

Toepassing van Internetstandaarden voor websites van bedrijven 2023

Een statistische analyse van Internet.nl-scores



Toepassing van Internetstandaarden voor websites van bedrijven 2023

Een statistische analyse van Internet.nl-scores

Verklaring van tekens

Niets (blanco)	Een cijfer kan op logische gronden niet voorkomen
·	Het cijfer is onbekend, onvoldoende betrouwbaar of geheim
*	Voorlopige cijfers
**	Nader voorlopige cijfers
2023–2024	2023 tot en met 2024
2023/2024	Het gemiddelde over de jaren 2023 tot en met 2024
2023/'24	Oogstjaar, boekjaar, schooljaar enz., beginnend in 2023 en eindigend in 2024
2021/'22–2023/'24	Oogstjaar, boekjaar, enz., 2021/'22 tot en met 2023/'24

In geval van afronding kan het voorkomen dat het weergegeven totaal niet overeenstemt met de som van de getallen.

Colofon

Uitgever

Centraal Bureau voor de Statistiek
Henri Faasdreef 312, 2492 JP Den Haag
www.cbs.nl

Prepress

Centraal Bureau voor de Statistiek

Ontwerp

Edenspiekermann

Inlichtingen

Tel. 088 570 70 70
Via contactformulier: www.cbs.nl/infoservice

© Centraal Bureau voor de Statistiek, Den Haag/Heerlen/Bonaire, 2024.
Verveelvoudigen is toegestaan, mits het CBS als bron wordt vermeld.

Inhoud

Inhoud	3
1	Introductie 5
1.1	Achtergrond 6
1.2	Type scans 6
2	Methodebeschrijving 8
2.1	Statistische analyse van het gebruik van internetstandaarden voor websites van bedrijven 9
2.2	Verdeling van de website over de verschillende domeinextensies 14
2.3	Enkele internetstandaarden van alle .nl-websites volgens SIDN 16
3	Resultaten websitescans 18
3.1	Introductie 19
3.2	Resultaten van Internet.nl per bedrijfsgrootteklasse en -tak 19
3.3	Verdelingen van de eindscores van de websitescan van alle bedrijven 30
3.4	Welke bedrijven hebben de hoogste en laagste score voor de websitescan? 31
4	Resultaten e-mailscans 36
4.1	Introductie 37
4.2	Resultaten van Internet.nl per bedrijfsgrootteklasse en -tak 37
4.3	Verdelingen van de eindscores van de e-mailscan van alle bedrijven 47
4.4	Welke bedrijven hebben de hoogste en laagste score voor de e-mailscan? 48
5	Conclusies 52
	Bibliografie 54
A	Tabellen 56
A.1	Overzicht Bedrijfsgrootteklassen en bedrijfstakken 56
A.2	Kenmerken websitescans Internet.nl 57
A.3	Kenmerken e-mailscan Internet.nl 58

B Alle websitetestuitslagen 59

- B.1 Website-testuitslagen voor categorie 'IPv6' 59
- B.2 Website-testuitslagen voor categorie 'Domeinnaamhandtekening' (DNSSEC) 65
- B.3 Website-testuitslagen voor categorie 'HTTPS' 68
- B.4 Website-testuitslagen voor categorie 'Beveiligingsopties' 89
- B.5 Website-testuitslagen voor categorie 'RPKI' 94
- B.6 Website-scan eindscoreverderlingen 99

C Alle e-mailtestuitslagen 102

- C.1 E-mailtestuitslagen voor categorie 'IPv6' 102
- C.2 E-mailtestuitslagen voor categorie 'Domeinnaamhandtekening' (DNSSEC) 107
- C.3 E-mailtestuitslagen voor categorie 'Authenticatie' 112
- C.4 E-mailtestuitslagen voor categorie 'StartTLS' 118
- C.5 E-mailtestuitslagen voor categorie 'RPKI' 136
- C.6 Email-scan eindscoreverderling 143

1.

Introductie

1.1 Achtergrond

In 2020 is het CBS in opdracht van het ministerie van Economische Zaken en Klimaat samen met [Platform Internetstandaarden](#) een onderzoek begonnen naar het gebruik van internetstandaarden bij websites van bedrijven in Nederland. Doel van dit onderzoek is om in kaart te brengen hoe goed bedrijven per bedrijfsgrootteklasse en bedrijfstak (veilige) Internetstandaarden voor hun website gebruiken.

Het toepassen van internetstandaarden verhoogt de veiligheid, betrouwbaarheid en toegankelijkheid van het internet. In dit onderzoek wordt de webtool [Internet.nl](#) van Platform Internetstandaarden gebruikt, om websites van bedrijven te testen op gebruik het van internetstandaarden. Op Internet.nl is het mogelijk om een websiteadres in te voeren; Internet.nl zal dan een scan van de ingevoerde website maken om deze te toetsen op ruim dertig internetstandaarden. Met de uitkomsten van deze testen wordt een eindscore toegekend als percentage tussen 0 en 100 procent; een website met een 100 procent eindscore voldoet aan alle eisen om de website zo veilig en gestandaardiseerd mogelijk te maken.

In dit onderzoek wordt de scanmethodiek van Internet.nl toegepast op een representatieve steekproef van websites van bedrijven. De websites die gescand zijn, worden verkregen uit de CBS-enquête 'ICT-gebruik bij bedrijven' (verder kortweg ICT-enquête genoemd) van de jaren 2020, 2021, 2022 en 2023 (Zie Statline enquêtes [CBS](#), [2020](#), [2021](#), [2022a](#), [2023a](#)). In deze enquête wordt gevraagd of het bedrijf een eigen website heeft en, zo ja, wat de website (domeinnaam of URL) is met de meeste bezoekers (de hoofdwebsite). Deze websites worden achteraf via Internet.nl gescand. Doordat de websites via een representatieve steekproef verkregen zijn, kan per bedrijfsgrootteklasse en bedrijfstak bepaald worden hoe goed de juiste internetstandaarden worden toegepast voor de website van bedrijven.

De resultaten van de eerste scanronde op basis van de ICT-enquête 2020 zijn eerder gepubliceerd in de long-read [CBS \(2022c\)](#). In het rapport daarna ([CBS, 2023b](#)) werden daar nog drie scans bijgevoegd; twee scans op basis van de websites die verzameld zijn met de ICT-enquête van 2021 en 2022; de derde scan is in april 2023 uitgevoerd met dezelfde websites als 2022. Deze laatste scan bevatte voor het eerst ook een scan naar de e-mail kenmerken van de mail-servers van het bedrijf. In het rapport dat nu verschijnt worden weer twee nieuwe scan toegevoegd op basis van de website verkregen uit de ICT-enquête van 2023: één scan uitgevoerd in december 2023, één scan uitgevoerd in april 2024. In het huidige rapport kunnen we dus de resultaten van zes scans voor de web servers en drie scan voor de mail servers terugvinden. Een overzicht van alle scan data wordt in tabel [2.1.2](#) gegeven.

1.2 Type scans

In dit onderzoek zijn twee type scans op de website van bedrijven uitgevoerd: een scan naar het gebruik van Internetstandaarden van de website van bedrijven en een scan naar het gebruik van Internetstandaarden van het e-maildomein van het bedrijven. Beide type scans leveren uiteindelijk per domeinnaam een score tussen de 0 en 100 procent op. Deze score wordt door Internet.nl berekend aan de hand van de uitslag van bijna veertig onderliggende testen voor zowel de websitescan als de e-mailscan. De testen van de websitescan zijn weer onder te verdelen in vijf categorieën, namelijk:

- [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

Iedere categorie bestaat weer uit losse subtesten waarmee bepaald wordt of een bedrijf slaagt voor een categorie of niet. In tabel [A.2.1](#) wordt een overzicht van de categorieën van de website scan met alle onderliggende subtesten gegeven.

De testen van de e-mailscans zijn ook op te verdelen in vijf categorieën, namelijk:

- [IPv6](#): bereikbaarheid via een modern internetadres.
- [DNSSEC](#): gebruik van een ondertekende domeinnaam.
- [DMARC](#), [DKIM](#), [SPF](#): Authenticatie als protectie tegen e-mail phishing.
- [STARTTLS](#) en [DANE](#): beveiligde mailserver-verbinding.
- [RPKI](#): Autorisatie voor routing

Iedere categorie bestaat weer uit losse subtesten waarmee bepaald wordt of een bedrijf slaagt voor een categorie of niet. In tabel [A.3.1](#) wordt een overzicht van de categorieën van de e-mailscan met alle onderliggende subtesten gegeven.

