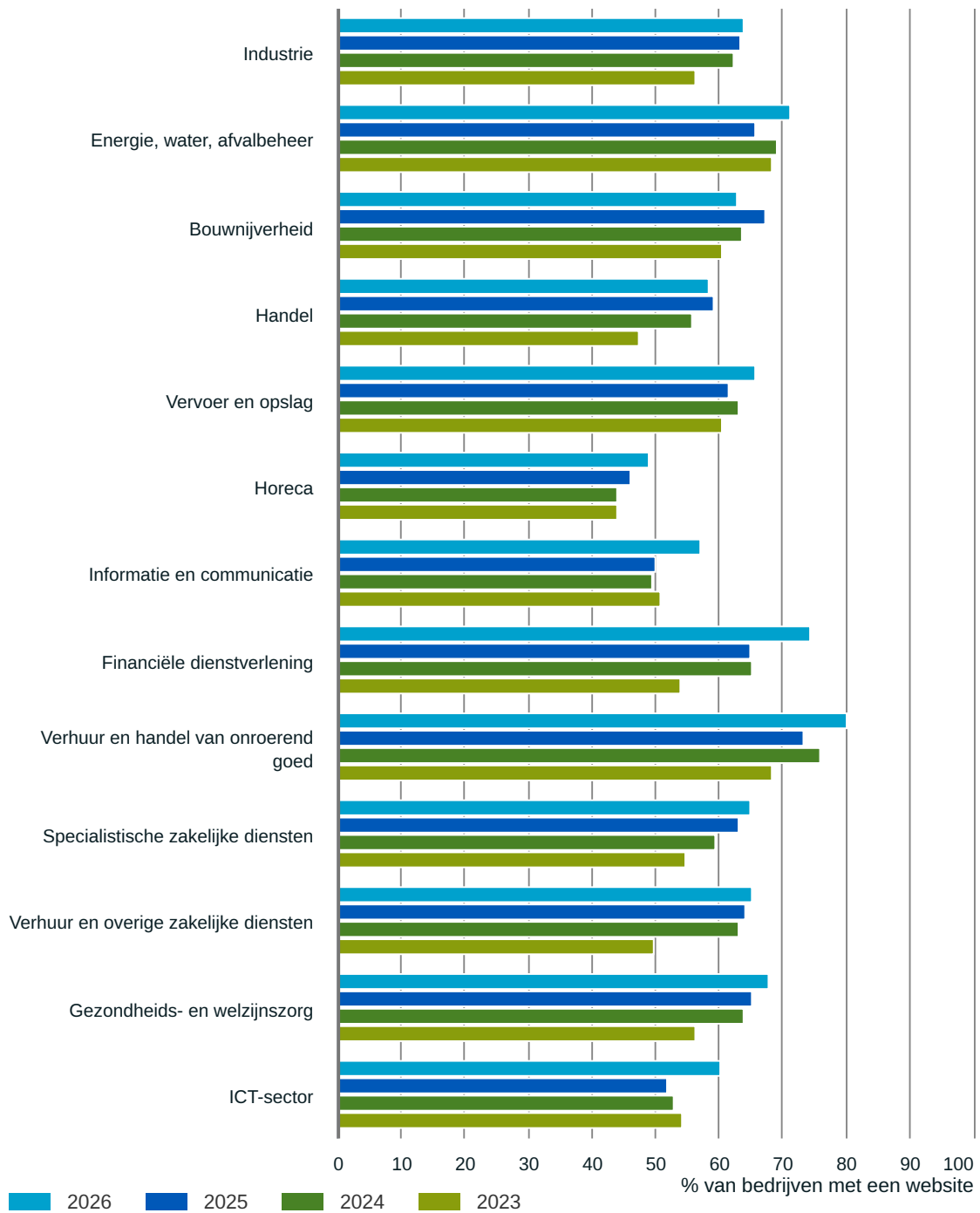
Figuur C.32.: Percentage van bedrijven met een website met geslaagde e-mailtest 'Hashfunctie voor sleuteluitwisseling' naar bedrijfstak (2 of meer werkzame personen)



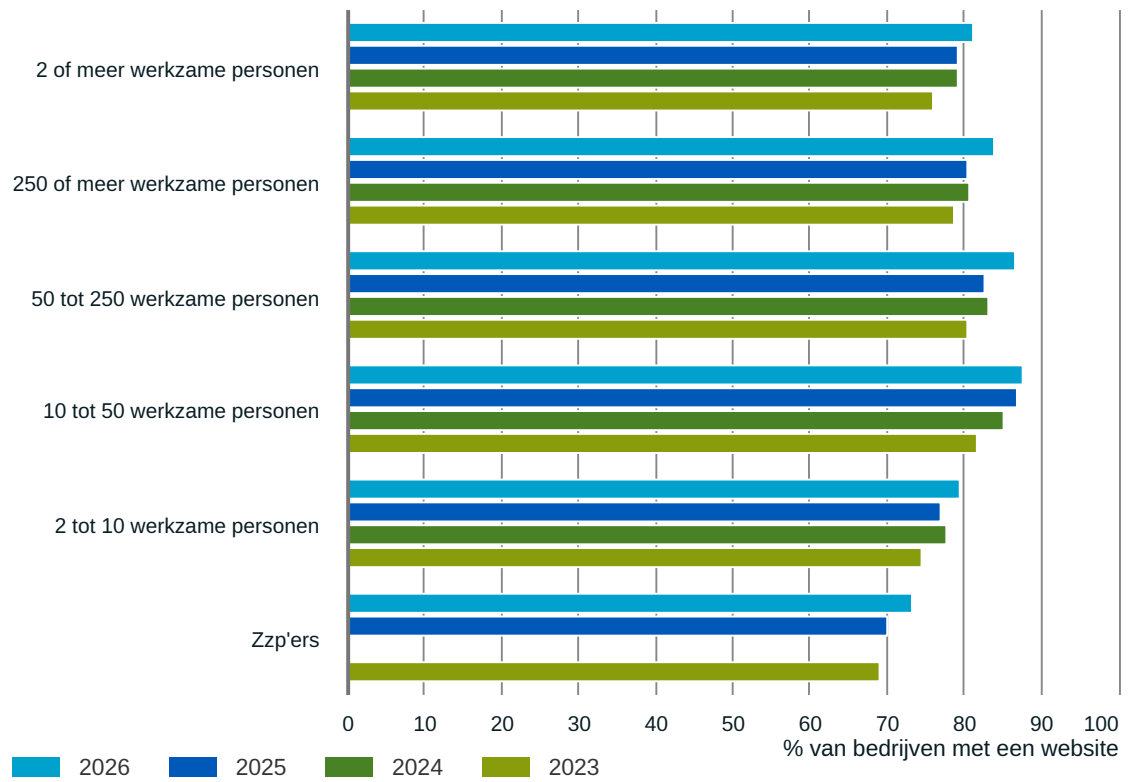
Figuur C.33.: Percentage van bedrijven met een website met geslaagde e-mailtest 'Ciphers (algoritmeselectie)' naar bedrijfsgrootteklasse



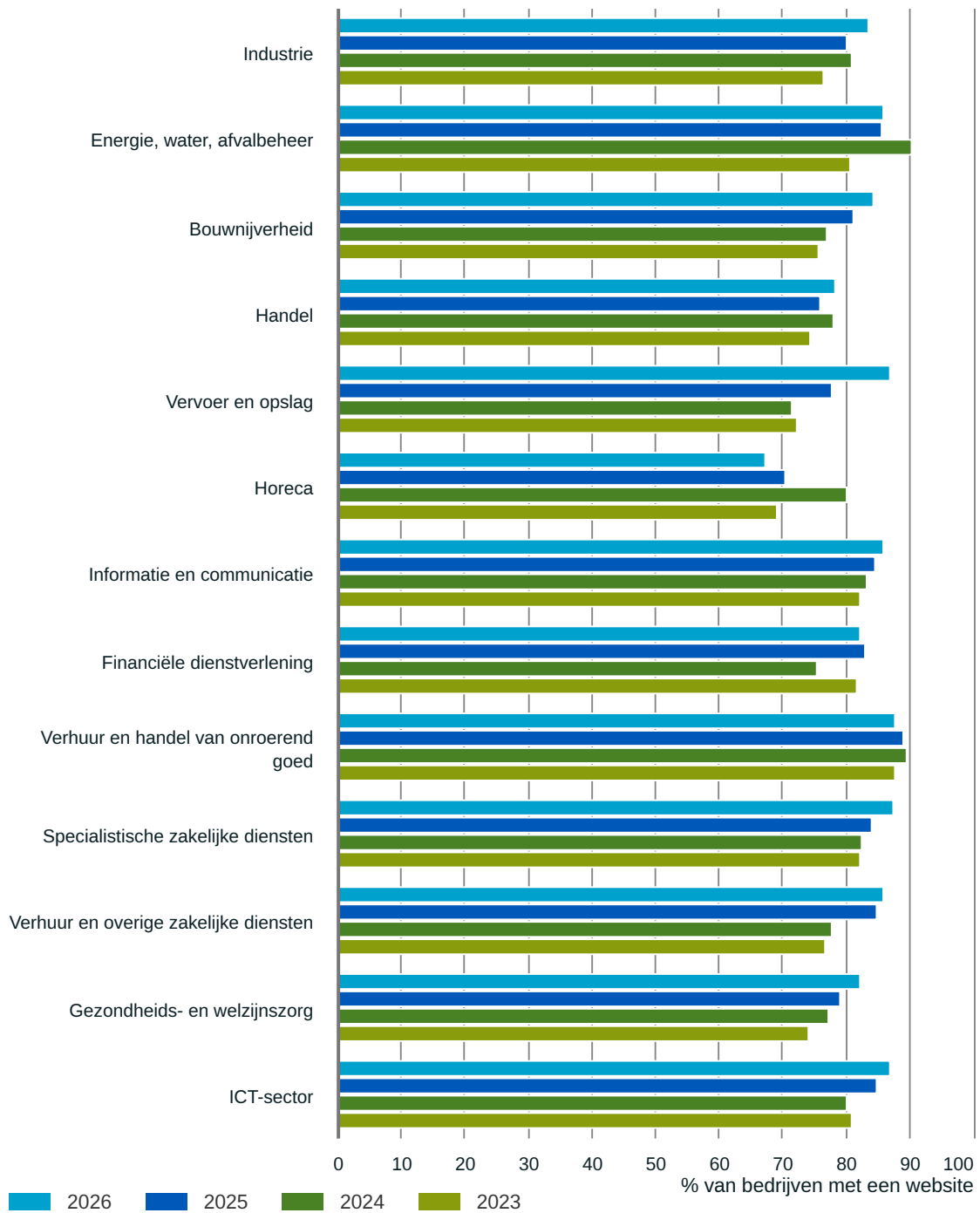
Figuur C.34.: Percentage van bedrijven met een website met geslaagde e-mailtest 'Ciphers (algoritme selectie)' naar bedrijfstak (2 of meer werkzame personen)



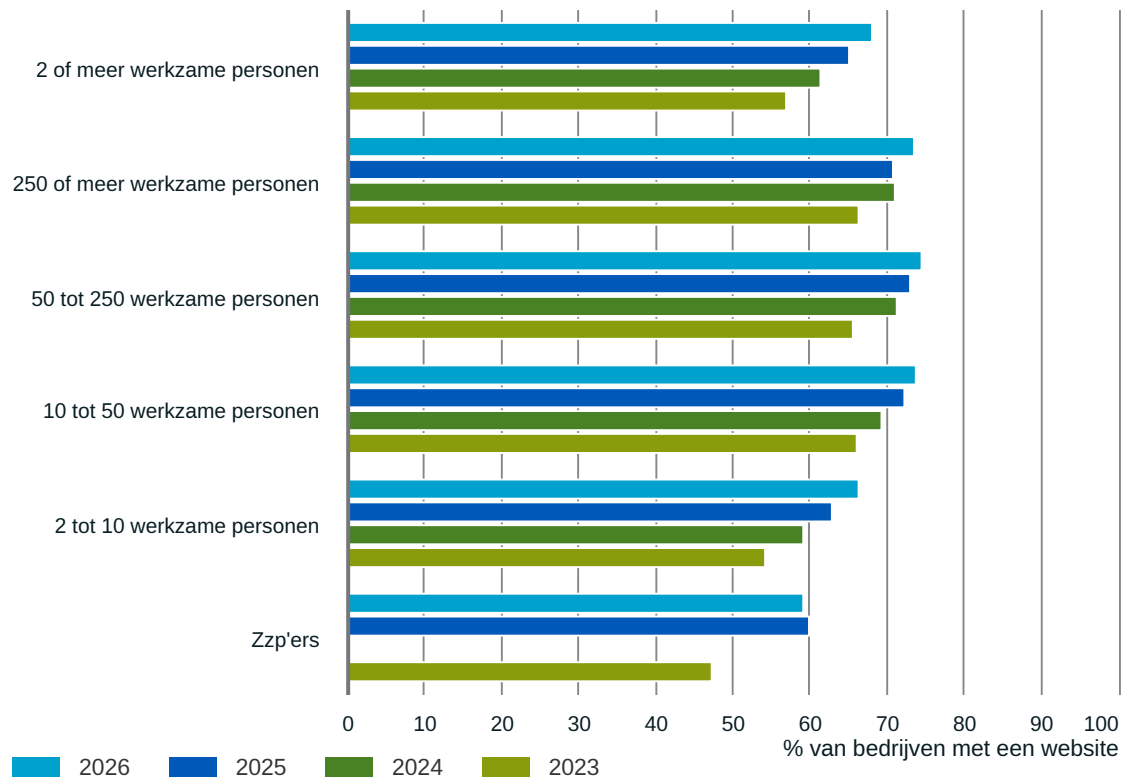
Figuur C.35.: Percentage van bedrijven met een website met geslaagde e-mailtest 'Cijfer-  
volgorde' naar bedrijfsgrootteklasse



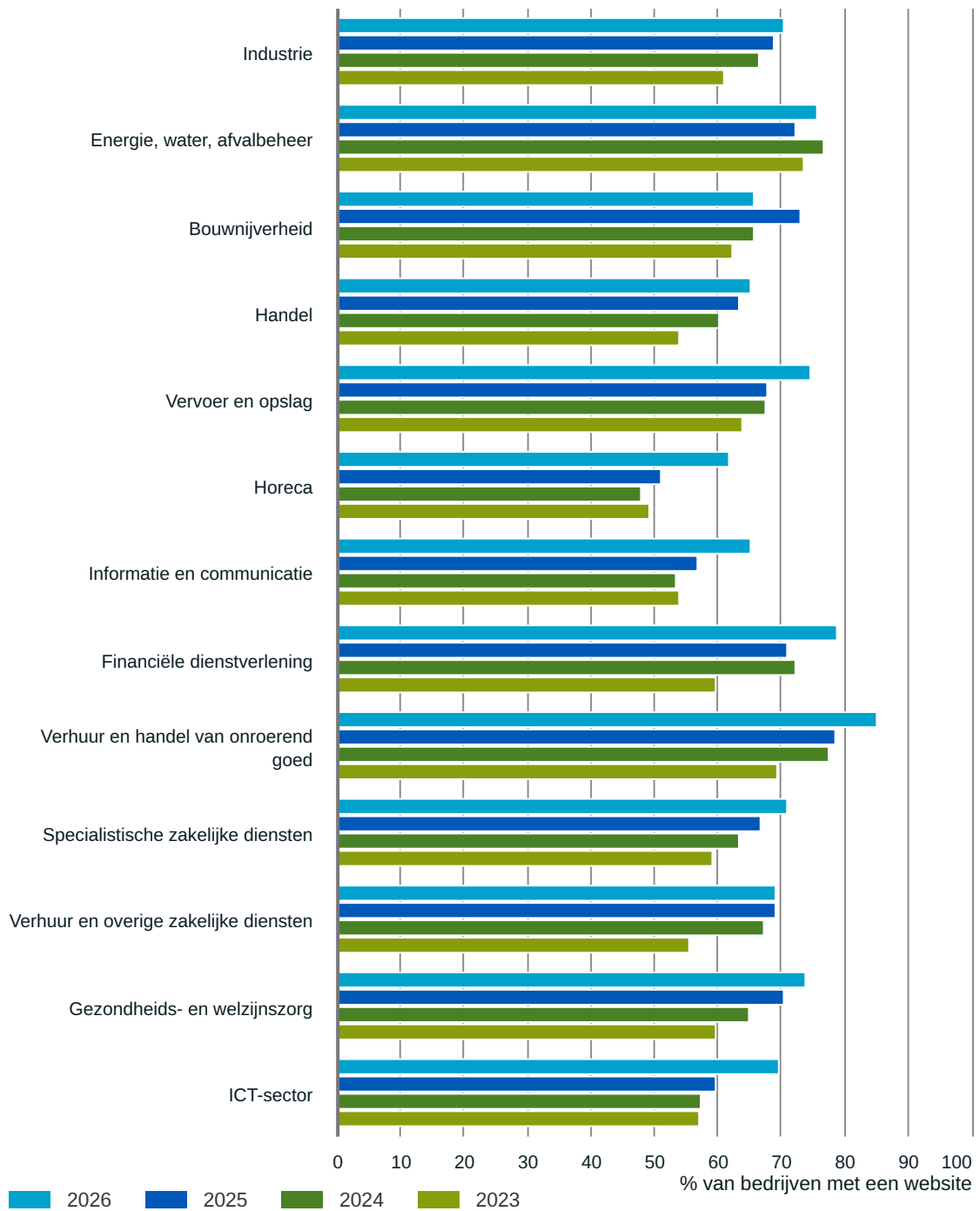
Figuur C.36.: Percentage van bedrijven met een website met geslaagde e-mailtest 'Cijfervolgorde' naar bedrijfstak (2 of meer werkzame personen)