Zoals gezegd worden de resultaten van zowel de website- als e-mailscans gepresenteerd. De e-mailscans zijn alleen toegevoegd in de laatste twee scanrondes van 2023 en 2024. Alhoewel er in 2021 en 2022 wel e-mailscans uitgevoerd zijn, bleek bij de analyse achteraf dat voor deze scans het subdomain van de website niet correct verwijderd was. Er werd bijvoorbeeld op [www.example.com](#) gescand, terwijl voor de e-mailscans het subdomain [www](#) verwijderd had moeten worden om alleen [example.com](#) te scannen. In de laatste drie scans van april 2023 (waarbij dezelfde steekproef als 2022 genomen is) en december 2023 en april 2024 (waarbij het steekproef van 2023 is genomen) is het subdomein wel correct verwijderd. De uitkomsten van de e-mailscan met of zonder subdomein [www](#) verschillen echter van elkaar, waardoor de e-mailscan van 2021 en 2022 niet met de latere scans vergeleken kunnen worden. Om deze reden worden van de websitescans zes opeenvolgende perioden gepresenteerd, terwijl van de e-mailscans alleen de resultaten van de laatste drie rondes worden getoond.

Eerst wordt in hoofdstuk [2](#) in het kort de methode beschreven die gebruikt is om de Internet.nl scans uit te voeren en te analyseren. De resultaten van de websitescans en e-mailscans worden achtereenvolgens in hoofdstuk [3](#) en hoofdstuk [4](#) besproken. Een overzicht van alle onderliggende website en email testen wordt in de bijlagen [B](#) en [C](#) gegeven. In hoofdstuk [5](#) worden de conclusies van dit onderzoek gegeven.

2.

Methodebeschrijving

2.1 Statistische analyse van het gebruik van internetstandaarden voor websites van bedrijven

Enquête ‘ICT-gebruik bij bedrijven’

De domeinnamen die in dit onderzoek gebruikt worden, zijn verkregen uit de enquête ‘ICT-gebruik bij bedrijven’ (kort: de ICT-enquête). In deze jaarlijkse enquête onderzoekt het CBS het gebruik van informatie- en communicatietechnologie (ICT) door bedrijven. Er wordt op verschillende aspecten van ICT-gebruik ingegaan, zoals ‘ICT-veiligheid’, ‘ICT en personeel’ en ‘software- en hardwaregebruik’. De gegevens worden uiteindelijk uitgesplitst naar bedrijfsgrootteklasse en bedrijfstak gepubliceerd op Statline.

In de *ICT-enquête* wordt gevraagd of het bedrijf een website heeft. In figuur 2.1.1(a) is te zien dat in 2023 bijna drie op de vier (71 procent) van de bedrijven met twee of meer werknemers deze vraag positief beantwoordt. Dit is minder dan het jaar hiervoor; in 2022 gaf nog 77 procent van de bedrijven met 2 of meer werknemers aan een website te hebben. Grote bedrijven hebben vaker een eigen website hebben dan kleine bedrijven: in 2023 had van de bedrijven met 250 en meer werknemers 93 procent een website tegen 67 procent van de bedrijven met 2 tot 10 werknemers. Zzp’ers zijn pas recent toegevoegd en worden in dit onderzoek alleen bij de scans van 2022 en april 2023 meegenomen. Voor deze laatste twee jaren worden de websites van dezelfde ICT-enquête 2022 genomen; daarom wordt in figuur 2.1.1 alleen het jaar 2022 getoond. Daarnaast is de vraag over websites niet in de laatste enquête van 2023 opgenomen. De scans van december 2023 en april 2024 zijn op deze laatste enquête gebaseerd. Hierdoor kunnen we helaas voor de laatste scan geen gegevens over zzp’ers laten zien.

Aan bedrijven die aangeven een website te hebben, wordt in de ICT-enquête vervolgens gevraagd om de URL (*Uniform Resource Locator* oftewel het internetadres) van de website gevraagd. Als het bedrijf meerdere websites heeft, wordt gevraagd de URL van de website met de meeste bezoekers per dag op te geven (de hoofdwebsite). Op deze manier heeft een bedrijf altijd hooguit één website gekoppeld. De websites die op deze manier verkregen zijn, vormen de invoer van de veiligheidsscan van Internet.nl, de website-scantool van Platform Internetstandaarden.

Websitescan bij Internet.nl

De websites die uit de ICT-enquête verkregen worden, zijn vervolgens met de API van [Internet.nl](https://internet.nl) gescand. Op deze manier is er per bedrijf met een website een score voor het gebruik van internetstandaarden van de website verkregen. Ook worden alle uitslagen van de onderliggende subtesten geleverd, zodat per internetstandaard bepaald kan worden of hieraan voldaan wordt. Doordat is gewerkt met een statistisch representatieve steekproef, kunnen ook de landelijke gemiddelden van de uitkomsten per bedrijfsgrootteklasse en bedrijfstak worden berekend.

De Internet.nl webtool kan zowel de website als de e-mail van een bedrijf testen op het gebruik van (veilige) internetstandaarden. De scan van de websites is zes keer gedaan op basis van vier verschillende steekproeven voor de jaren 2020, 2021, 2022, en 2023 (Zie Statline enquêtes [CBS](#), [2020](#), [2021](#), [2022a](#), [2023a](#)). De vierde scan is gedaan op basis van de steekproef van 2022, alleen zijn de websites nogmaals 5 maanden later gescand. Hetzelfde geldt voor de laatste scan in april 2024 die uitgevoerd is op de steekproef van het enquêtejaar 2023. De details van de scandata zijn in tabel [2.1.2](#) terug te vinden. Per scan is de steekproef van websites van het bijbehorende enquêtejaar gebruikt. De scans worden dan ook aangeduid met het jaar en maand dat de scan uitgevoerd is. Als er maar één scan in een jaar gebruikt is, dan wordt alleen het jaartal ter referentie gebruikt.

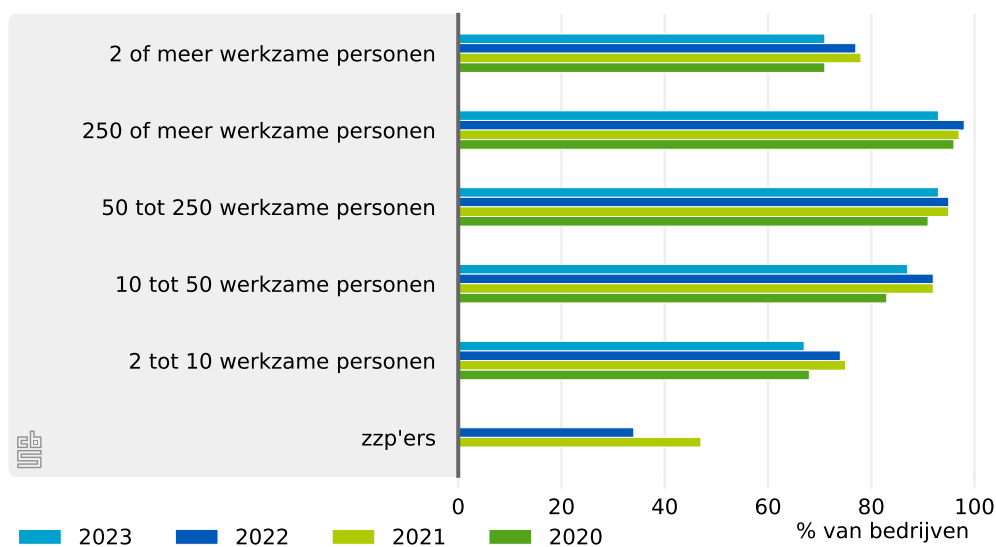
In figuren [2.1.3\(a\)](#) en [2.1.3\(b\)](#) worden de verdelingen van de bedrijfsgrootteklassen en bedrijfstakken voor de achtereenvolgende jaren gegeven. Merk op dat in 2022 voor het eerst ook zzp'ers aan de enquête deelnamen met de grootteklasse van één werkzame persoon. Voor de verdeling over de bedrijfstakken worden altijd alleen de bedrijven met twee of meer werkzame personen meegenomen. Dit geldt ook voor alle gepresenteerde statistieken voor de bedrijfstakken in dit rapport. Daarnaast wordt in figuur [2.1.3\(b\)](#) de verdeling over de bedrijfstakken getoond. In de resultaten zullen we ook de uitkomsten voor de ICT-sector presenteren; hierbij moet wel opgemerkt worden dat dit een samengestelde bedrijfstak is.