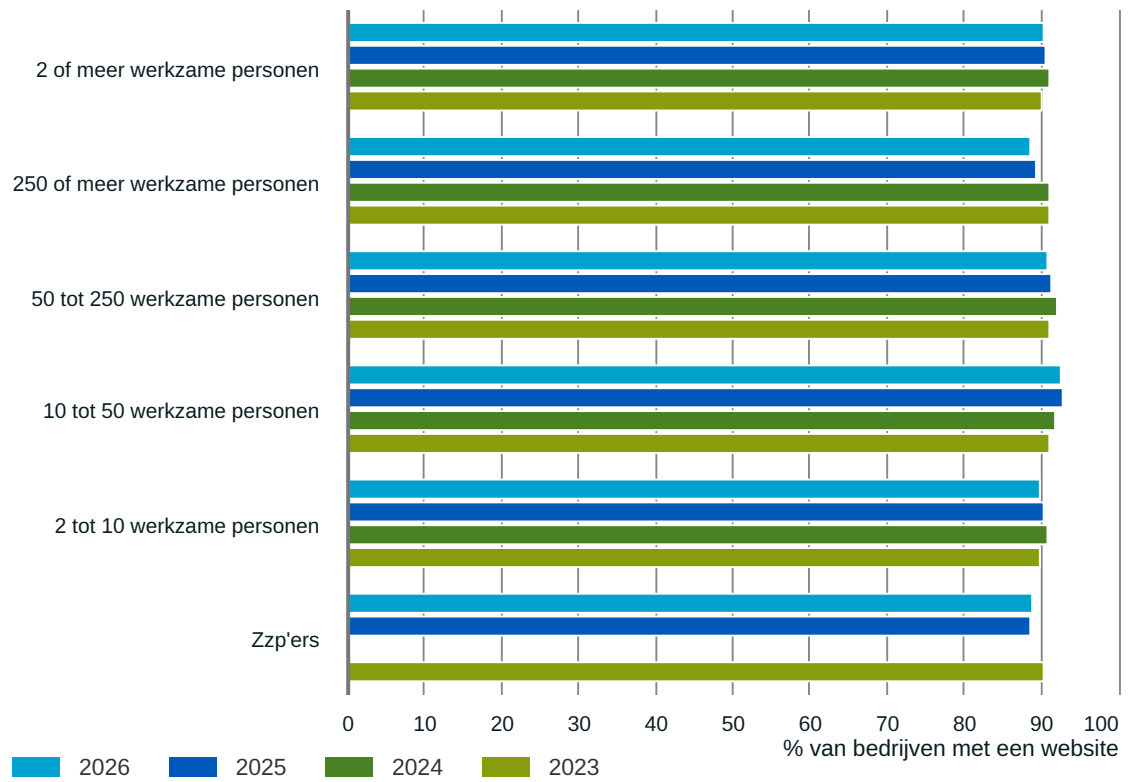
Figuur C.37.: Percentage van bedrijven met een website met geslaagde e-mailtest 'TLS-versie' naar bedrijfsgrootteklasse



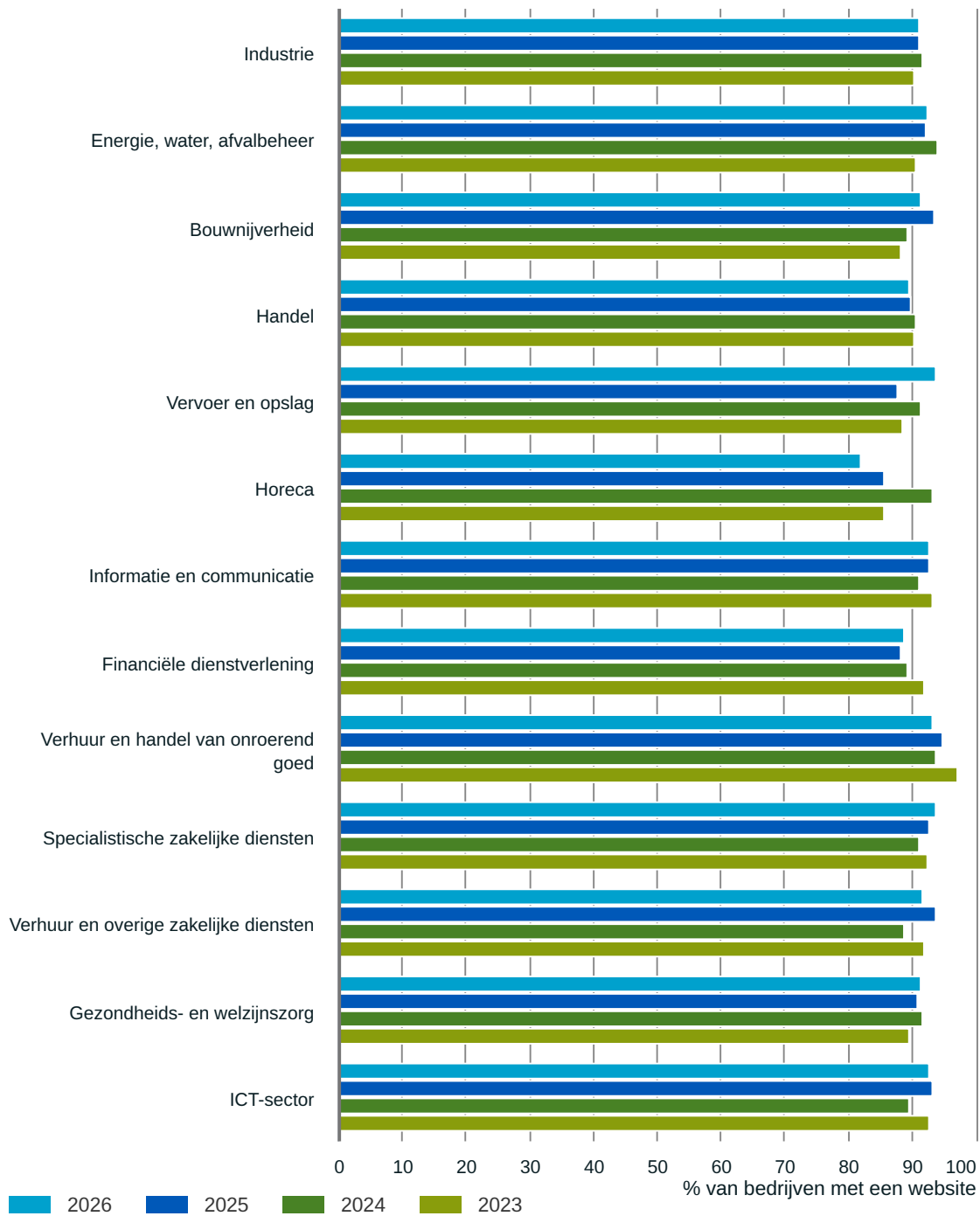
Figuur C.38.: Percentage van bedrijven met een website met geslaagde e-mailtest 'TLS-versie' naar bedrijfstak (2 of meer werkzame personen)



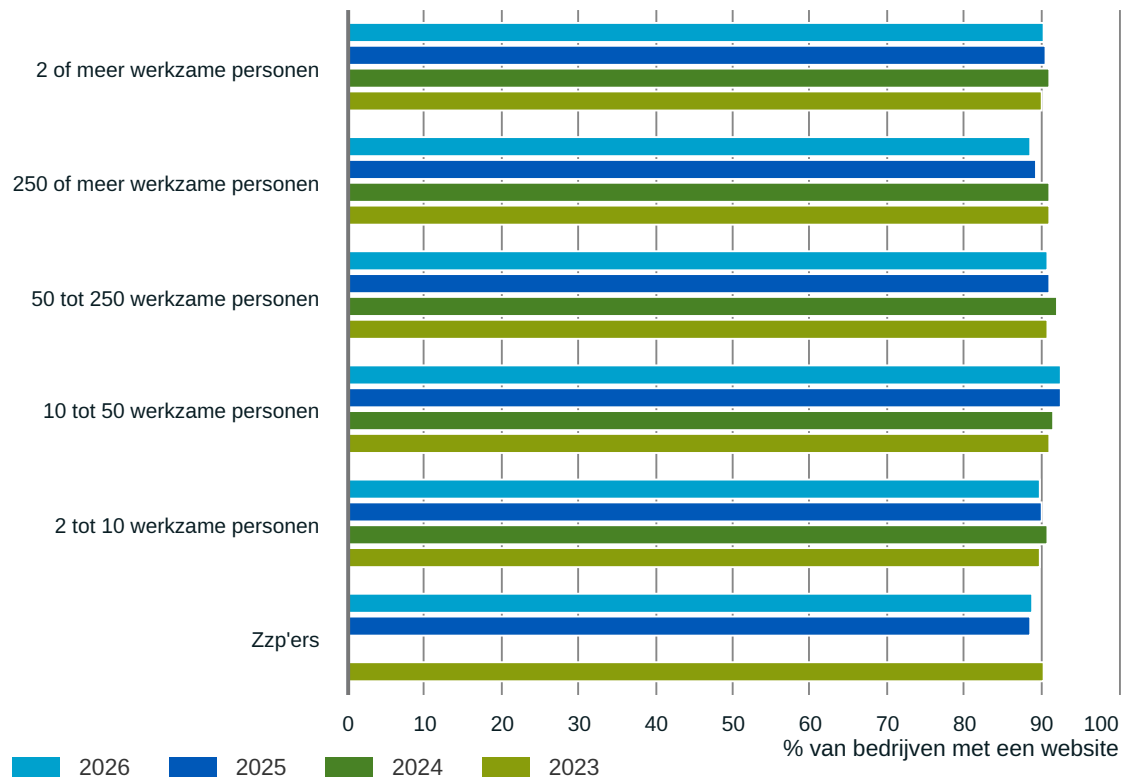
Figuur C.39.: Percentage van bedrijven met een website met geslaagde e-mailtest 'TLS-compressie' naar bedrijfsgrootteklasse



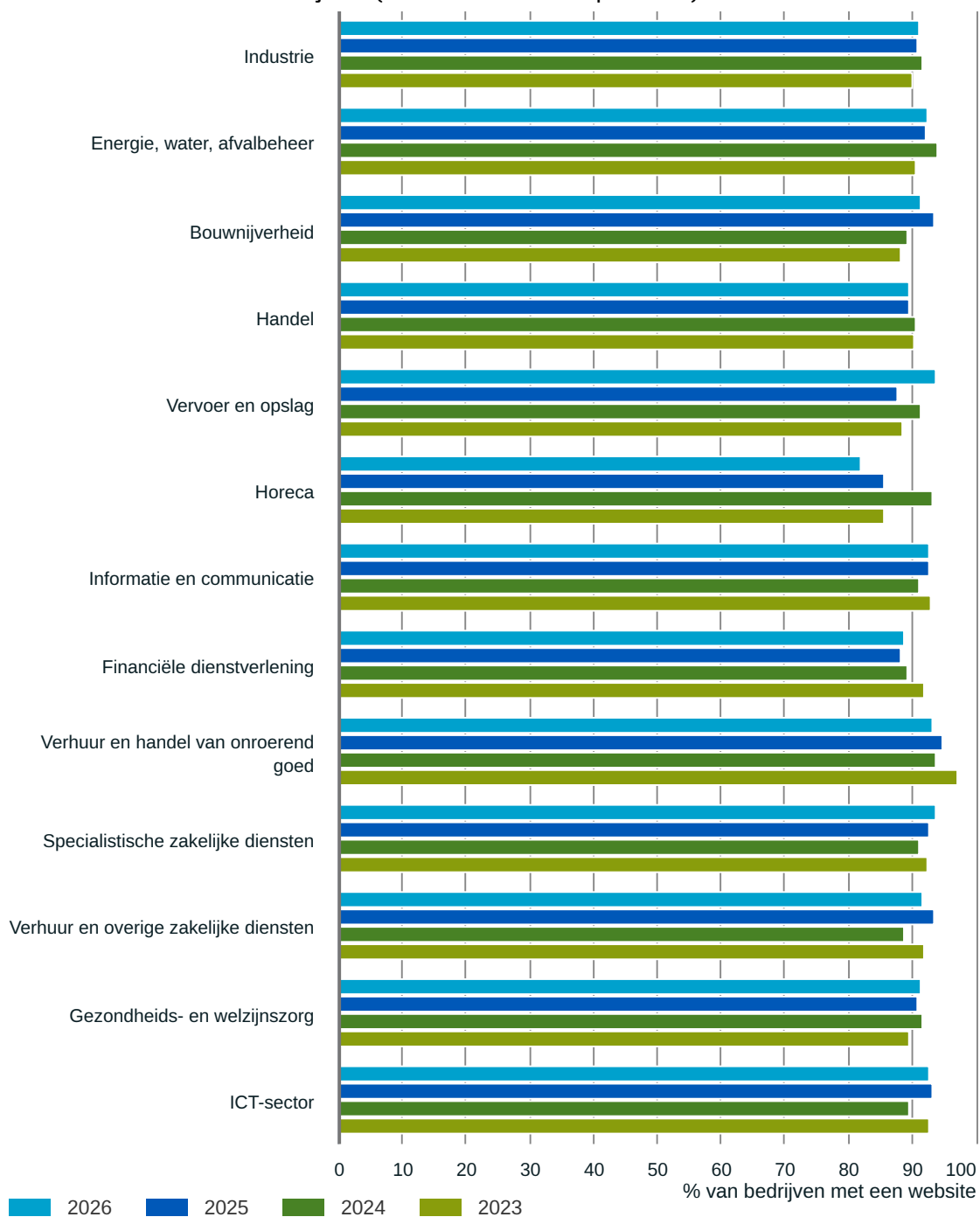
Figuur C.40.: Percentage van bedrijven met een website met geslaagde e-mailtest 'TLS-compressie' naar bedrijfstak (2 of meer werkzame personen)



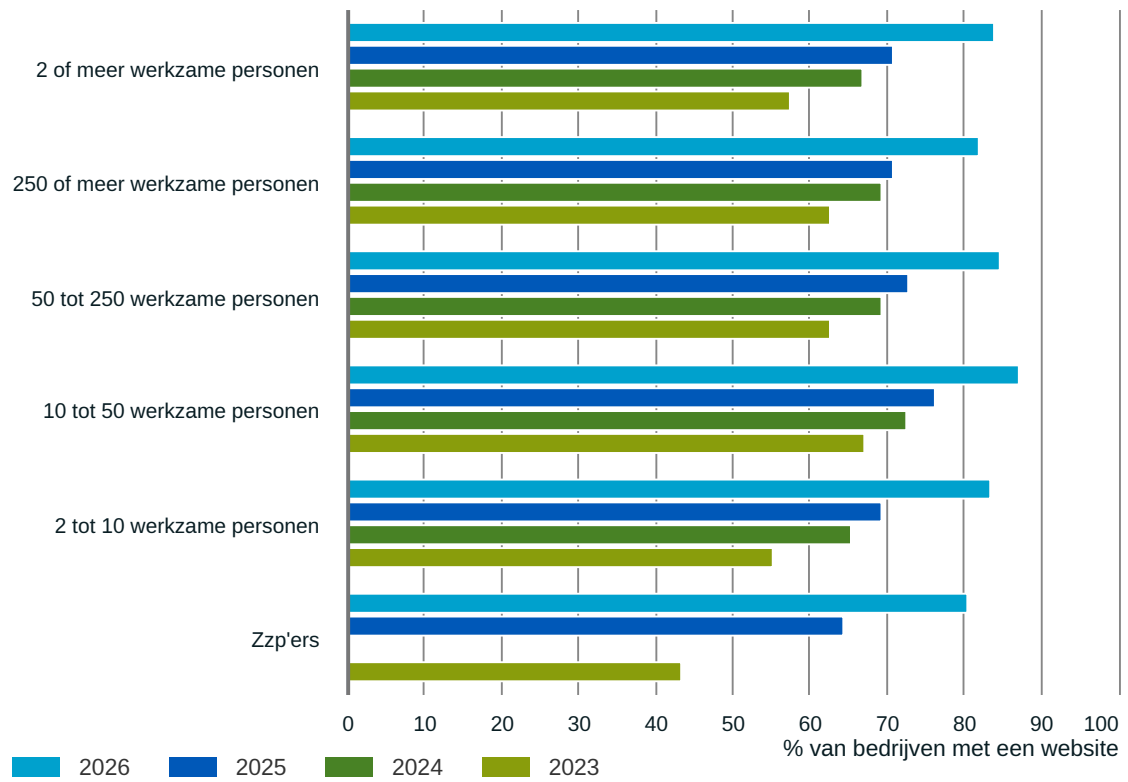
Figuur C.41.: Percentage van bedrijven met een website met geslaagde e-mailtest 'Secure renegotiation' naar bedrijfsgrootteklasse