Ophoging van de eindscore

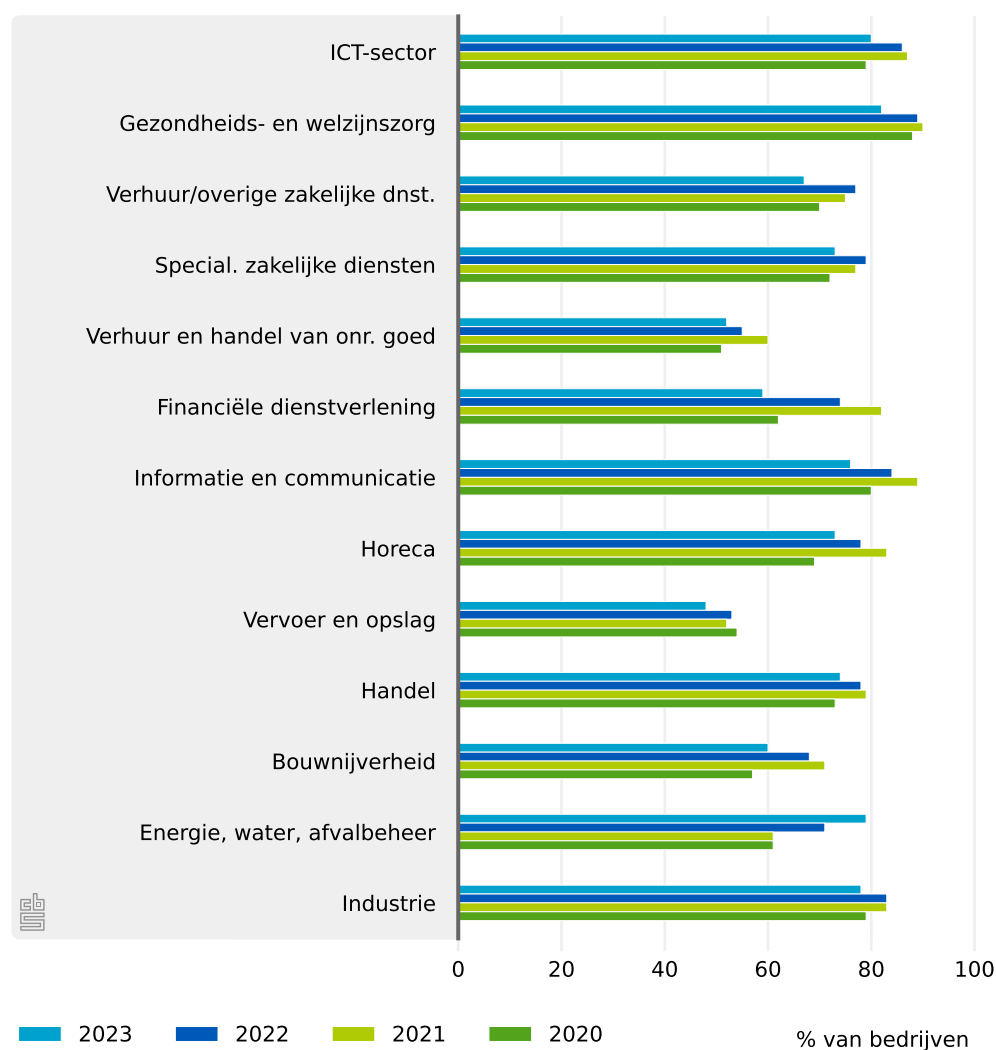
Zoals gezegd wordt per domeinnaam een eindscore bepaald met de scanmethodiek van Internet.nl die weergeeft hoe goed de website van het bedrijf internetstandaarden toepast. Deze eindscore wordt berekend met subtesten die opgedeeld zijn naar de vijf categorieën die in paragraaf [1.2](#) gegeven zijn. Doordat de websites uit een representatie steekproef verkregen zijn, is het mogelijk om de gemiddelde score van de testuitslag per bedrijfsgrootteklasse en bedrijfstak te berekenen. Hiertoe wordt het gewogen gemiddelde met weegfactoren berekend, waarbij de weegfactor verkregen wordt door per bedrijfsgrootteklasse en bedrijfstak het aantal bedrijven in de populatie te delen door het aantal bedrijven in de steekproef. De uiteindelijk grootteklassen en bedrijfstakken die in dit rapport worden gebruikt, zijn opgenomen in tabel [A.1.1](#) en tabel [A.1.2](#).

2.1.1 Bedrijven met een website per bedrijfsgrootteklasse (a) en bedrijfstak (b) in 2023

(a) Bedrijfsgrootteklasse



(b) Bedrijfstak



2.1.2 Detail van de Internet.nl scans

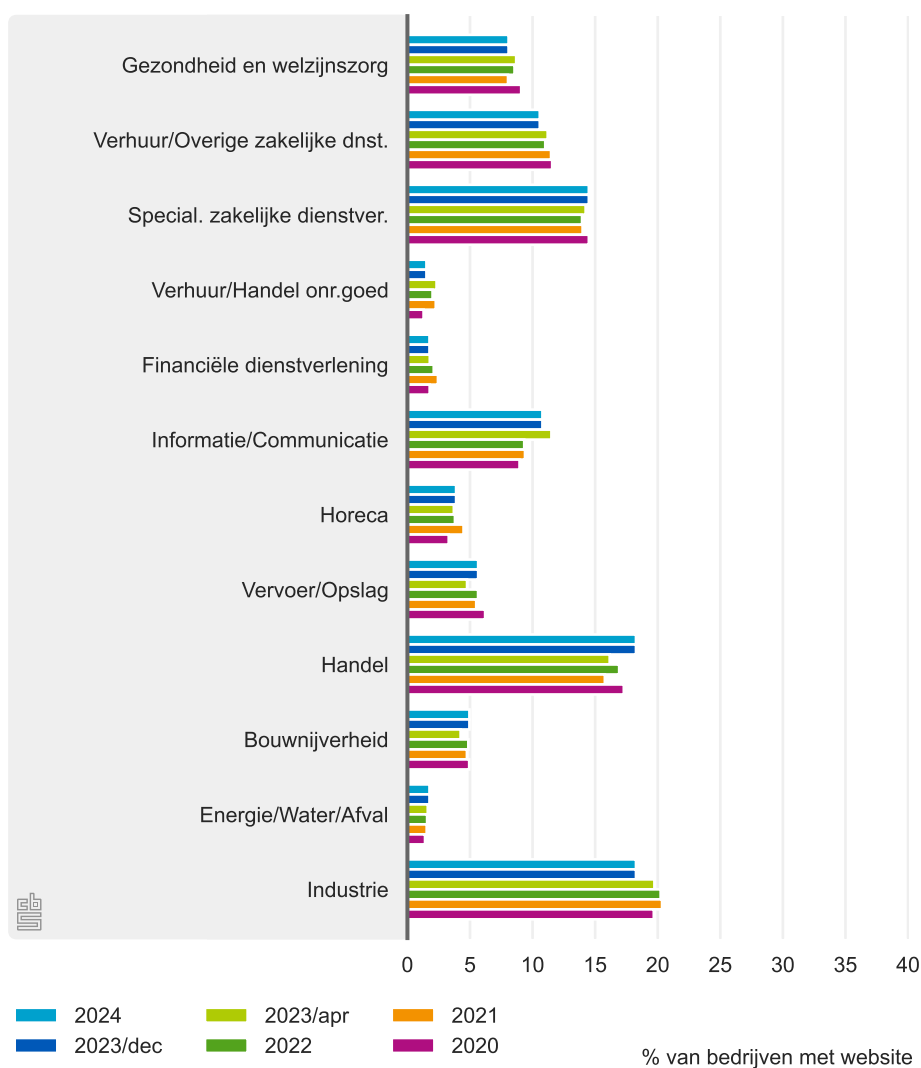
Label	Scandatum	Enquêtejaar	Websitescan	E-mailscan
2020	2020-10-22	2020	✓	X
2021	2022-03-31	2021	✓	X
2022	2022-12-24	2022	✓	X
2023/apr	2023-04-06	2022	✓	✓
2023/dec	2023-12-07	2023	✓	✓
2024	2024-04-03	2023	✓	✓

2.1.3 Verdeling van de gescande domeinnamen over de bedrijfsgrootteklassen (a) en bedrijfstakken (b).

(a) Bedrijfsgrootteklasse



(b) Bedrijfstak



2.2 Verdeling van de website over de verschillende domeinextensies

In de figuren 2.2.1(a) en 2.2.1(b) wordt per bedrijfsgrootteklasse en bedrijfstak de verdeling getoond van de domeinextensies over de meeste voorkomende extensies: *.nl*, *.com* en *.eu*. De figuur is gebaseerd op de websites verkregen uit de ICT-bedrijven enquête van het jaar 2023. Alle overige extensies zijn in één categorie *overig* samengenomen. Deze verdeling geeft dus de verdeling van de domeinextensies van de hoofdwebsite van bedrijven. Veel bedrijven hebben meerdere websites, dus de verdeling van alle websites bij elkaar genomen kan verschillen.