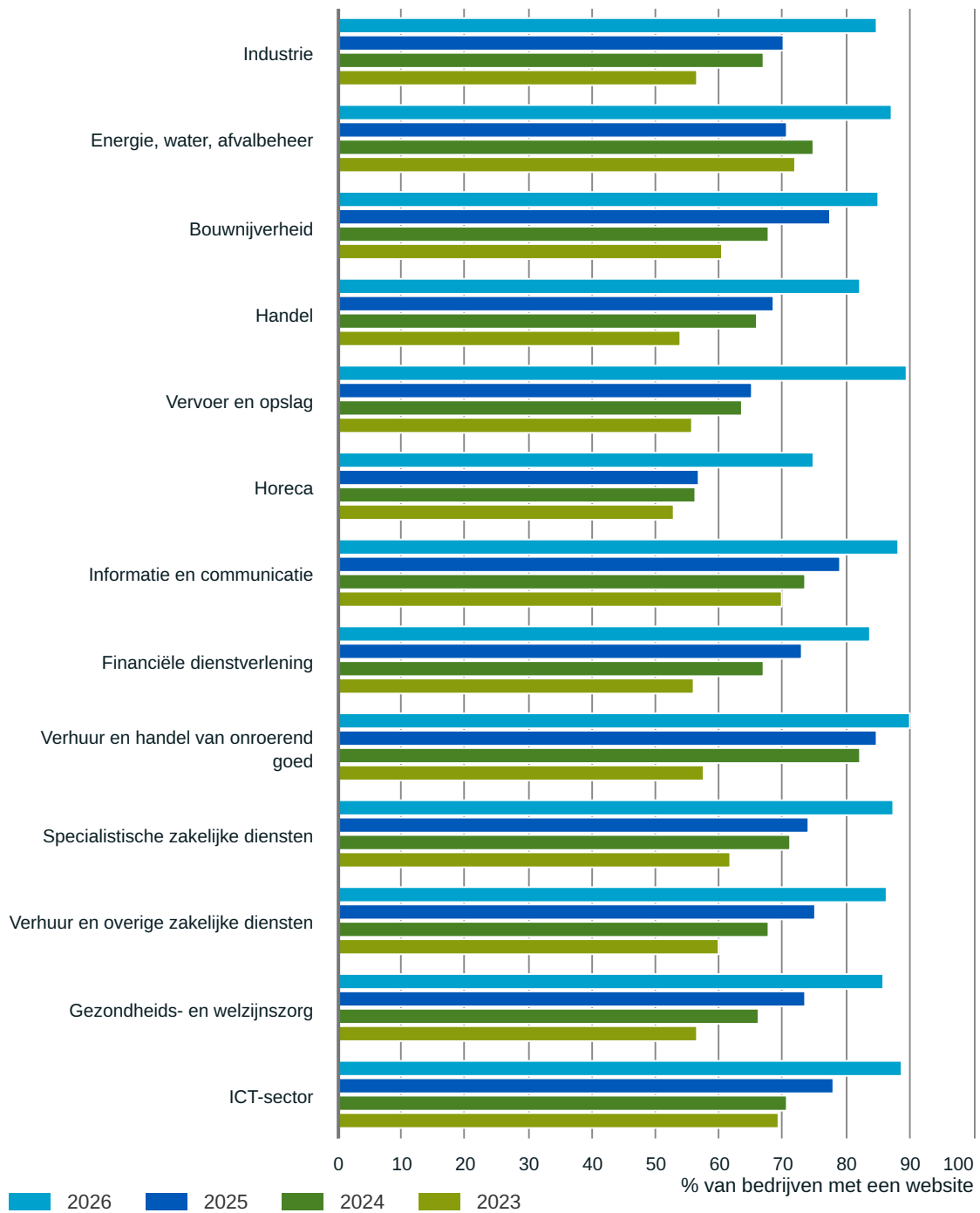
Figuur C.42.: Percentage van bedrijven met een website met geslaagde e-mailtest 'Secure renegotiation' naar bedrijfstak (2 of meer werkzame personen)



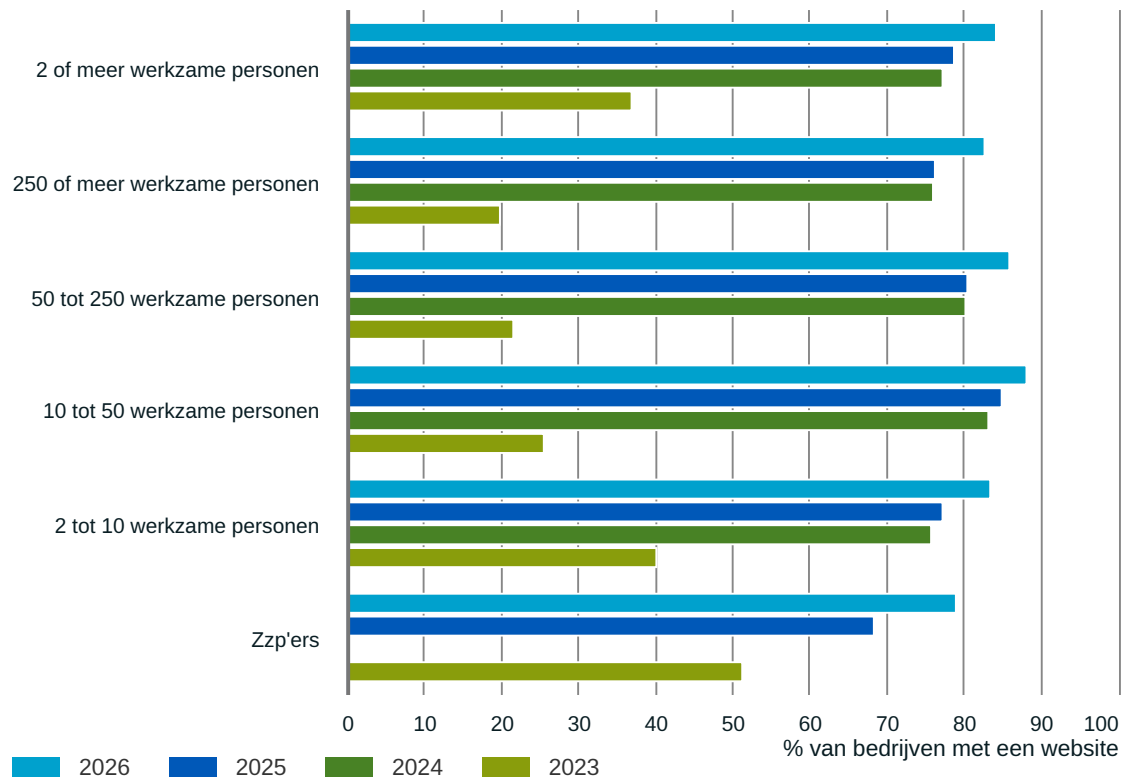
Figuur C.43.: Percentage van bedrijven met een website met geslaagde e-mailtest 'Client-initiated renegotiation' naar bedrijfsgrootteklasse



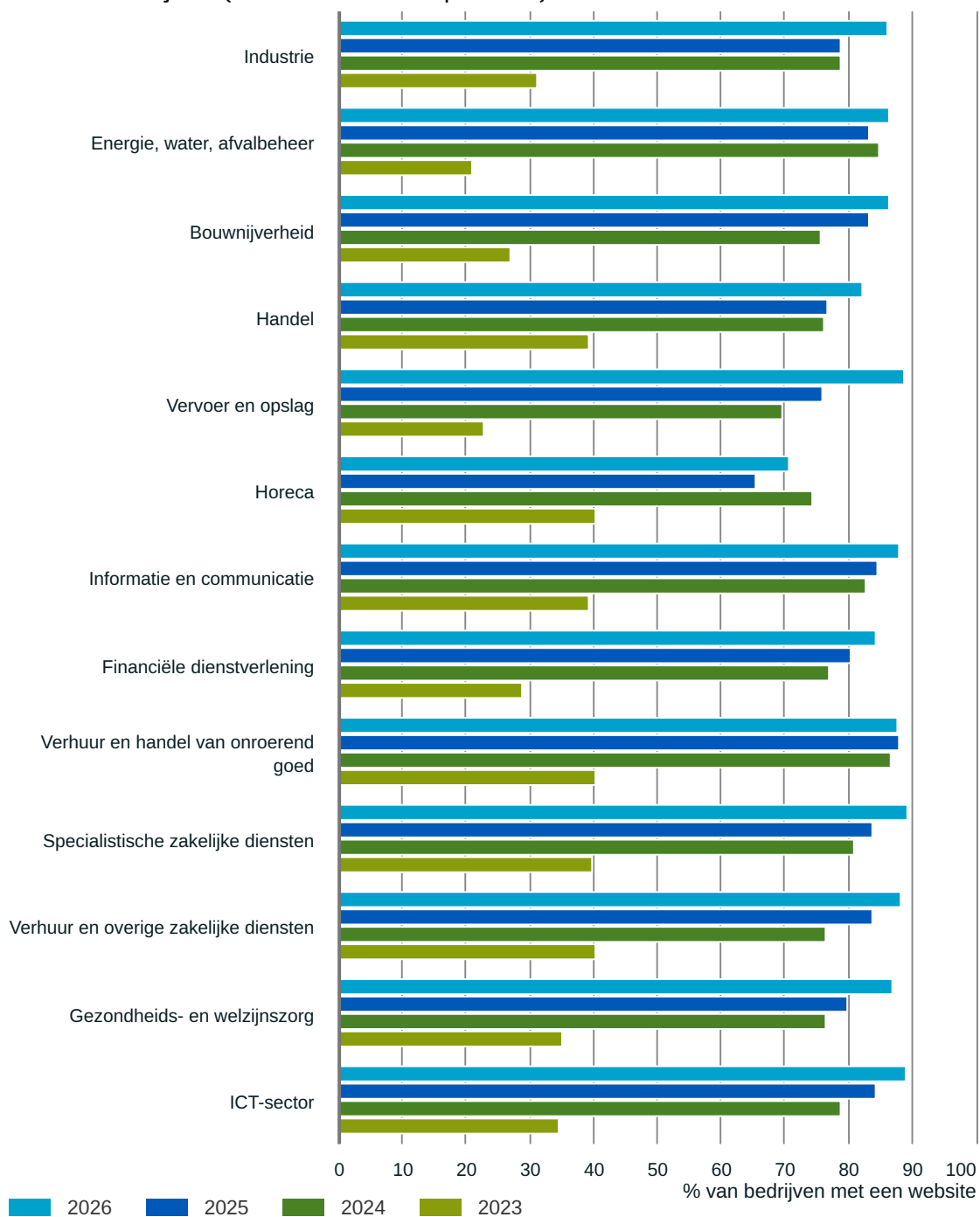
Figuur C.44.: Percentage van bedrijven met een website met geslaagde e-mailtest 'Client-initiated renegotiation' naar bedrijfstak (2 of meer werkzame personen)



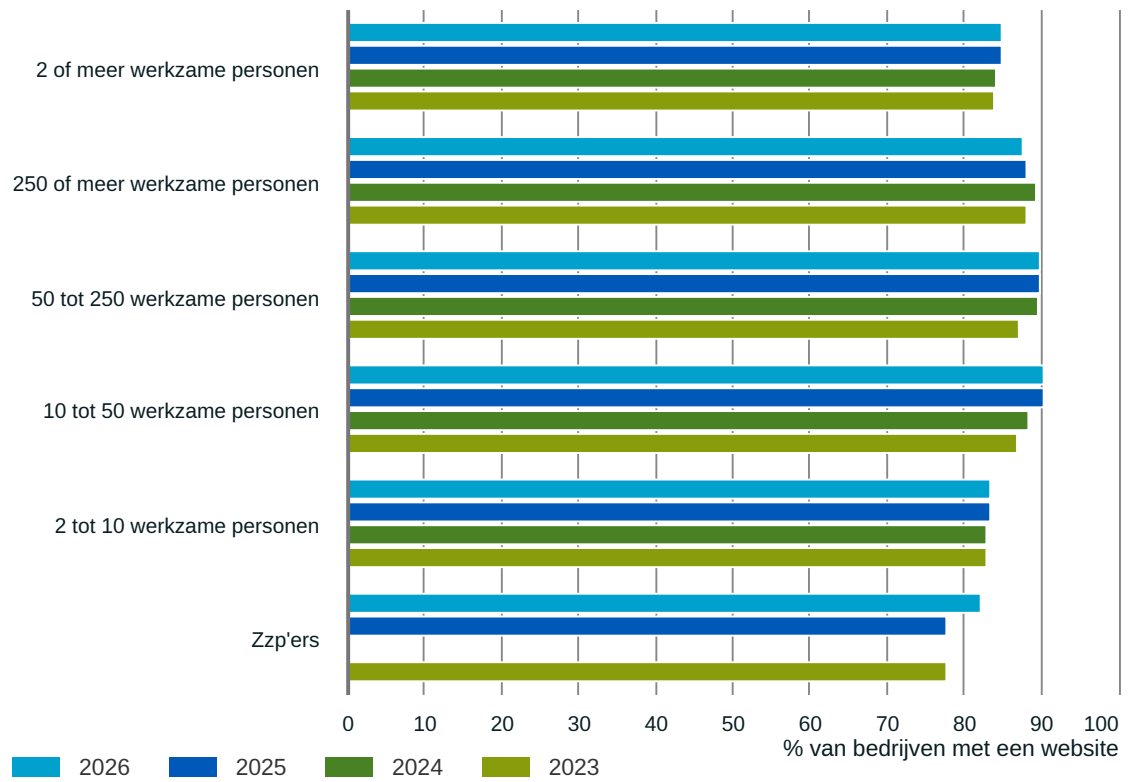
Figuur C.45.: Percentage van bedrijven met een website met geslaagde e-mailtest '0-RTT' naar bedrijfsgrootteklasse



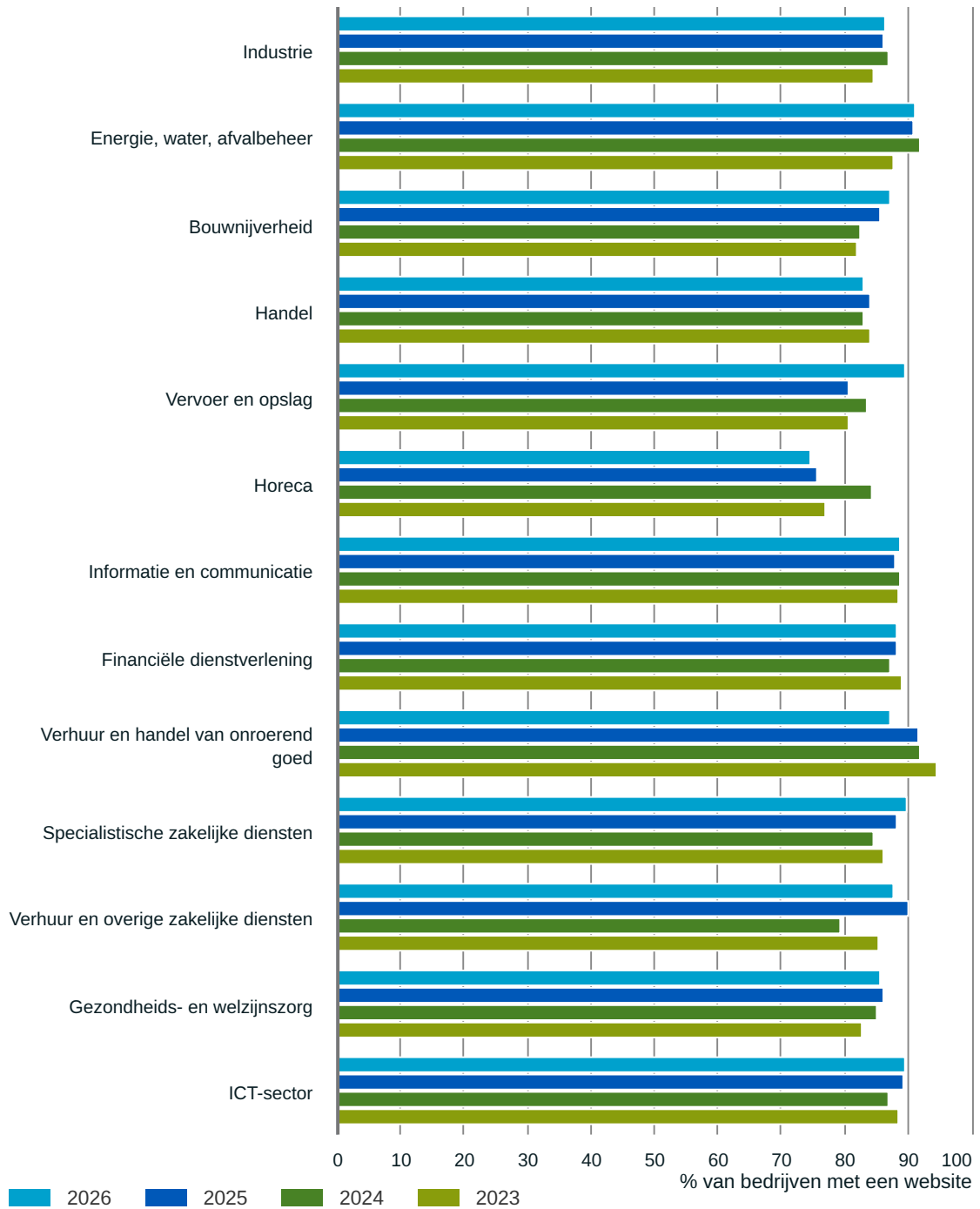
Figuur C.46.: Percentage van bedrijven met een website met geslaagde e-mailtest '0-RTT' naar bedrijfstak (2 of meer werkzame personen)



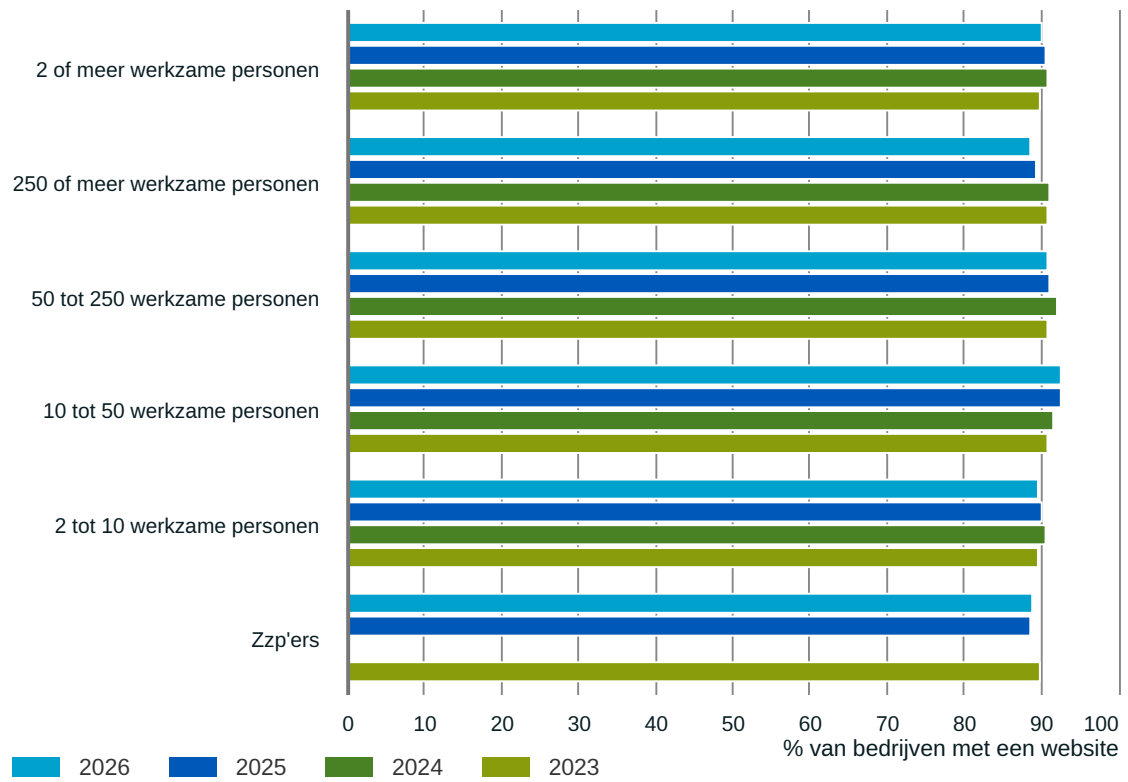
Figuur C.47.: Percentage van bedrijven met een website met geslaagde e-mailtest 'Vertrouwensketen van certificaat' naar bedrijfsgrootteklasse



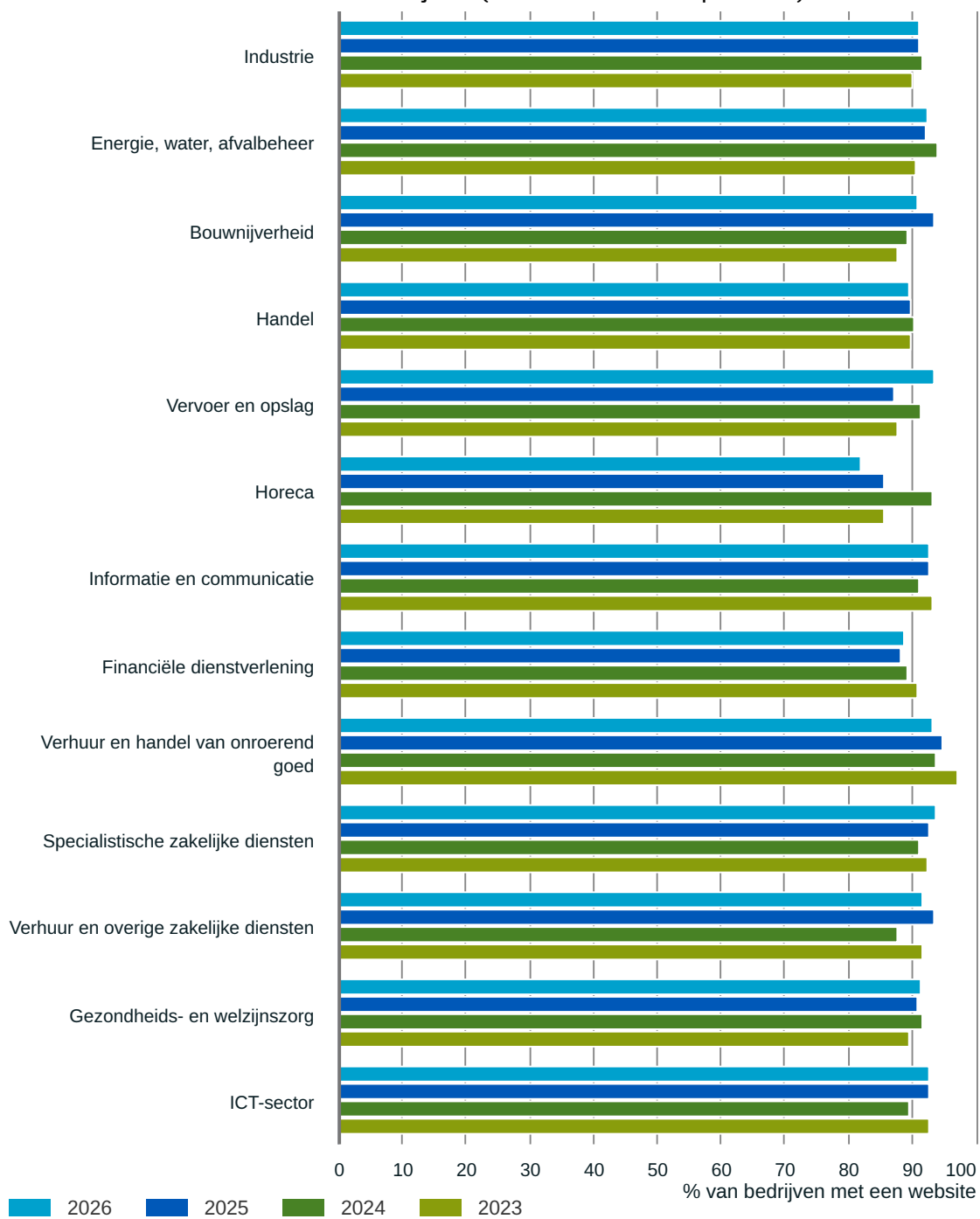
Figuur C.48.: Percentage van bedrijven met een website met geslaagde e-mailtest 'Vertrouwensketen van certificaat' naar bedrijfstak (2 of meer werkzame personen)



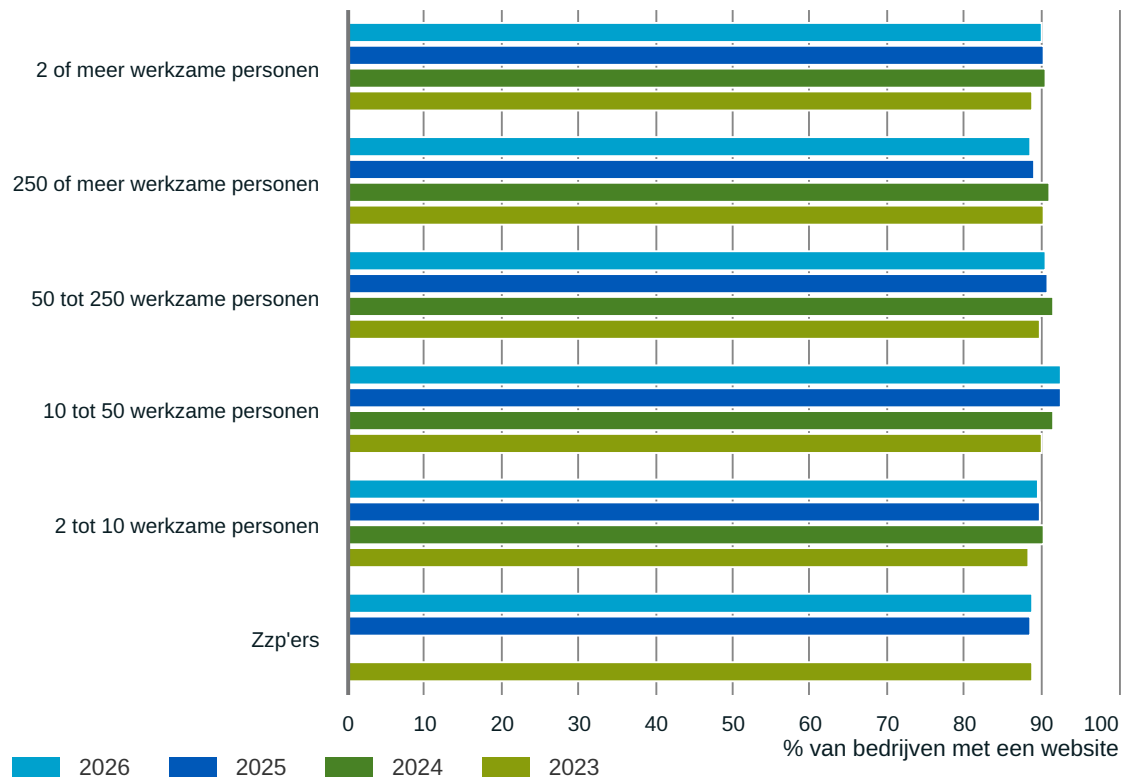
Figuur C.49.: Percentage van bedrijven met een website met geslaagde e-mailtest 'Publieke sleutel van certificaat' naar bedrijfsgrootteklasse



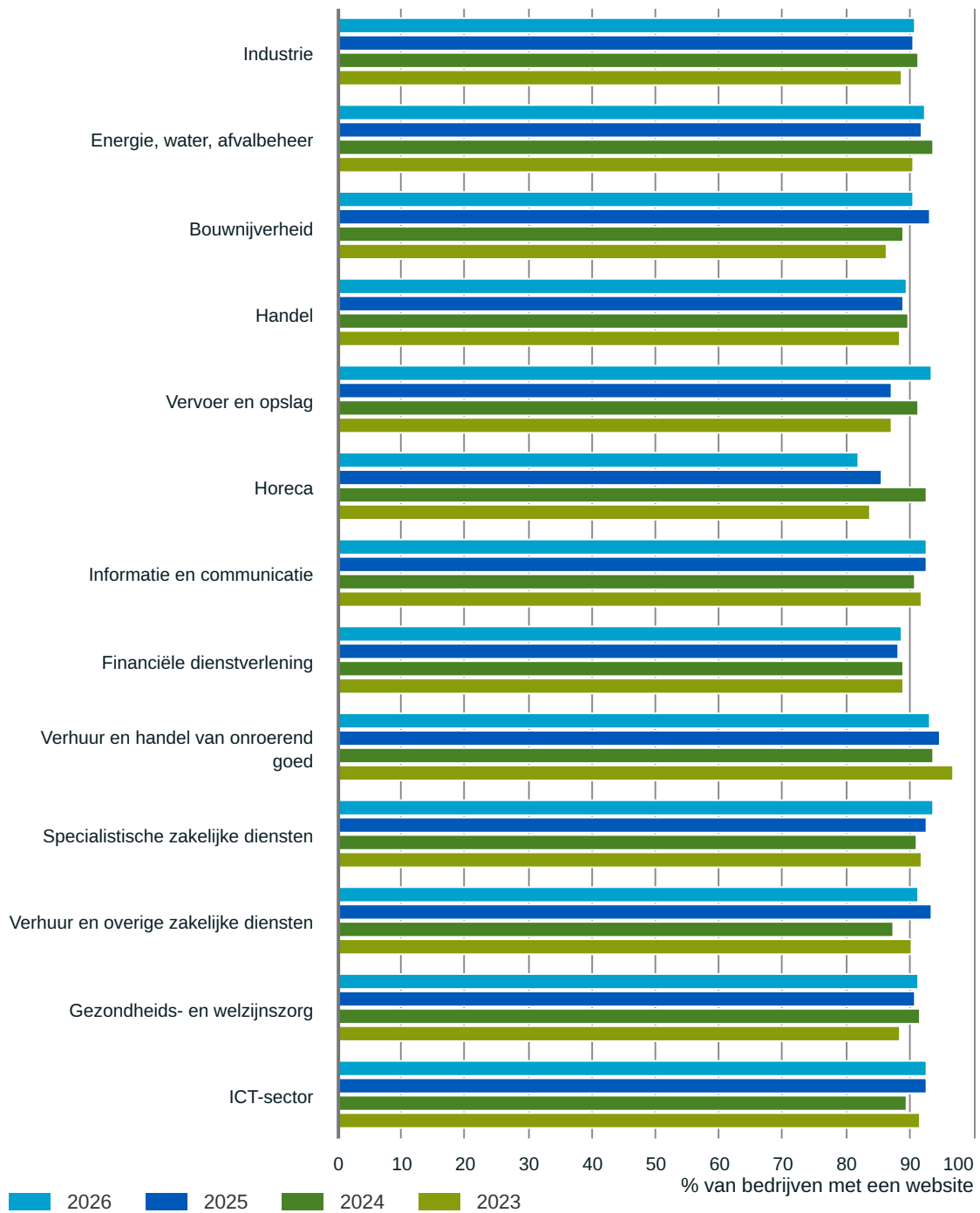
Figuur C.50.: Percentage van bedrijven met een website met geslaagde e-mailtest 'Publieke sleutel van certificaat' naar bedrijfstak (2 of meer werkzame personen)



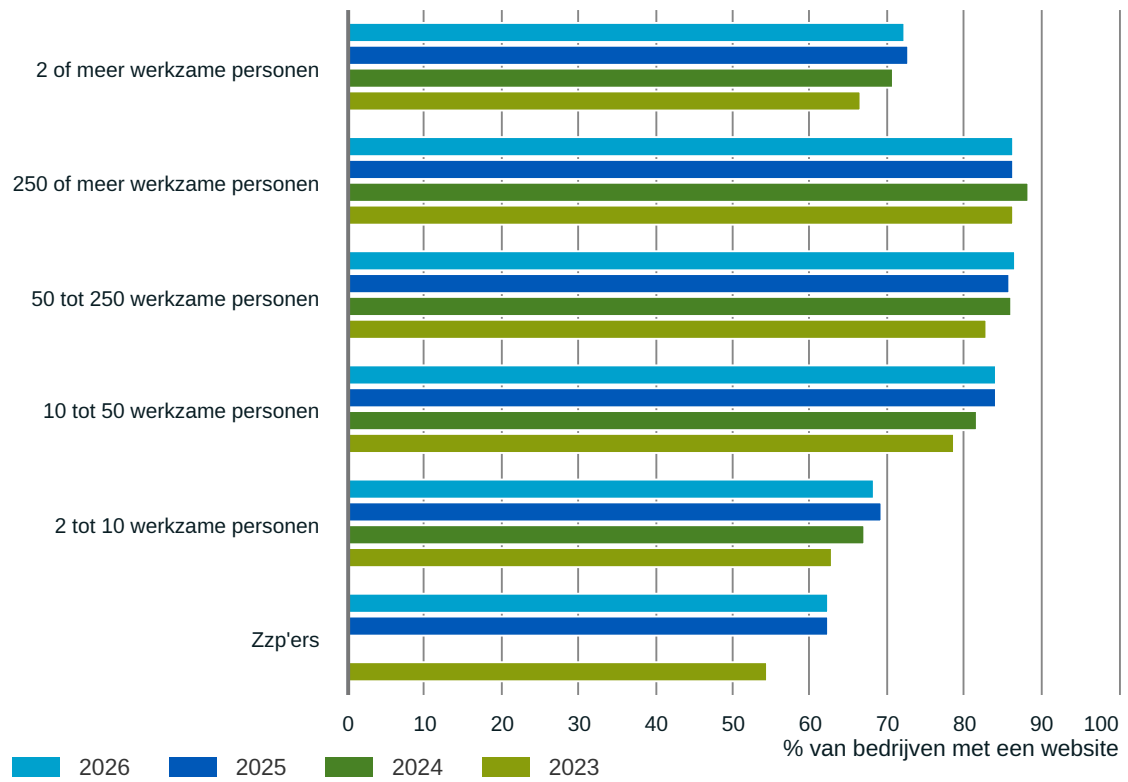
Figuur C.51.: Percentage van bedrijven met een website met geslaagde e-mailtest 'Handtekening van certificaat' naar bedrijfsgrootteklasse