De verdeling per bedrijfsgrootteklasse getoond in figuur 2.2.1(a), toont aan dat *.nl* de meest voorkomende domeinextensie (of top level domain/tld) is: ruim 80 procent van de bedrijven met website met twee of meer werknemers heeft *.nl* als domeinextensie voor de hoofdwebsite. Ook is te zien dat *.nl* vaker voorkomt voor kleinere bedrijven, terwijl grote bedrijven met vijftig werknemers of meer relatief wat vaker *.com* als domeinextensie opgeven. Toch geeft ook van deze groep minimaal 62 procent van de bedrijven aan *.nl* als domeinextensie te hebben.

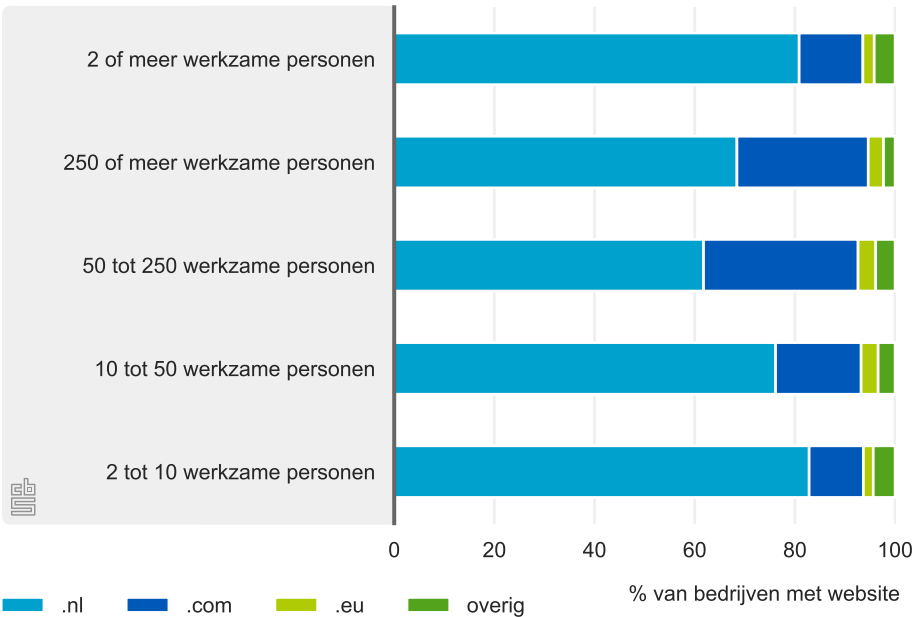
Naast *.nl* wordt ook *.com* vaak opgegeven als domeinnaamextensie: tot zo'n 30 procent van de bedrijven met 50 tot 250 werknemers¹⁾. De domeinextensie *.eu* heeft als derde nog een klein aandeel. Daarna zijn er nog veel domeinextensies (meer dan 70 verschillende) die met zijn allen niet meer dan 4 procent van het totaal uitmaken. Deze domeinextensies worden met de categorie *overig* aangeduid.

Figuur 2.2.1(b) toont tenslotte de verdeling van domeinnaamextensies per bedrijfstak voor alle bedrijven met website met twee of meer werknemers. Het gebruik van de domeinextensie *.nl* ligt rond de 80 procent voor alle bedrijfstakken, waarbij de 'Gezondheid en welzijnzorg' met ruim 96 procent van de bedrijven relatief vaker *.nl* gebruikt, terwijl de 'ICT-Sector' met 61 procent van de bedrijven relatief minder *.nl* gebruikt.

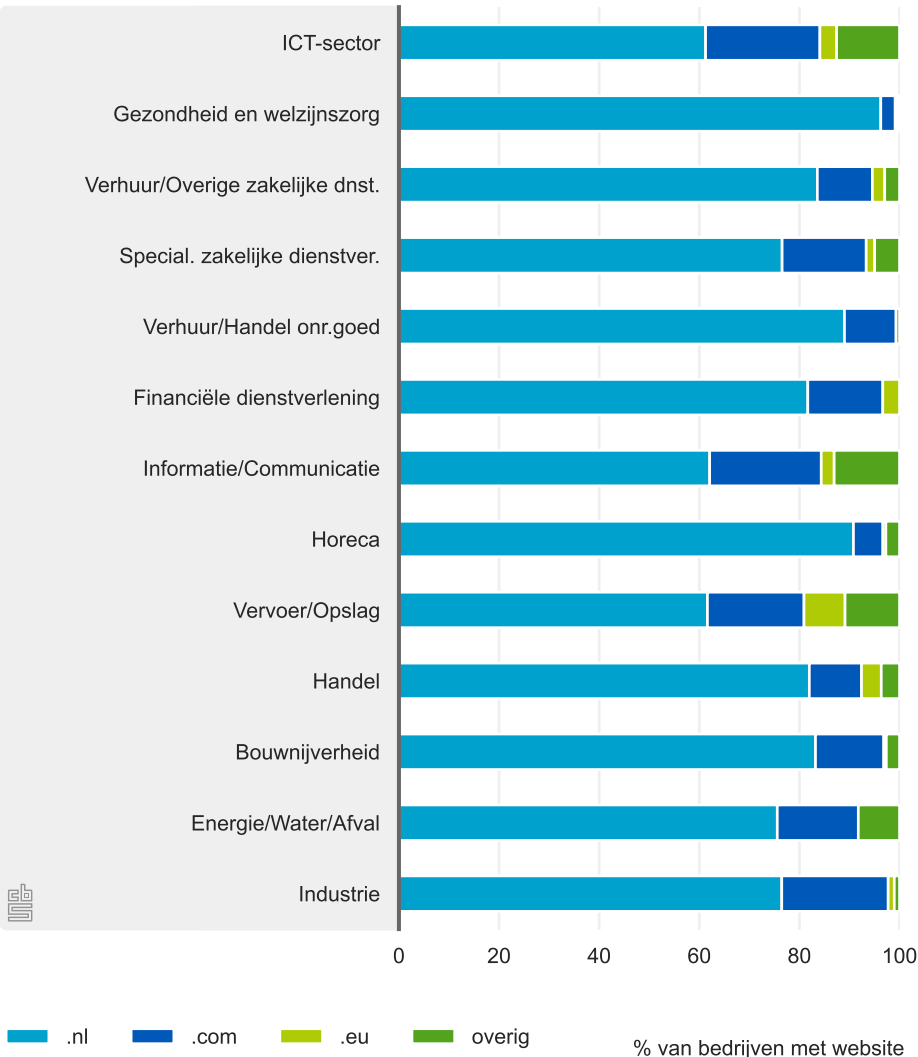
¹⁾ Zzp'ers zijn niet in de laatste scan's meegenomen omdat de vraag over de websites niet aan zzp'ers gevraagd is, zodat we ook geen websites van zzp'ers hebben om te scannen.

2.2.1 Verdeling van de domeinextensies per bedrijfsgrootteklasse (a) en bedrijfstak (b) zoals verkrijgen uit de ICT-enquete, 2023 (CBS, 2023a).

(a) Verdeling domeinextensies per bedrijfsgrootteklasse



(b) Verdeling domeinextensies per bedrijfstak



2.3 Enkele internetstandaarden van alle .nl-websites volgens SIDN

In dit rapport wordt het gebruik van (veilige) internetstandaarden bij websites van bedrijven in kaart gebracht. Uitgesplitst naar bedrijfsgrootte en bedrijfstak wordt gepresenteerd welk percentage van bedrijven volgens Internet.nl de internetstandaarden correct toepast voor hun website. Per bedrijf wordt altijd hooguit één website gekoppeld zoals deze in de ICT-enquête door het bedrijf zelf ingevuld is. Er wordt gevraagd naar de website met gemiddeld de meeste bezoekers per dag, hier aangeduid als de hoofdwebsite van het bedrijf. In dit rapport wordt dus de bedrijfseenheid als statistische eenheid gebruikt.