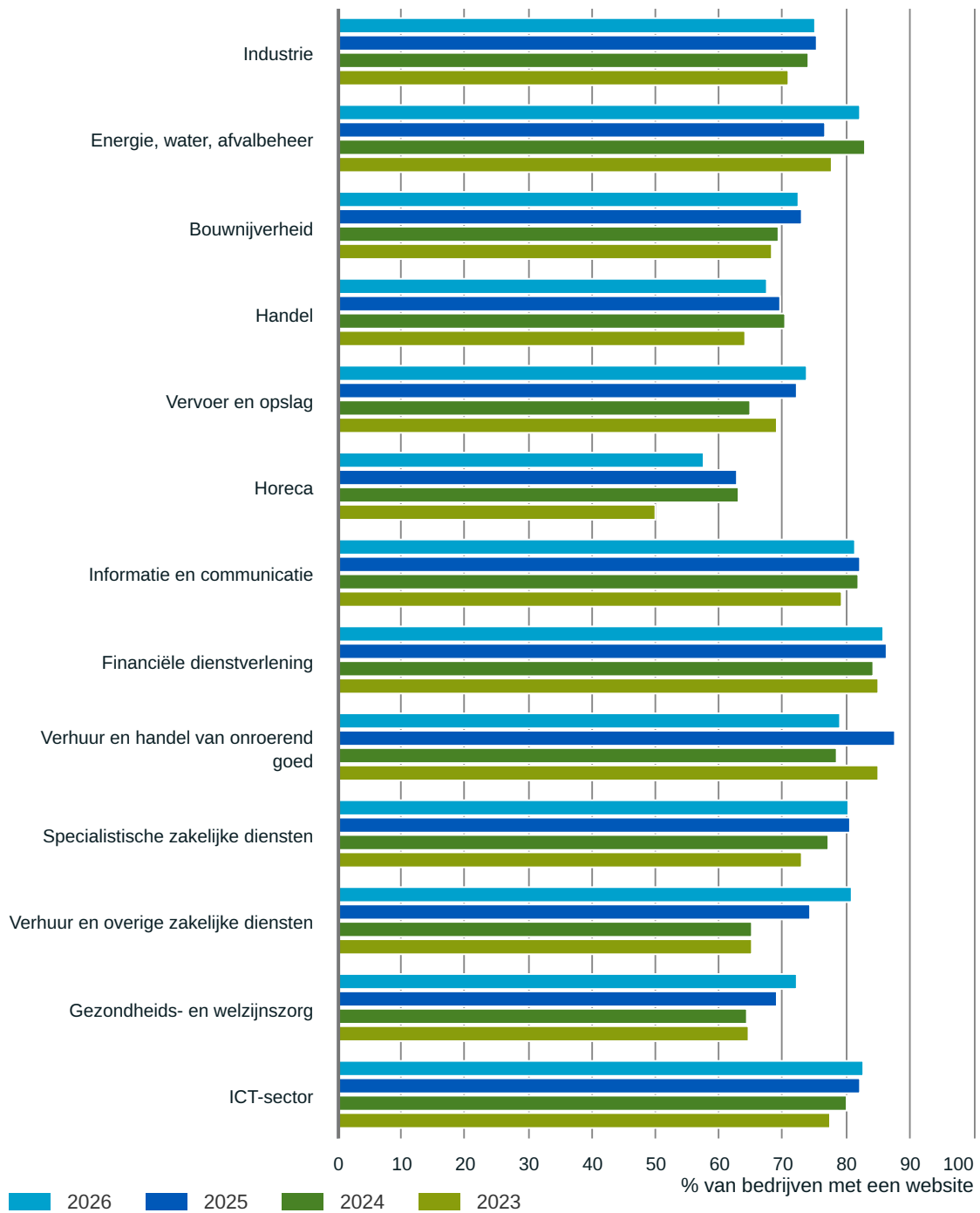
Figuur C.52.: Percentage van bedrijven met een website met geslaagde e-mailtest 'Handtekening van certificaat' naar bedrijfstak (2 of meer werkzame personen)



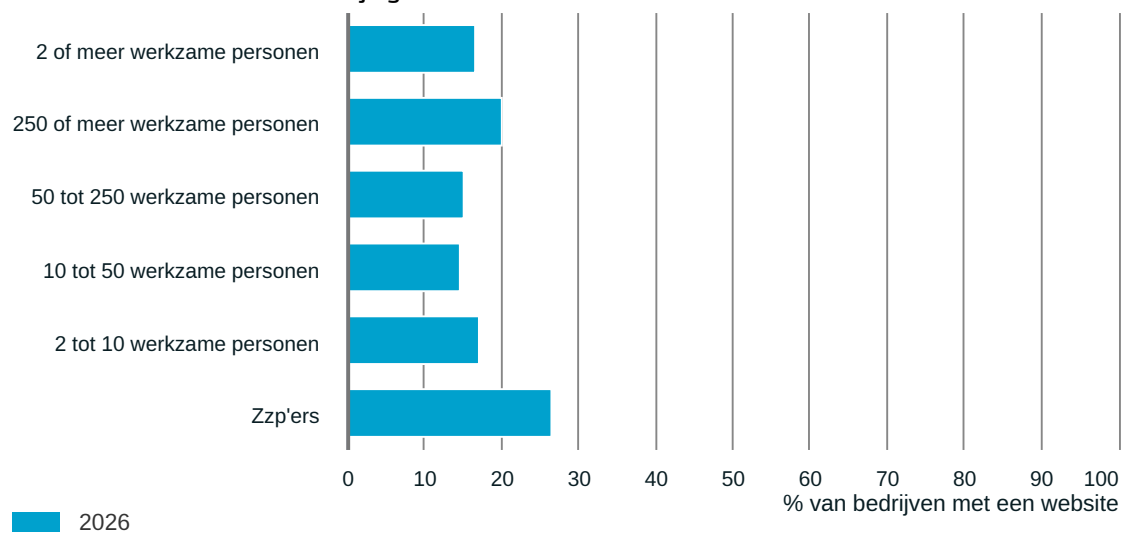
Figuur C.53.: Percentage van bedrijven met een website met geslaagde e-mailtest 'Domeinnaam op certificaat' naar bedrijfsgrootteklasse



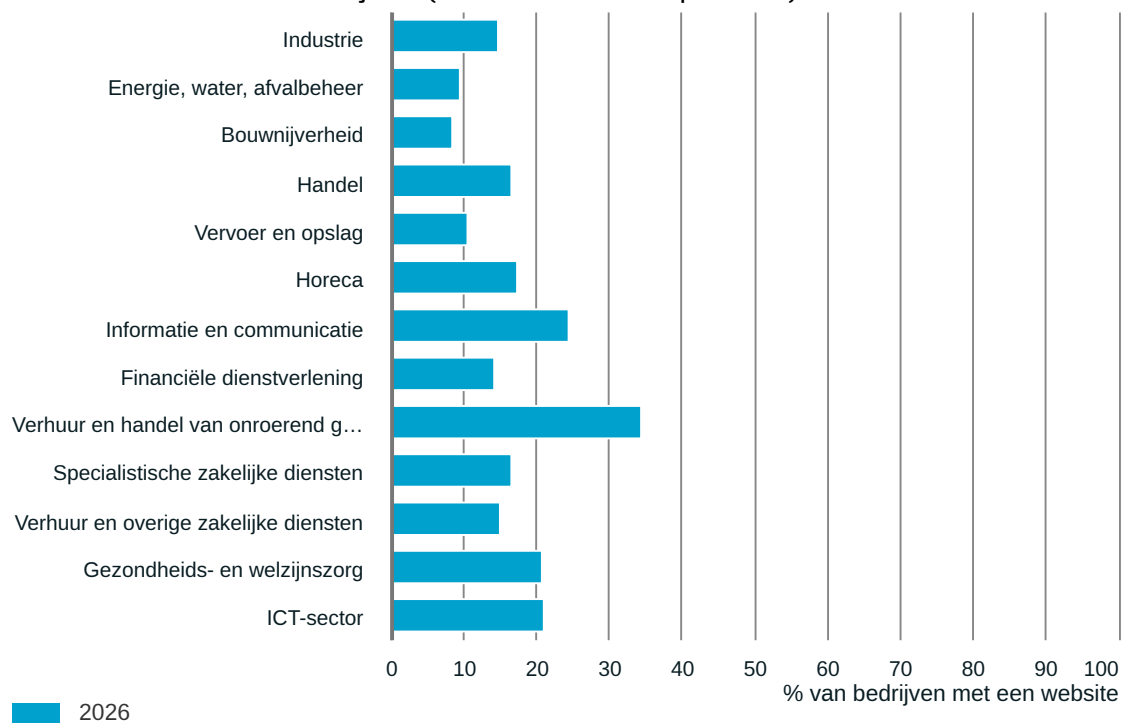
Figuur C.54.: Percentage van bedrijven met een website met geslaagde e-mailtest 'Domeinnaam op certificaat' naar bedrijfstak (2 of meer werkzame personen)



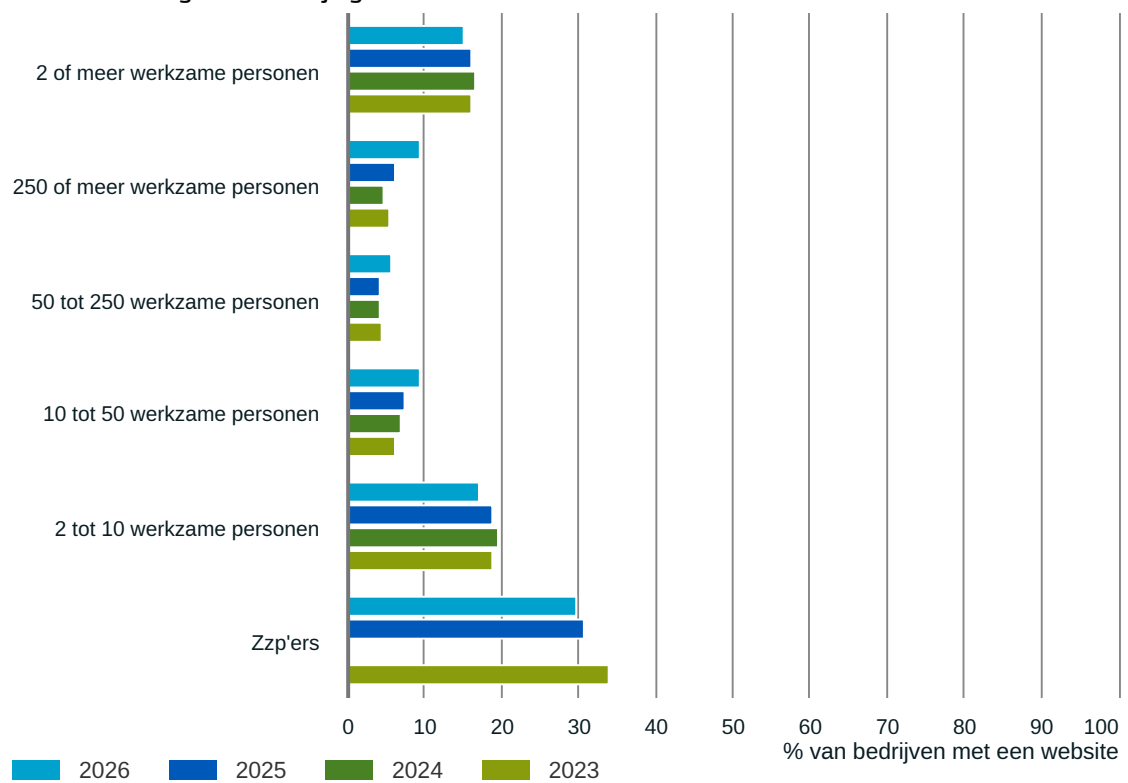
Figuur C.55.: Percentage van bedrijven met een website met geslaagde e-mailtest 'CAA voor mail-server' naar bedrijfsgrootteklasse



Figuur C.56.: Percentage van bedrijven met een website met geslaagde e-mailtest 'CAA voor mail-server' naar bedrijfstak (2 of meer werkzame personen)



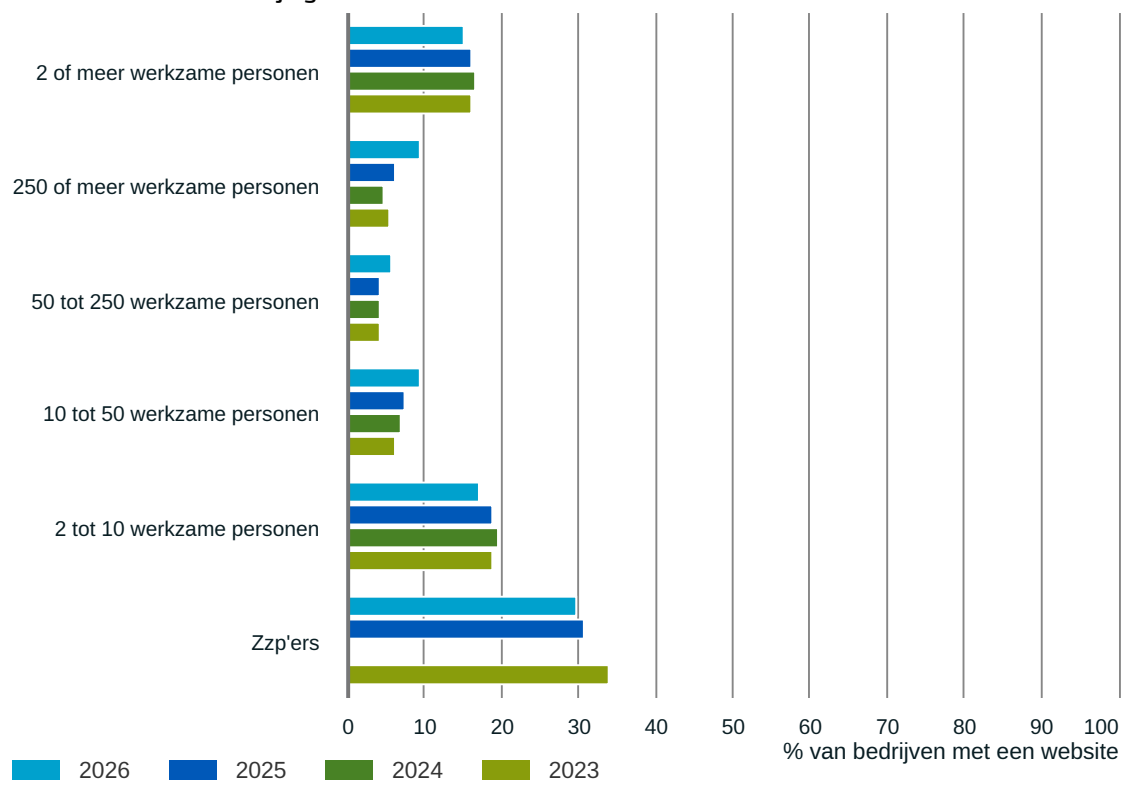
Figuur C.57.: Percentage van bedrijven met een website met geslaagde e-mailtest 'DANE aanwezig' naar bedrijfsgrootteklasse



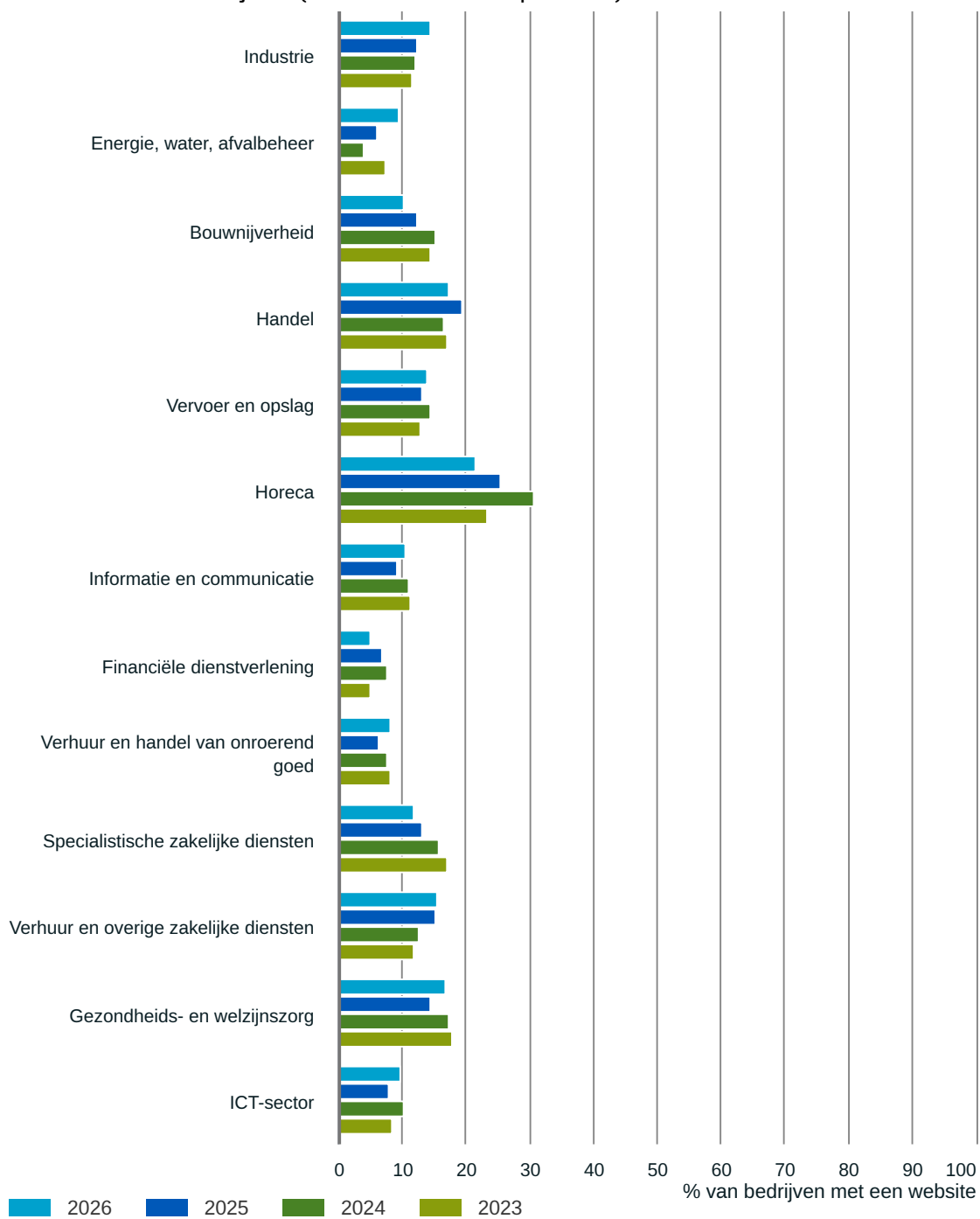
Figuur C.58.: Percentage van bedrijven met een website met geslaagde e-mailtest 'DANE aanwezig' naar bedrijfstak (2 of meer werkzame personen)