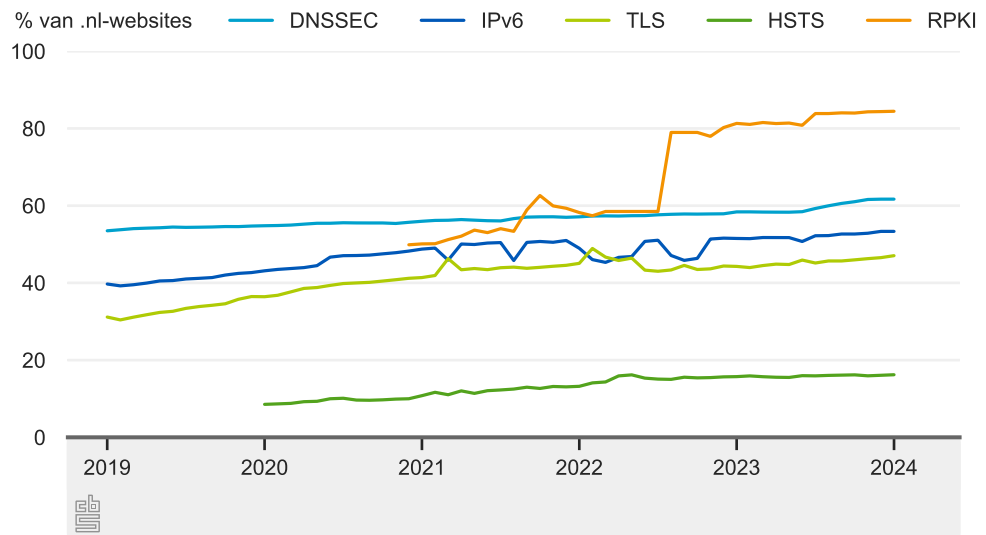
De Stichting Internet Domeinregistratie Nederland (SIDN, 2024) rapporteert op hun dashboard (SIDN Lab, 2024) de tijdseries van een aantal internetstandaarden van alle websites met een .nl domeinextensie. In de rapportage van de SIDN is de website zelf de statistische eenheid: per internetstandaard wordt gerapporteerd welk percentage van alle websites met een .nl-domeinextensie deze standaard toepast. Door het verschil in statistische eenheid kunnen de cijfers in dit rapport dus niet direct vergeleken worden met de percentages van bedrijven die de veiligheidskenmerken toepast. Toch is het zinnig om enkele kenmerken naast elkaar te leggen zodat we kunnen zien of de trends in ieder geval ongeveer hetzelfde zijn.

Figuur 2.3.1 laat de ontwikkeling van vijf veiligheidskenmerken zien als percentage van alle websites met een .nl-domeinnaam zoals gemeten door het SIDN. Het gaat om de volgende kenmerken:

- **DNSSEC** Percentage van alle .nl-websites dat is beveiligd met DNSSEC.
- **IPv6** Percentage van alle .nl-websites dat bereikbaar is via IPv6.
- **TLS** Percentage van alle .nl-websites waarbij de verbinding tussen de webserver en gebruiker met TLS versleuteld is.
- **HSTS** Percentage van alle .nl-websites met een HTTP Strict-Transport-Security HTTP-header (HSTS) waarmee ze browser laten weten dat de website alleen met HTTPS benaderd dient te worden.
- **RPKI** Percentage van alle .nl-websites dat Autorisatie voor routing gebruikt. Hiermee kunnen netwerkbeheerders valideren of een gepubliceerde route tussen netwerken geldig is.

De grafieken op het dashboard van SIDN tonen aan dat een steeds groter wordend aandeel van de .nl-websites de internetstandaarden correct toepast. In dit rapport kunnen we deze trend vergelijken met het toepassen van veiligheidsstandaarden per bedrijfsgroottesklasse en bedrijfstak. Voor de scans in dit rapport zijn alle domeinextensies meegenomen zijn, niet alleen .nl-websites. In paragraaf 2.2 is aangetoond dat rond de 80 procent van de hoofdwebsite bij bedrijven een .nl-website is. Toch zijn de uitkomsten in dit rapport niet direct te vergelijken met de cijfers gepresenteerd bij SIDN, omdat in dit rapport alleen de hoofdwebsite van ieder bedrijf genomen wordt, terwijl bedrijven best meerdere websites kunnen hebben. Daarnaast worden bij SIDN *alle* .nl-websites meegenomen, ook websites die geen eigendom zijn van een bedrijf, maar bijvoorbeeld eigendom zijn van particulieren of *domain resellers*. Direct vergelijken is dus niet mogelijk, maar we kunnen wel trends naast elkaar leggen.

2.3.1 Ontwikkeling van veiligheidskenmerken van websites met een .nl-domeinnaam (Bron: SIDN Lab, 2024)



3.

Resultaten

websitescans

3.1 Introductie

Met de websitescan van [Internet.nl](#) wordt getest of websites, mailservers en internetverbindingen aan de moderne internetstandaarden voldoen. In dit hoofdstuk worden de resultaten van de websitescan van de websites van bedrijven besproken om zo per bedrijfsgrootteklasse 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 website-analyse van [Internet.nl](#) bevat vijf categorieën:

1. [IPv6](#): bereikbaarheid via een modern internetadres.
2. [DNSSEC](#): gebruik van een ondertekende domeinnaam.
3. [HTTPS](#): gebruik van een beveiligde verbinding.
4. [Beveiligingsopties](#): gebruik van ingestelde Applicatie-beveiligingsopties.
5. [RPKI](#): Autorisatie voor routing

De laatste categorie is pas in 2022 toegevoegd. De score per categorie wordt bepaald met verschillende losse subtesten die binnen de categorie vallen. In dit hoofdstuk worden de resultaten per categorie gepresenteerd; in Appendix B worden de resultaten van alle onderliggende subtesten gegeven die per categorie uitgevoerd zijn. Een overzicht van de vijf categorieën met de bijbehorende subtesten kan in Tabel A.2.1 gevonden worden.

In sectie 3.2 wordt eerst naar de gemiddelde Internet.nl-eindscores en de gemiddelde scores per categorie per bedrijfsgrootteklasse en bedrijfstak gekeken. Daarna wordt in paragraaf 3.3 nog de verdeling van alle eindscores laten zien.

3.2 Resultaten van Internet.nl per bedrijfsgrootteklasse en -tak

Eindscore niet afhankelijk van bedrijfsgrootte, wel van bedrijfstak

In figuren 3.2.1(a) en 3.2.1(b) wordt per bedrijfsgrootteklasse en bedrijfstak voor de jaren 2020 tot en met april 2024 de eindscores van de websites van bedrijven in Nederland getoond zoals die door de scan met [Internet.nl](#) bepaald zijn. De gemiddelde eindscore per bedrijfsgrootte (figuur 3.2.1(a)) is per jaar voor alle bedrijfsgrootteklassen ongeveer gelijk en neemt met de tijd gestaag toe. Zo stijgt de gemiddelde Internet.nl-eindscore voor alle bedrijven met website met 2 of meer werknemers van 60,3 procent in 2020 naar 65,5 procent in april 2024; een absolute stijging van 5,2 procentpunten en een relatieve stijging van 8,6 procent in april 2024 ten opzichte van 2020. Voor bedrijven met website met 250 of meer werknemers was de Internet.nl-eindscore in 2020 nog 59,2 procent, terwijl dat in 2024 tot 67,2 procent is toegenomen. Deze toename van de eindscore is in dezelfde mate te zien voor

de andere bedrijfsgrootteklassen. De zzp'ers zijn pas in 2022 toegevoegd, dus hiervoor zijn nog maar 2 waardes beschikbaar¹⁾.

In de Cybersecuritymonitor (CBS, 2022b) wordt geconstateerd dat kleine bedrijven vaak minder maatregelen treffen dan grote bedrijven om hun ICT-systemen te beveiligen, maar bij het toepassen van internetstandaarden valt het op dat kleine bedrijven het even goed, zo niet beter, doen dan grote bedrijven. Een verklaring zou kunnen zijn dat kleine bedrijven vaker ICT-specialisten inhuren om hun website te bouwen en dat hierbij nieuwere standaarden worden gebruikt. Grote bedrijven hebben mogelijk vaker een website die al wat langer geleden ontwikkeld is in een tijd dat er nog minder aandacht was voor standaarden en dat deze later ook niet alsnog zijn toegepast bij onderhoudswerkzaamheden.