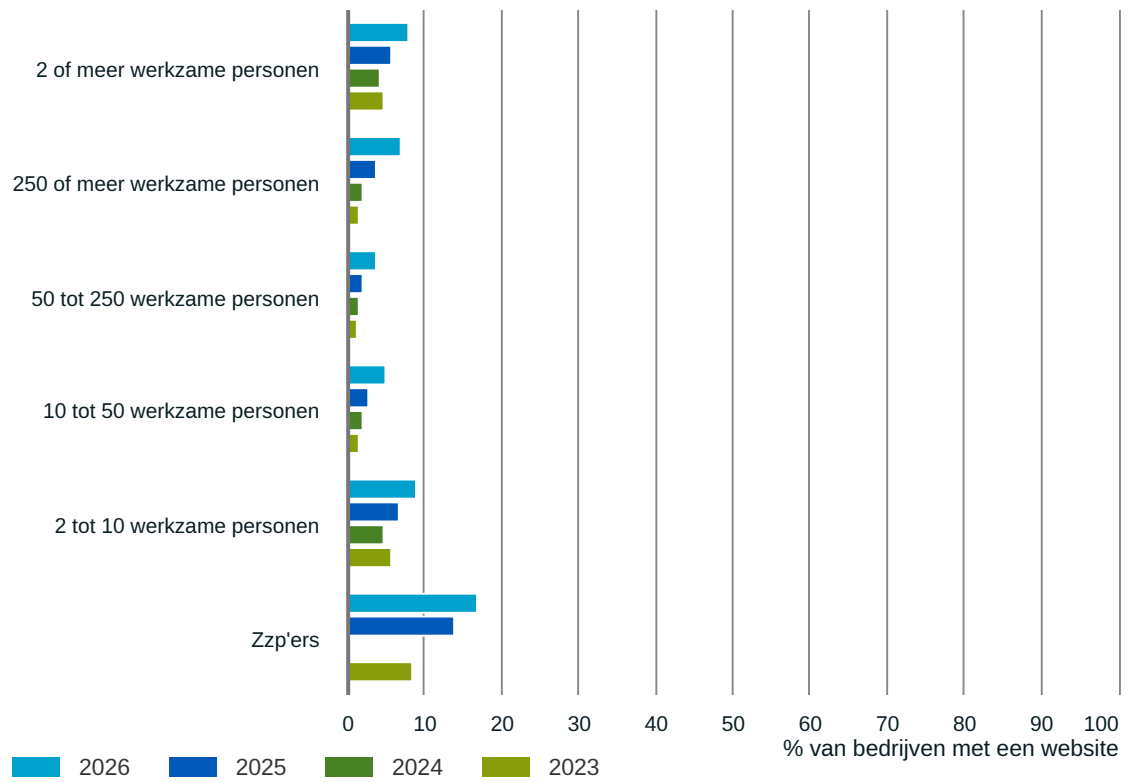
Figuur C.59.: Percentage van bedrijven met een website met geslaagde e-mailtest 'DANE geldig' naar bedrijfsgrootteklasse



Figuur C.60.: Percentage van bedrijven met een website met geslaagde e-mailtest 'DANE geldig' naar bedrijfstak (2 of meer werkzame personen)



Figuur C.61.: Percentage van bedrijven met een website met geslaagde e-mailtest 'DANE-  
vervangingschema' naar bedrijfsgrootteklasse

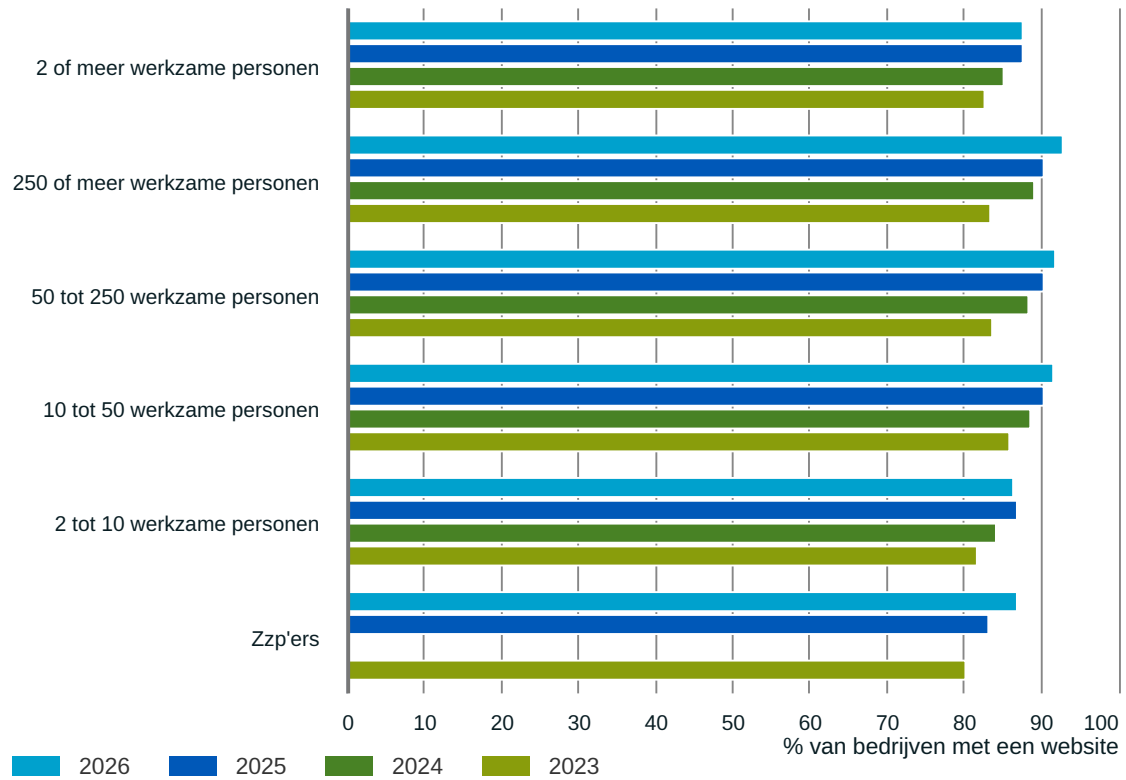


Figuur C.62.: Percentage van bedrijven met een website met geslaagde e-mailtest 'DANE-  
vervangingschema' naar bedrijfstak (2 of meer werkzame personen)

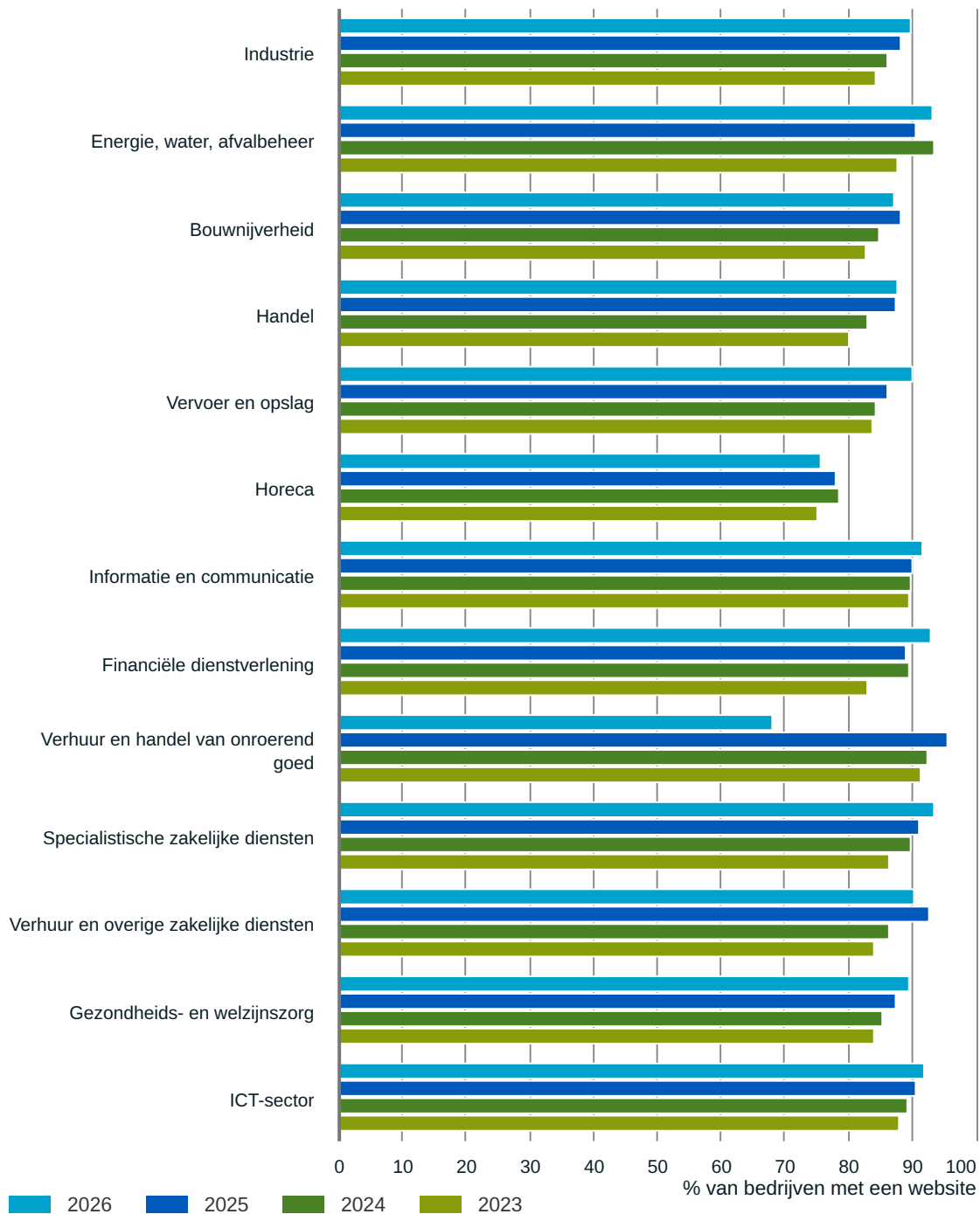


## C.5. E-mailscanuitslagen voor categorie RPKI

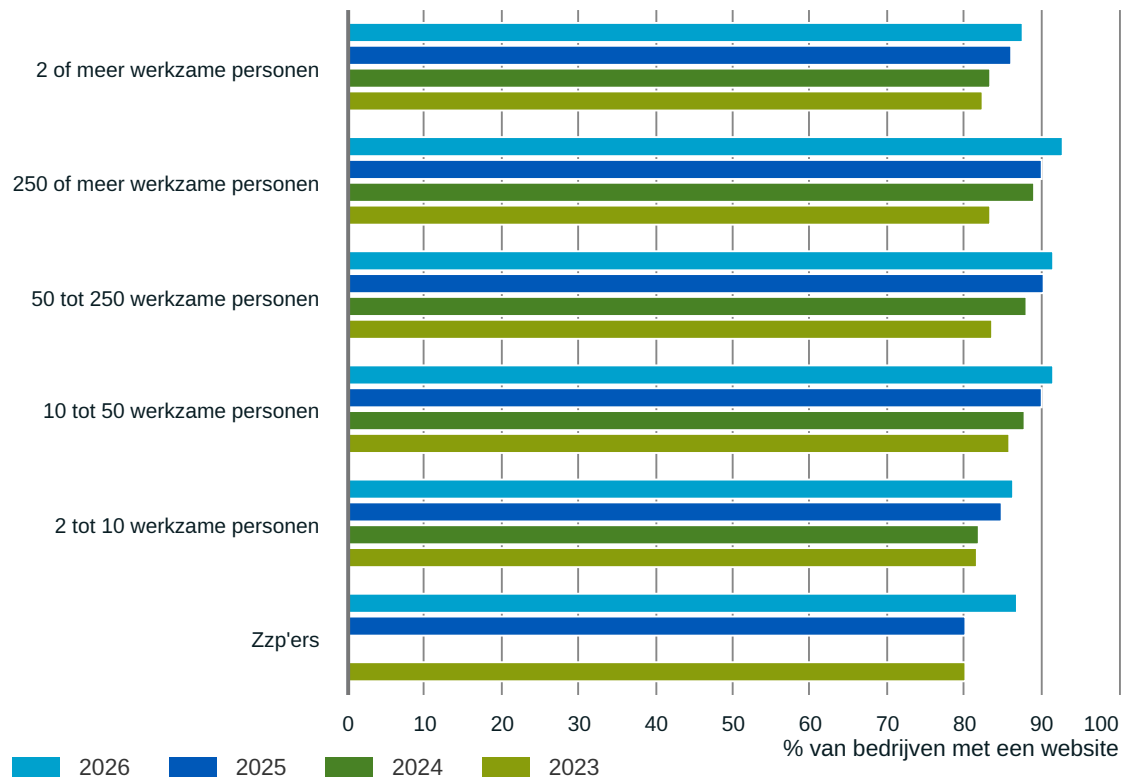
Figuur C.63.: Percentage van bedrijven met een website met geslaagde e-mailtest 'Aanwezigheid van Route Origin Authorisation voor ontvangende mailservers' naar bedrijfsgrootteklasse



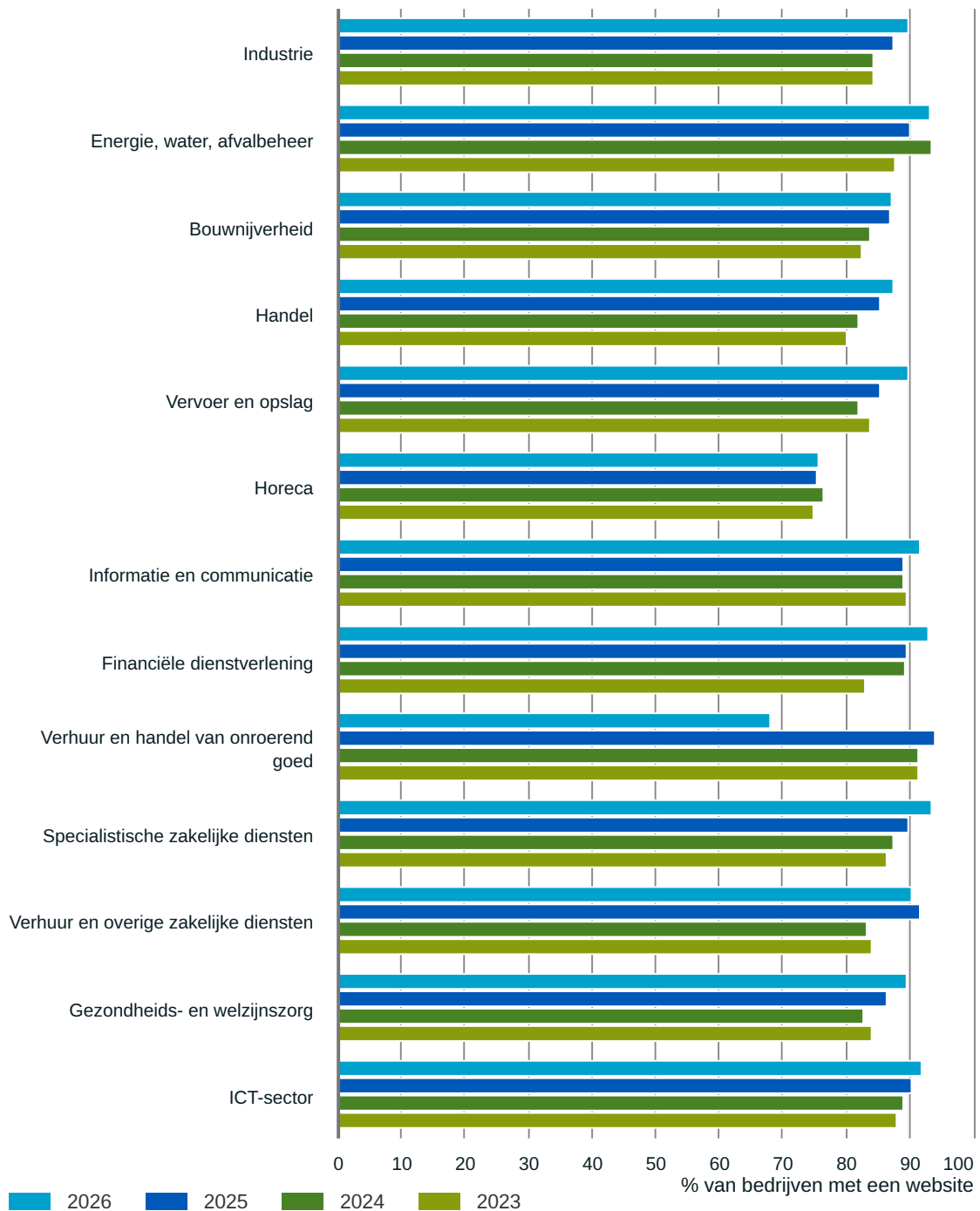
Figuur C.64.: Percentage van bedrijven met een website met geslaagde e-mailtest 'Aanwezigheid van Route Origin Authorisation voor ontvangende mailservers' naar bedrijfstak (2 of meer werkzame personen)



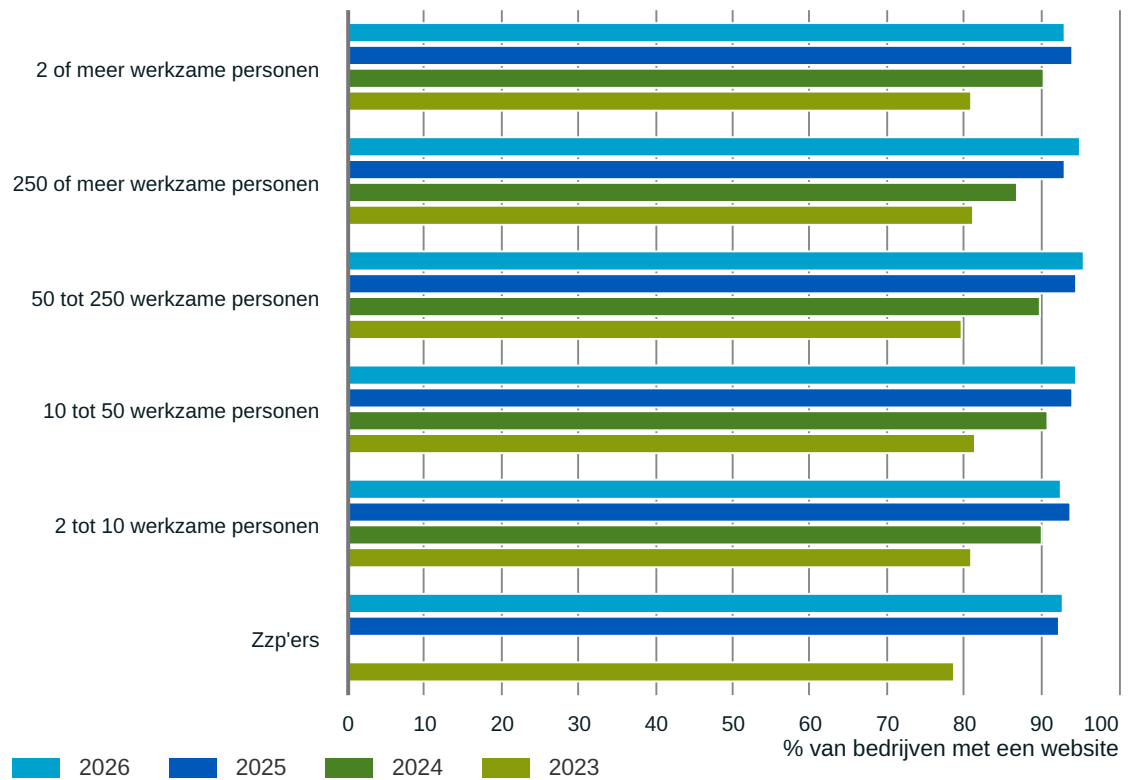
Figuur C.65.: Percentage van bedrijven met een website met geslaagde e-mailtest 'Geldigheid van route-aankondiging voor ontvangende mailservers' naar bedrijfsgrootteklasse



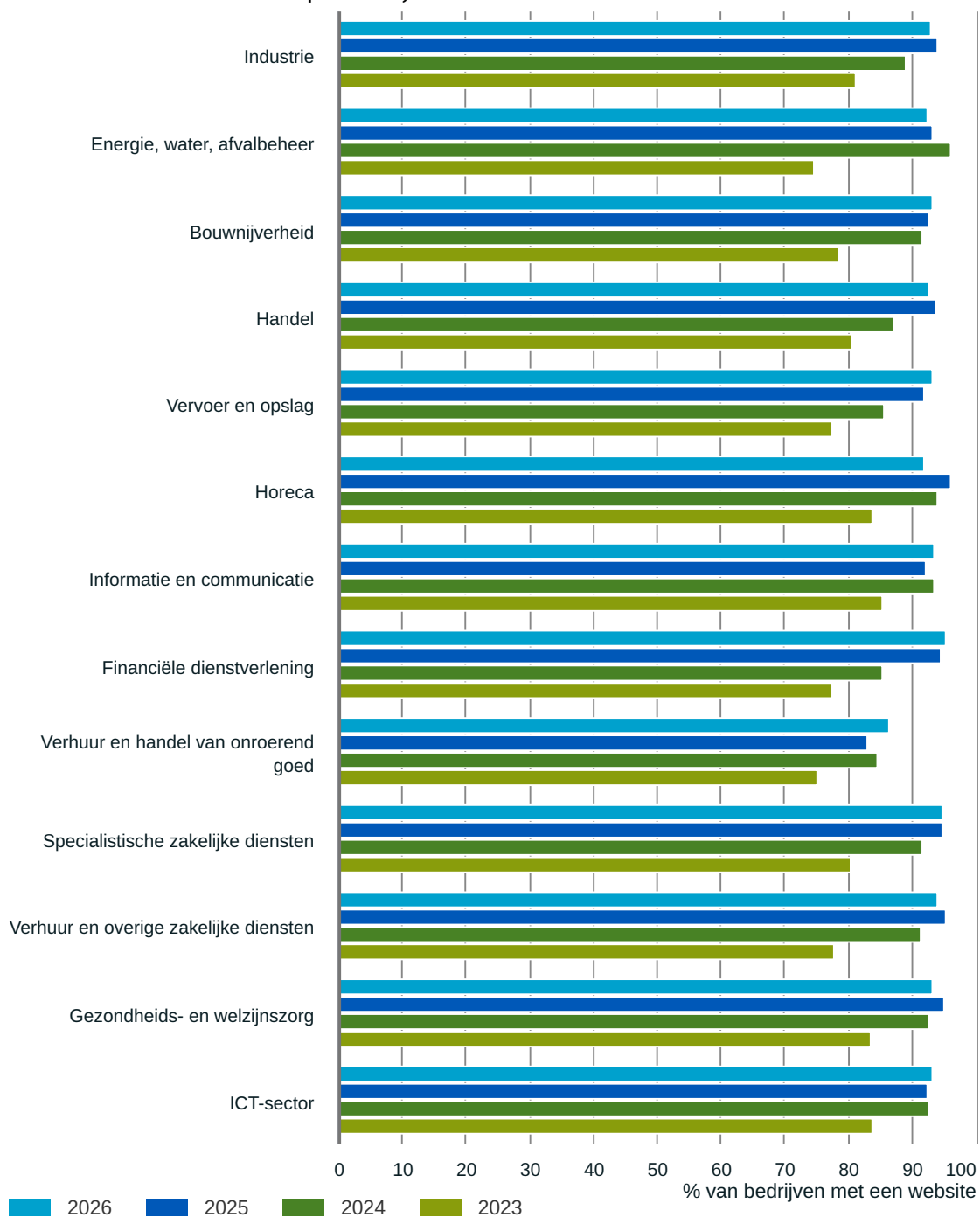
Figuur C.66.: Percentage van bedrijven met een website met geslaagde e-mailtest 'Geldigheid van route-aankondiging voor ontvangende mailservers' naar bedrijfstak (2 of meer werkbare personen)



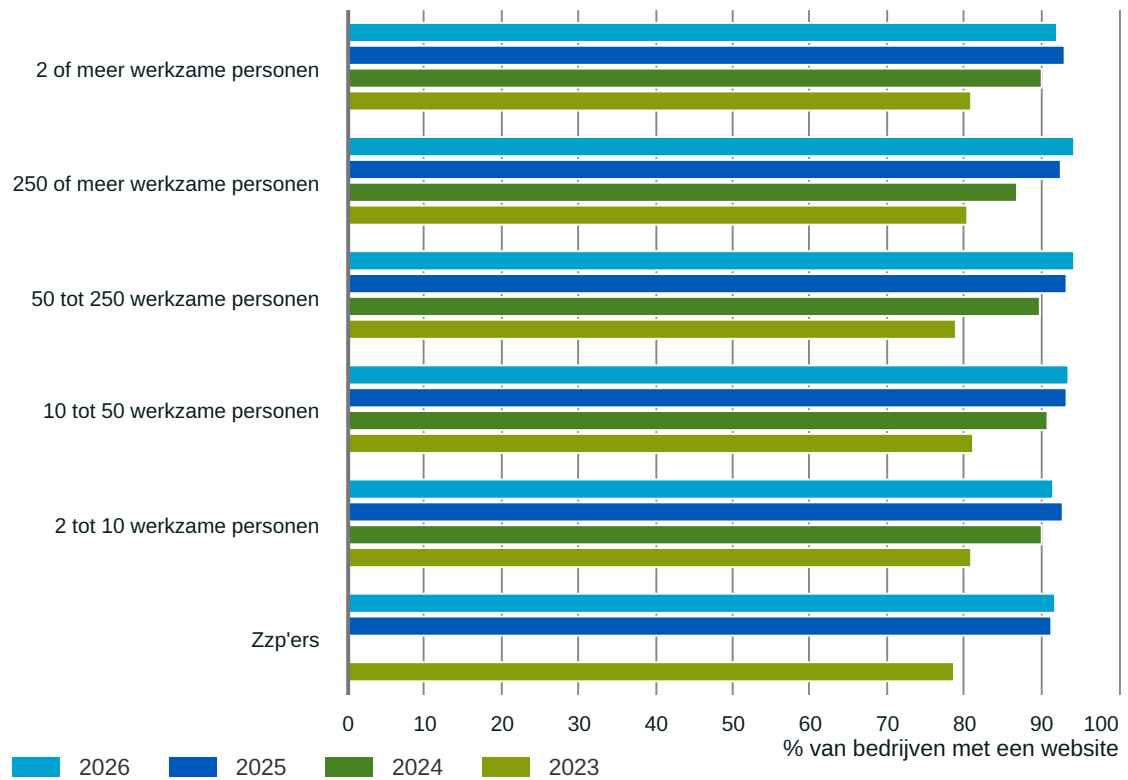
Figuur C.67.: Percentage van bedrijven met een website met geslaagde e-mailtest 'Aanwezigheid van Route Origin Authorisation voor nameserver van domein' naar bedrijfsgrootte-klasse



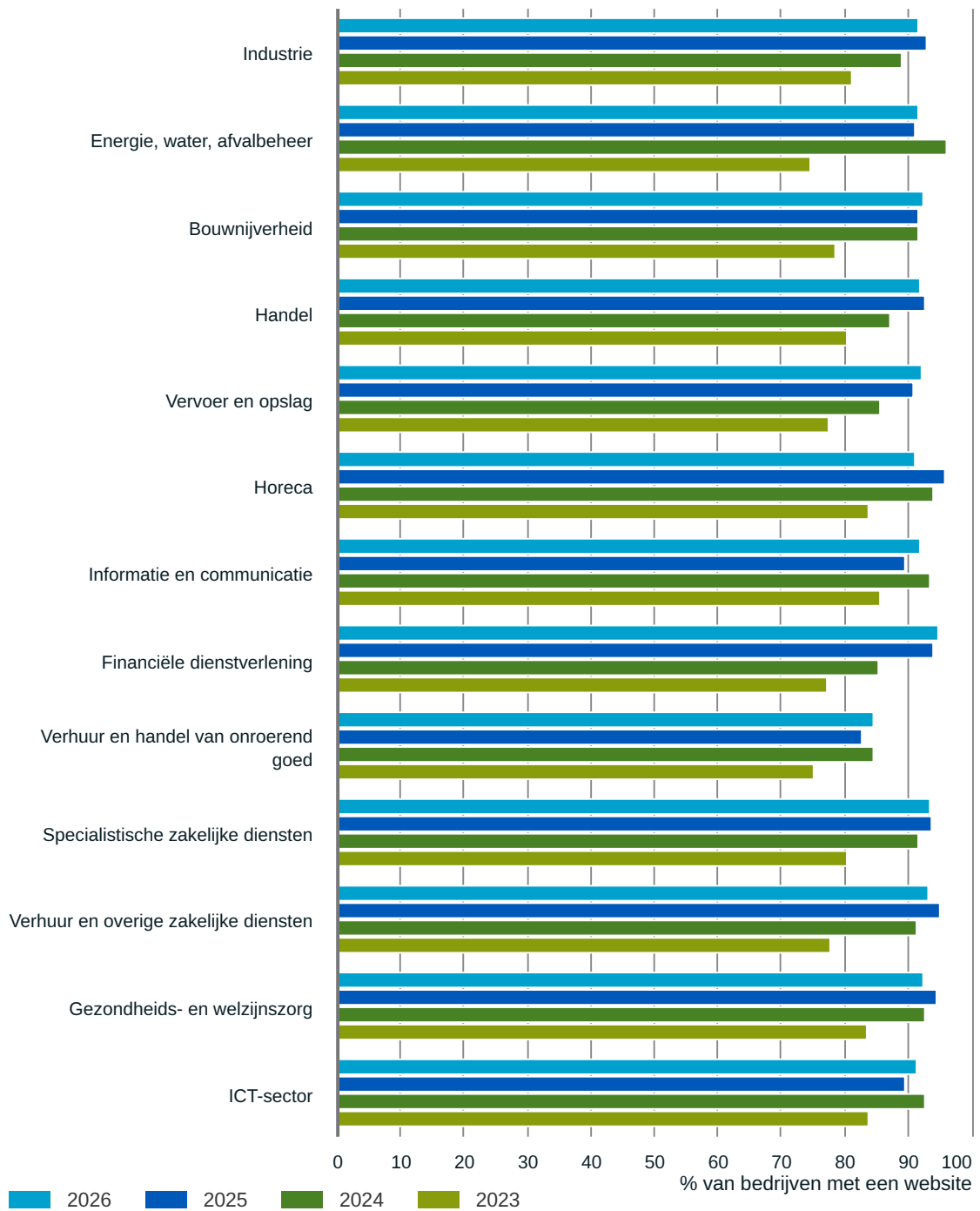
Figuur C.68.: Percentage van bedrijven met een website met geslaagde e-mailtest 'Aanwezigheid van Route Origin Authorisation voor nameserver van domein' naar bedrijfstak (2 of meer werkzame personen)



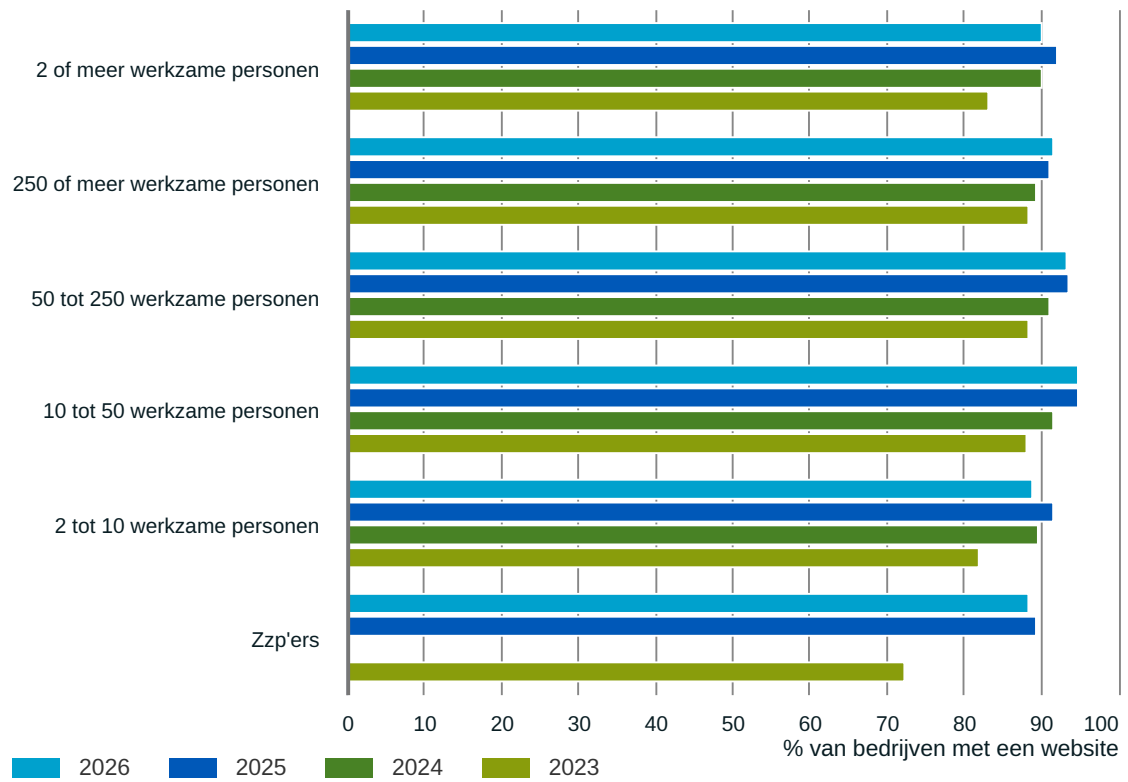
Figuur C.69.: Percentage van bedrijven met een website met geslaagde e-mailtest 'Geldigheid van route-aankondiging voor nameserver van domein' naar bedrijfsgrootteklasse