Figuur 3.2.1(b) toont de gemiddelde eindscore per bedrijfstak voor de jaren 2020 tot en met april 2024. In april 2024 varieerde de gemiddelde eindscore van 61,6 procent voor de bedrijfstak 'Verhuur en handel van onroerend goed' tot 75,5 procent voor de Financiële dienstverlening. Daarnaast is te zien dat de totale eindscore voor alle bedrijfstakken tussen 2020 en april 2024 gestegen is, met stijgingen van een paar procentpunt voor bijvoorbeeld de Handel tot ruim achttien procentpunt voor de Financiële dienstverlening. De Financiële dienstverlening heeft met name het afgelopen jaar relatief veel aandacht besteed aan het implementeren van veiligheidsstandaarden voor hun website. Opvallend is verder dat de eindscore van de ICT-sector in april 2024 is gedaald ten opzichte van april 2023: van 72,2 procent naar 66,5 procent. Naast de ICT-sector vertonen ook andere sectoren tussen april en december 2023 een daling in de eindscore. In de volgende paragraaf wordt aangetoond dat deze daling met name komt door de daling in bedrijven die slagen voor de categorie IPv6.

Uitkomsten Internet.nl-websitescan per categorie

De eindscore per categorie wordt samengesteld uit de onderliggende testen zoals in tabel A.2.1 gegeven is. Deze testen zijn in vijf categorieën opgedeeld: *IPv6*, *DNSSEC*, *HTTPS*, *Beveiligingsopties* en *RPKI*. Als een bedrijf binnen een categorie aan voldoende testen voldoet, zal de categorie door de Internet.nl-scan met 'geslaagd' aangeduid worden. In de figuren 3.2.2, 3.2.3, 3.2.4, 3.2.5 en 3.2.6 wordt voor de vijf categorieën het percentage van geslaagde bedrijven per bedrijfsgrootteklasse en bedrijfstak getoond. Terwijl de eindscores weinig per bedrijfsgrootteklasse en bedrijfstak variëren, is nu te zien dat er wel aanzienlijke verschillen per categorie zijn. Deze verschillen worden hier onder besproken.

De uitslag van een categorie wordt bepaald aan de hand van de uitkomsten van de onderliggende testen die door een scan van Internet.nl uitgevoerd wordt. De uitkomsten van alle onderliggende testen worden in de appendix B gegeven in de figuren B.1.1 tot en met B.5.4. In deze figuren is terug te vinden voor welke testen de verschillen tussen de verschillende bedrijfsgrootteklassen ontstaan. Hieronder worden de resultaten per categorie besproken en waar nodig naar de belangrijkste subtesten verwezen.

¹⁾ De scan in april 2023 vond 5 maanden later plaatst dan de scan in 2022; voor de scans van december 2023 en april 2024 was er geen scandata beschikbaar voor zzp'ers, omdat de vraag over websites niet in de enquête van 2023 gevraagd is. Voor de nu lopende enquête van 2024 is de vraag voor zzp'ers wel weer toegevoegd.

Categorie IPv6

De categorie IPv6 geeft aan in hoeverre een website bereikbaar is via een modern internetadres. Figuur 3.2.2(a) laat zien dat in april 2024 kleine bedrijven met twee tot tien werknemers bijna 50 procent vaker slagen voor de categorie IPv6 dan grote bedrijven met 250 of meer werknemers (respectievelijke 32,1 en 22,9 procent). Deze verhouding in is in april 2024 wel minder scheef geworden omdat er voor de grote bedrijven met 250 of meer werknemers een lichte stijging van het percentage geslaagde bedrijven te zien is, terwijl dit percentage voor kleine bedrijven juist gedaald is.

Dat kleine bedrijven vaker voor de categorie IPv6 slagen dan grote bedrijven komt wellicht doordat kleine bedrijven de website vaker bij externe providers hosten die meestal moderne netwerkinstellingen hebben. Grote bedrijven draaien de website vaker op hun eigen servers die niet altijd 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 minder aanleiding om hun servers aan te passen om IPv6 te gaan ondersteunen.

De uitsplitsing van de categorie IPv6 naar bedrijfstak getoond in figuur 3.2.2(b) laat zien dat de bedrijfstakken 'Financiële dienstverlening' en bedrijfstak 'Vervoer/Opslag' het ondersteunen van IPv6 goed op orde hebben. De scan van 2024 toont voor de Financiële dienstverlening ook een sterke toename van het percentage van bedrijven dat slaagt voor de categorie IPv6: waar in april 2023 nog gemiddeld 26,3 procent van bedrijven uit de Financiële dienstverlening bedrijven slaagde voor deze categorie, is dat in april 2024 toegenomen tot 47,0 procent.

Opvallend is dat in de scans van december 2023 en april 2024, een aantal bedrijfstakken juist een sterke daling laten zien op de categorie IPv6, met name de sectoren die daar in april 2023 nog vrij hoog in scoorden, zoals de 'ICT-sector' (daalde van 55,8% in april, 2023 naar 30,3% in april, 2024) en de 'Gezondheid en welzijnzorg' (daalde van 39,1% in april, 2023 naar 30,6% in april, 2024). Om bij Internet.nl te slagen voor categorie IPv6, moeten aan meer onderliggende testen voldaan worden. Deze uitslagen worden in appendix B gegeven. Het is te zien dat de daling van de categorie IPv6 voor de ICT-sector met name komt door de daling van de onderliggende testen van de adressen en bereikbaarheid van de *webserver* met IPv6 (respectievelijk figuren B.1.3 en B.1.4) en de test op gelijke website op IPv4 en IPv6, te zien in figuur B.1.5.

Categorie DNSSEC

De categorie DNSSEC geeft aan of een website met een geldige handtekening ondertekend is. In 2020 scoorden kleine bedrijven nog het beste op deze categorie, maar in figuur 3.2.3(a) is te zien dat de verschillen kleiner geworden zijn: in april 2024 slaagde gemiddeld 52,8 procent van de bedrijven met website met twee of meer werknemers voor de categorie DNSSEC (dit was in 2020 nog 44 procent). De bedrijven met een website met 50 tot 250 werknemers zitten daar het meest onder: 47,8 procent slaagt in 2024 voor de categorie DNSSEC. Bedrijven met 2 tot 10 werknemers score het hoogst voor deze categorie: bijna 54 procent van deze bedrijven heeft in 2024 een website met een geldige handtekening.

De categorie wordt in het geval van DNSSEC bepaald door maar twee onderliggende testen: *DNSSEC aanwezig* (figuur B.2.1) en *DNSSEC geldig* (figuur B.2.2) en daarom is te zien dat de scoreverdeling van de categorie DNSSEC bijna identiek is aan de onderliggende testen. Volgens SIDN Lab (2024) heeft begin 2024 ongeveer 62 procent van alle .nl-websites een geldige DNSSEC handtekening (zie figuur 2.3.1). In 2020 was dit nog ongeveer 55 procent.

Alhoewel het gemiddelde van alle bedrijven met een website onder deze waarde ligt, komt de stijgende trend tussen beide cijfers wel overeen.

Categorie HTTPS

De categorie HTTPS geeft aan of de website van een bedrijf voldoende beveiligd is. Ditmaal is in figuur 3.2.4(a) te zien dat grote bedrijven aanzienlijk beter scoren voor de categorie HTTPS dan kleine bedrijven. Wel is opvallend dat het slagingspercentage voor deze categorie vrij laag is: slechts 7,3 procent van alle bedrijven met website met 2 of meer werknemers had in 2024 een positieve uitslag voor de categorie HTTPS. Dit lage slagingspercentage voor de categorie HTTPS wordt veroorzaakt door het groot aantal subtesten dat gebruikt wordt om de categorie HTTPS te doen slagen; als één van de subtesten niet slaagt, zal hiermee ook de totale categorie HTTPS niet slagen.

Figuur 3.2.4(b) toont aan dat de websites van de bedrijfstakken 'ICT-sector' en 'Informatie/Communicatie' het beste scoren voor de categorie HTTPS. De ICT-sector is wel een samengestelde bedrijfstak bestaande uit bedrijfsactiviteiten van verschillende andere bedrijfstakken, waaronder enkele bedrijfsactiviteiten uit de 'Informatie /Communicatie' bedrijfstak, dus dit verklaart de overeenkomst tussen beiden. In de meeste bedrijfstakken is het aantal bedrijven met een website die in 2024 slaagt voor de categorie HTTPS, vergeleken met 2023, toegenomen. Dit geldt alleen niet voor de bedrijfstakken Verhuur/overige zakelijke diensten, Horeca, Handel en Energie/water/afval.

Ondanks dat niet veel bedrijven slagen voor de categorie HTTPS, is in figuur B.3.1(a) toch te zien dat ruim 93 procent van alle bedrijven met website met twee of meer werknemers HTTPS beschikbaar heeft op de website. Figuur B.3.1(b) toont dat dit min of meer gelijkmatig over de bedrijfstakken verdeeld is.