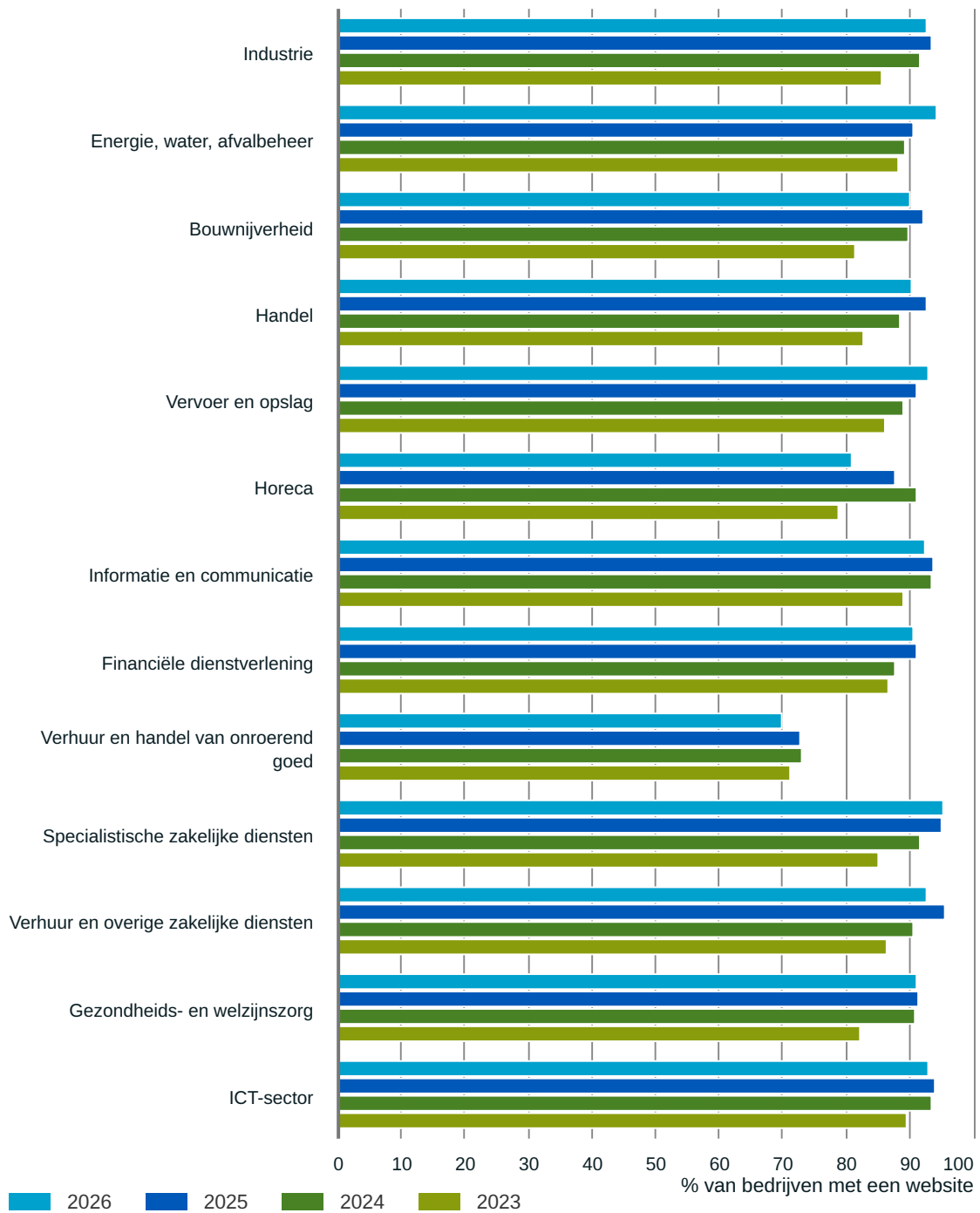
Figuur C.70.: Percentage van bedrijven met een website met geslaagde e-mailtest 'Geldigheid van route-aankondiging voor nameserver van domein' naar bedrijfstak (2 of meer werkbare personen)



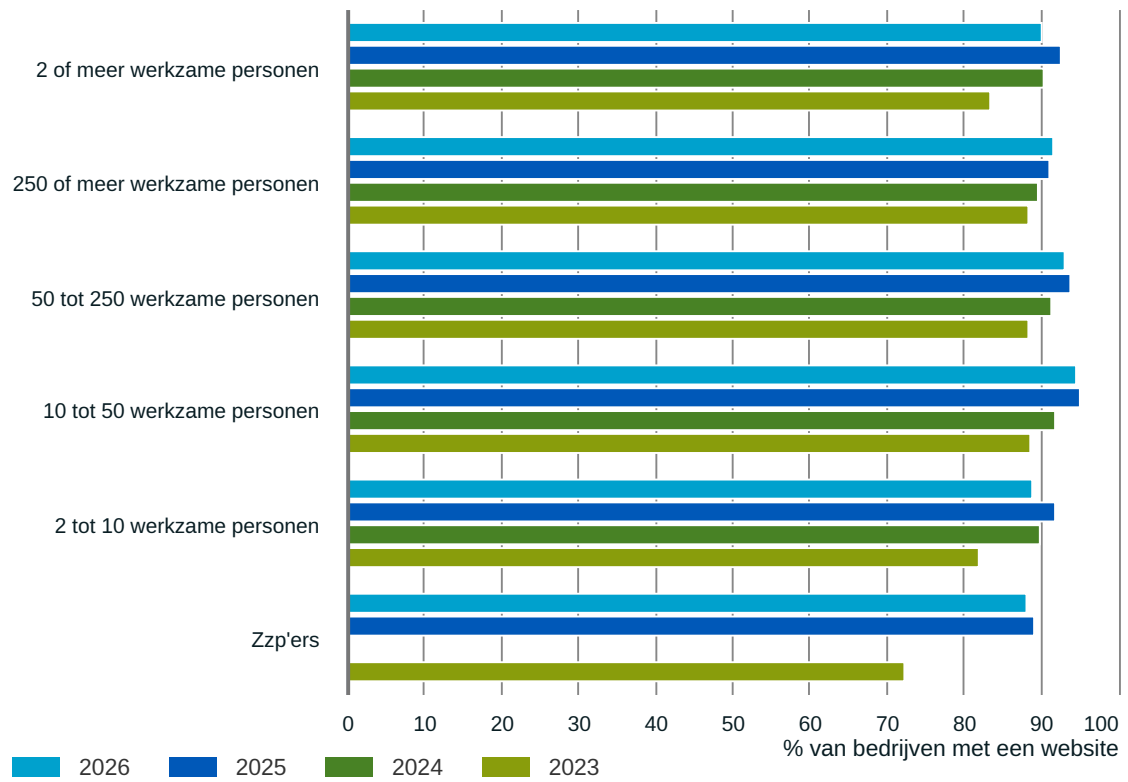
Figuur C.71.: Percentage van bedrijven met een website met geslaagde e-mailtest 'Aanwezigheid van Route Origin Authorisation voor nameserver van mailservers' naar bedrijfsgrootteklasse



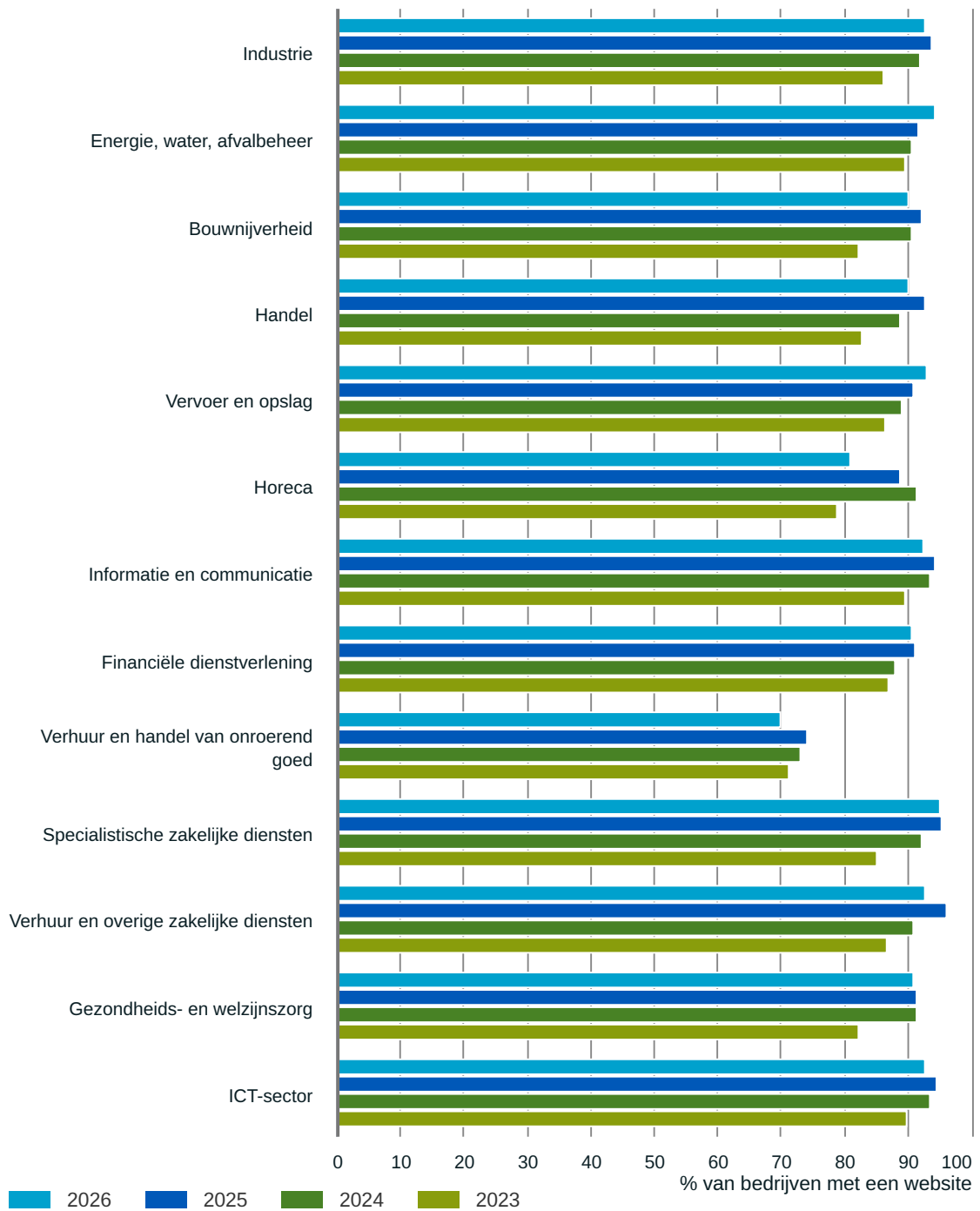
Figuur C.72.: Percentage van bedrijven met een website met geslaagde e-mailtest 'Aanwezigheid van Route Origin Authorisation voor nameserver van mailservers' naar bedrijfstak (2 of meer werkzame personen)



Figuur C.73.: Percentage van bedrijven met een website met geslaagde e-mailtest 'Geldigheid van route-aankondiging voor nameserver van mailservers' naar bedrijfsgrootteklasse

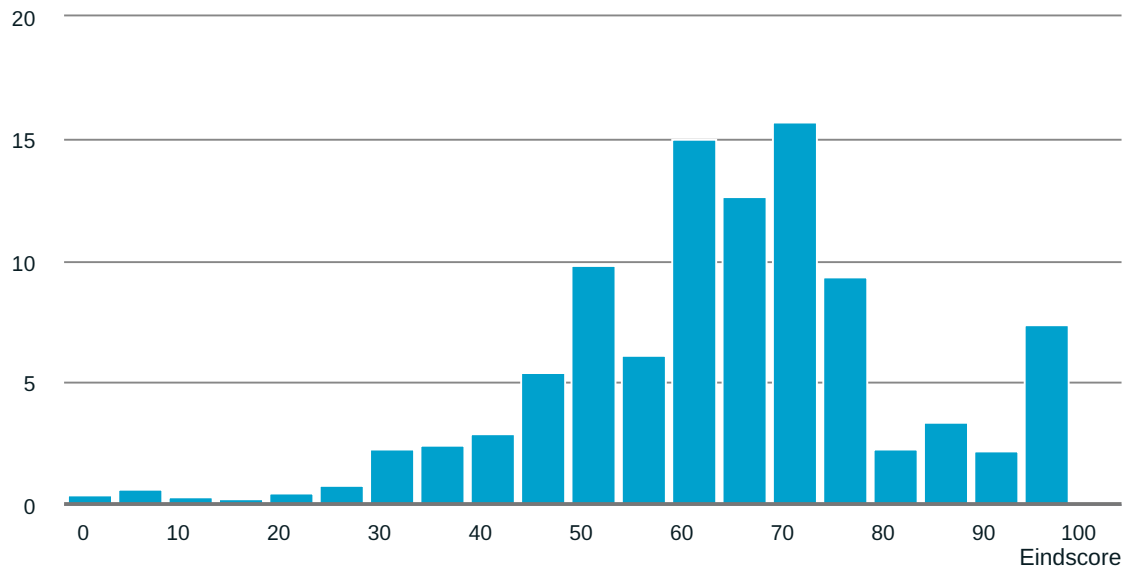


Figuur C.74.: Percentage van bedrijven met een website met geslaagde e-mailtest 'Geldigheid van route-aankondiging voor nameserver van mailservers' naar bedrijfstak (2 of meer werkzame personen)

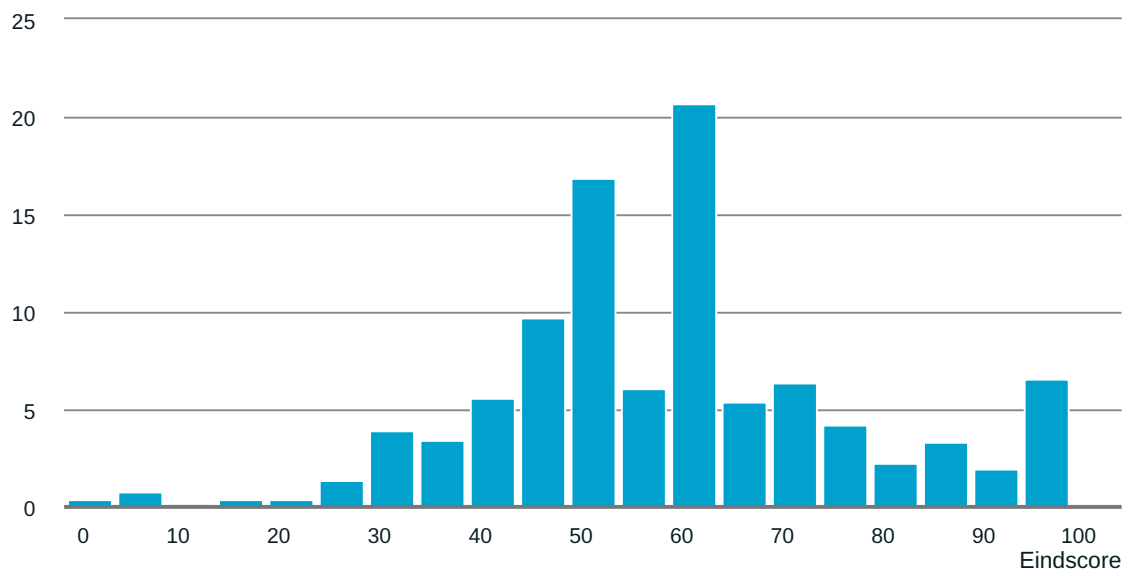


## C.6. Verdeling eindscores e-mailscan

Figuur C.75.: Verdeling eindscores e-mailscan voor bedrijven met 2 of meer werkzame personen, 2025



Figuur C.76.: Verdeling eindscores e-mailscan voor bedrijven met 2 of meer werkzame personen, 2024



Figuur C.77.: Verdeling eindscores e-mailscan voor bedrijven met 2 of meer werkzame personen, 2023