Één van de testen binnen de categorie HTTPS waar bedrijven slecht op scoren is het gebruik van HSTS, zoals in figuur B.3.4 te zien is. HSTS staat voor 'HTTP Strict-Transport-Security HTTP-header' en laat browsers weten dat een website alleen met HTTPS benaderd moet worden en 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 2 of meer werknemers slaagt in april 2024 maar 13,4 procent voor deze test (zie figuur B.3.4(a)). Het is waarschijnlijk deze test de uitkomst voor de totale categorie HTTPS bepaalt, omdat de verdeling van de slagingspercentages over de bedrijfsgrootteklasse en -takken voor de categorie HTTPS en de subtest HSTS sterk overeenkomen. De lage score op HSTS komt overeen de meting van [SIDN Lab \(2024\)](#): in figuur 2.3.1 is te zien dat in 2024 maar 16 procent van alle .nl-websites slaagt voor deze test.

Categorie Beveiligingsopties

Met beveiligingsopties wordt bedoeld het instellen van de juiste *Security Headers* om browsermechanismen te activeren om bezoekers te beschermen tegen aanvallen met bijvoorbeeld *cross-site scripting* (XSS) of *framing*. In 2020 slaagde nog ruim 10 procent van de grote bedrijven met 250 of meer werknemers voor deze categorie en 2,8 procent van alle bedrijven met twee of meer werknemers. Vanaf 2021 slaagde geen van gescande bedrijven

voor deze categorie, zodat de licht en donker blauwe staafje niet meer zichtbaar zijn. Dat geen van de bedrijven vanaf 2021 slaagde voor deze categorie komt doordat geen van de bedrijven slaagde voor één onderliggende subtest, namelijk de subtest 'Content-security policy', te zien in figuur B.4.3. Deze test is op 21 maart 2021 strenger geworden; waar het niveau van vereiste vóór deze datum nog optioneel was, is dat na deze datum verhoogd tot 'Aanbevolen' (Platform Internetstandaarden, 2021). Blijkbaar zijn er nog nauwelijks bedrijven die de subtest *Content Security Policy* volgens de laatste eisen voor hun website uitvoeren, waardoor ook de hele categorie 'beveiligingsopties' geen succesvolle resultaten oplevert.

De andere onderliggende subtesten van deze categorie vertonen nog wel een positieve trend over de jaren heen. Zo slagen over de jaren 2020, 2021 en 2022 steeds meer bedrijven met een website voor de subtest *X-frame-options* zoals getoond in B.4.1. Alle bedrijven met twee of meer werknemers stijgen van 12,1 procent in 2020 naar 15,7 procent in 2022. Alleen daalt het percentage van bedrijven dat slaagt voor deze test in 2023 naar 12,9, om vervolgens in de laatste scan van 2024 een lichte stijging te laten zien naar 14,3 procent. Verder slagen grote bedrijven vaker voor deze test dan kleine: van bedrijven met website met 250 of meer werknemers slaagt 29,7 procent tegen 12,9 procent van de bedrijven met website met 2 tot 10 werknemers.

Categorie autorisatie voor Routing (RPKI)

Als laatste wordt naar de categorie RPKI gekeken in figuur 3.2.6. Deze categorie test of een website een route-aankondiging heeft die kan worden gematcht aan de gepubliceerde route-autorisatie (RPKI). Deze categorie is pas in 2022 aan de web-scan door Internet.nl toegevoegd en er zijn daarom nog maar drie scans gemaakt waarin RPKI is meegenomen. De uitkomsten van de scans eind 2022 en begin 2023 zijn nagenoeg gelijk. De scan van begin 2024 laat wel een stijging zien bij alle bedrijfsgrootteklassen. Van alle bedrijven met website met 2 of meer werknemers slaagt bijna 80 procent voor deze categorie en geen van de andere bedrijfsgrootteklassen heeft een score lager dan 75 procent van de bedrijven met website (zie figuur 3.2.6(a)). Figuur 3.2.6(b) toont aan dat de bedrijfstak Energie/water/afval het hoogste scoort en dat geen van de bedrijfstakken een slagingspercentage onder de 68 procent voor de categorie RPKI heeft.

In figuren B.5.1 tot en met B.5.4 worden de resultaten van de onderliggende subtesten getoond. Deze waardes liggen allemaal boven de waarde voor de totale categorie. Dit komt doordat een website pas voor de hele categorie slaagt als zowel de website zelf als de *nameserver* een valide RPKI hebben. Het komt echter regelmatig voor dat alleen RPKI op de website geldig is en op de *nameserver* niet en vice versa, zodat de categorie RPKI minder vaak slaagt dan de onderliggende subtesten.

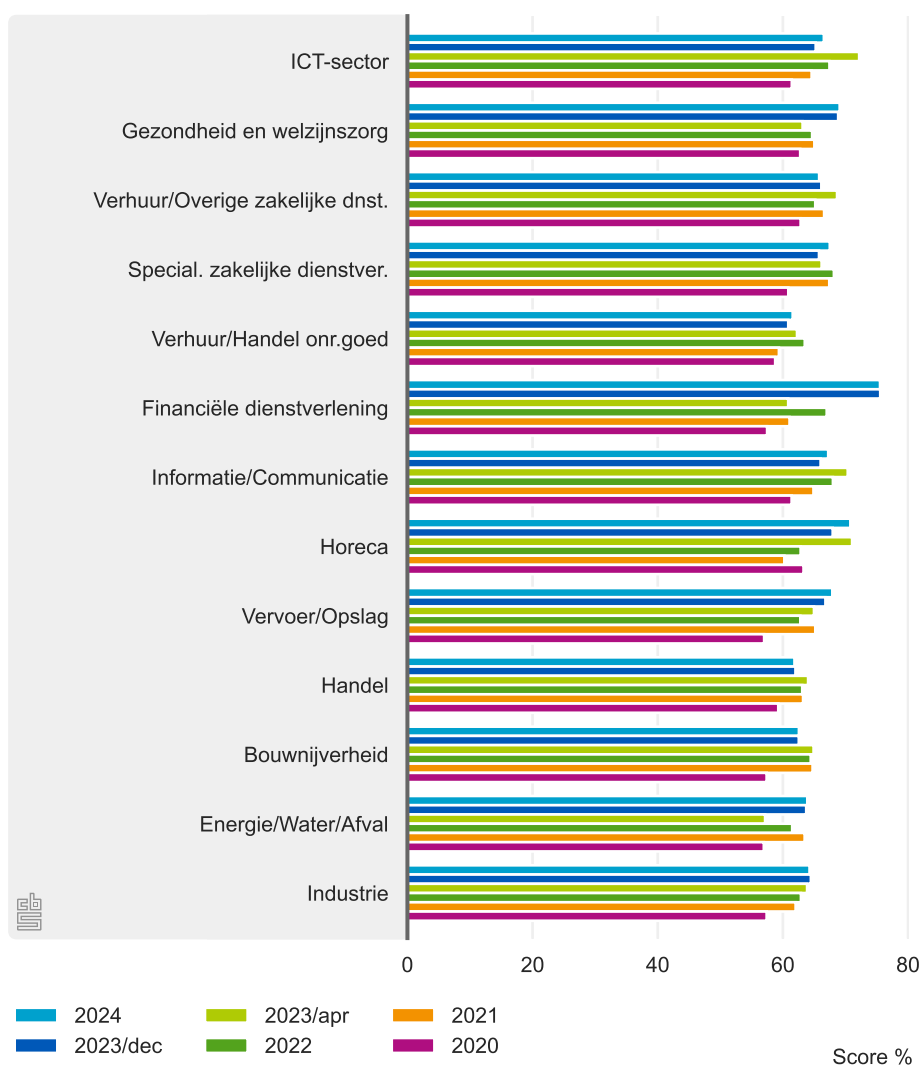
Als alleen naar de uitslag van een valide RPKI op de website gekeken wordt (figuur B.5.2) dan is te zien dat 80 procent van de bedrijven met een website een geldige RPKI op de website heeft. In figuur 2.3.1 kan teruggevonden worden dat SIDN Lab (2024) meet dat voor 11 januari 2024 zo'n 85 procent van alle .nl-websites een valide RPKI op de website heeft en dat na 11 februari 2024 dit percentage stabiel blijft voor alle .nl-websites. De Internet.nl scan was april, 2024 uitgevoerd; de resultaten voor RPKI op de website komen dus goed overeen.

3.2.1 Gemiddelde eindscore op Internet.nl per bedrijfsgrootteklasse (a) en bedrijfstak met 2 of meer werknemers (b).

(a) Bedrijfsgrootteklasse

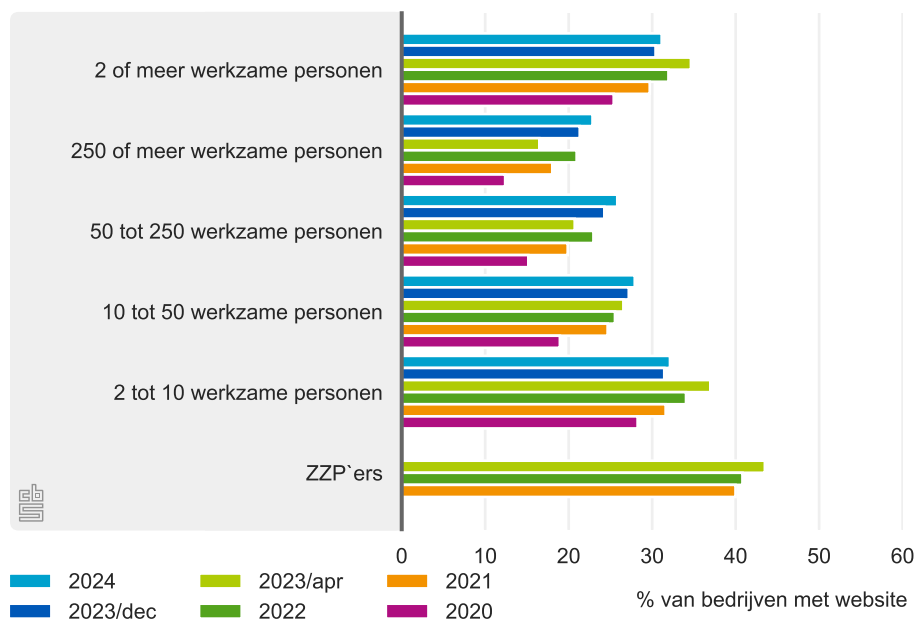


(b) Bedrijfstak

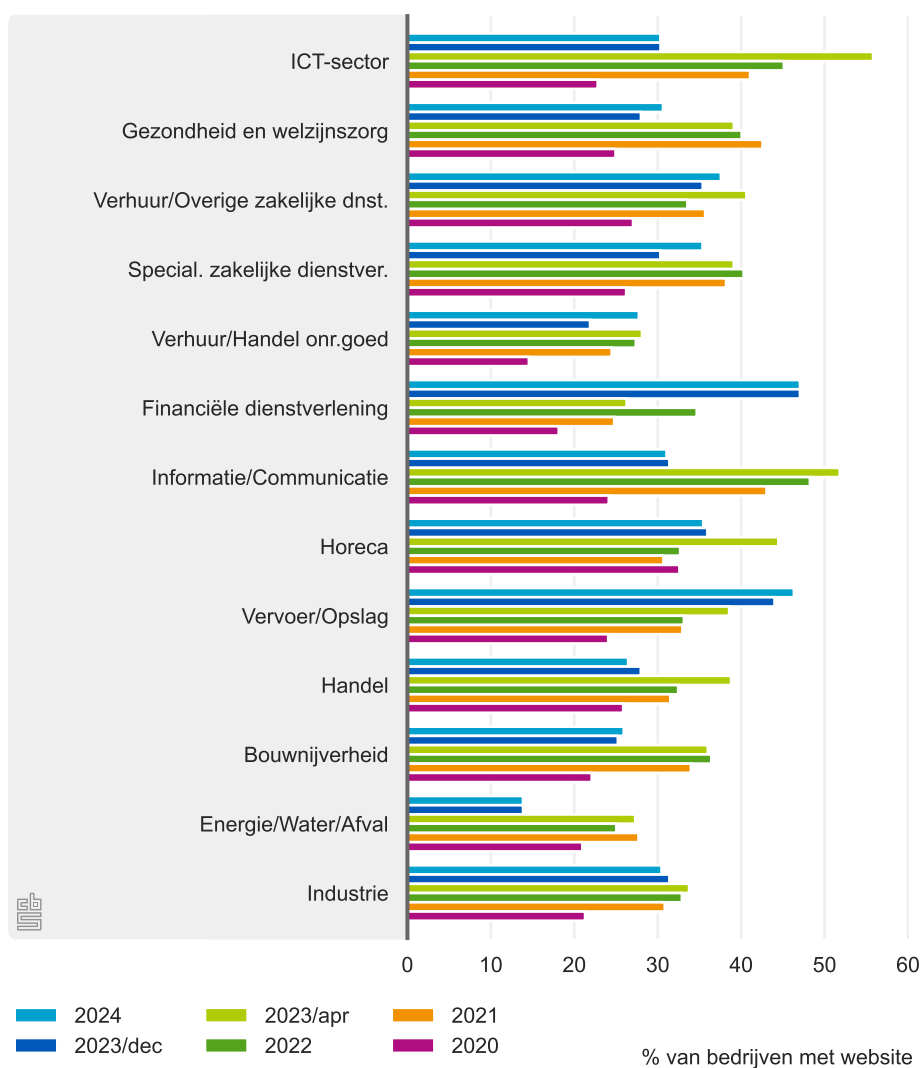


3.2.2 Percentage van bedrijven met website met geslaagde categorie 'IPv6' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse



(b) Bedrijfstak

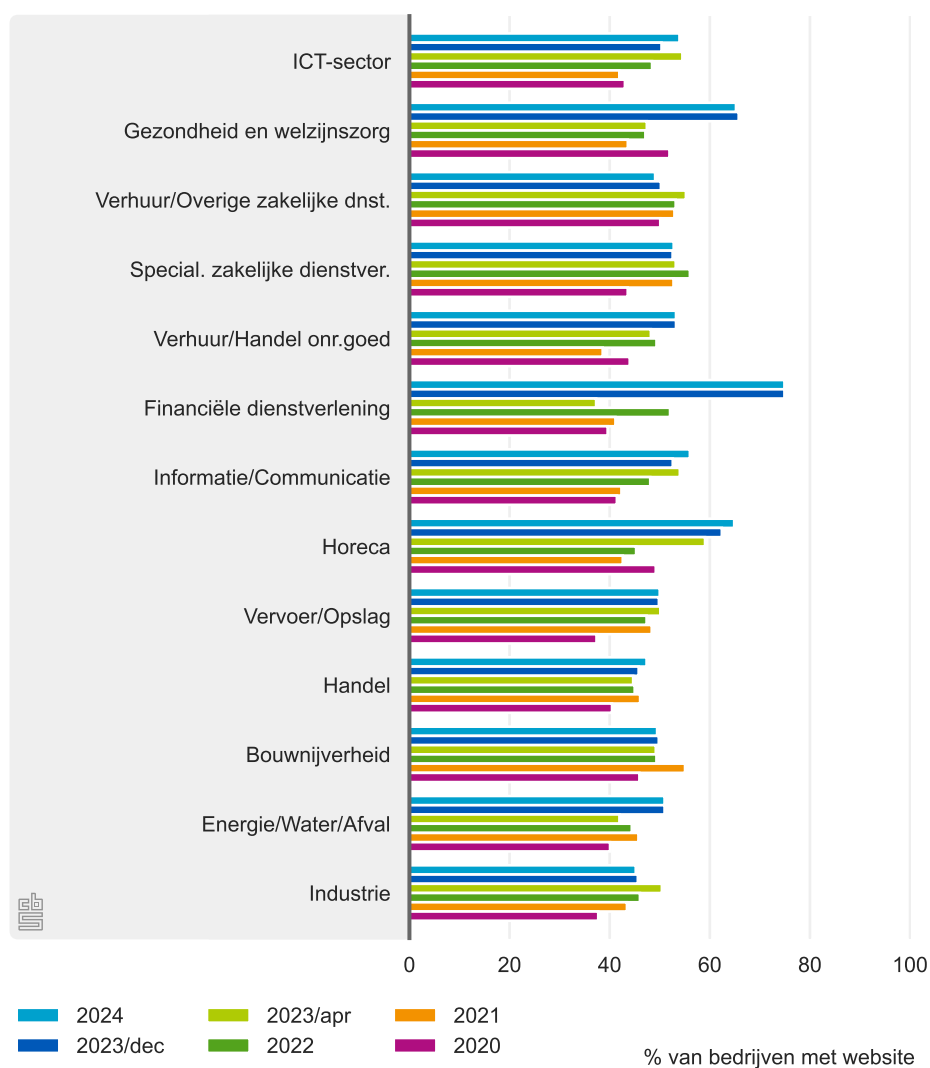


3.2.3 Percentage van bedrijven met website met geslaagde categorie `DNSSEC' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse

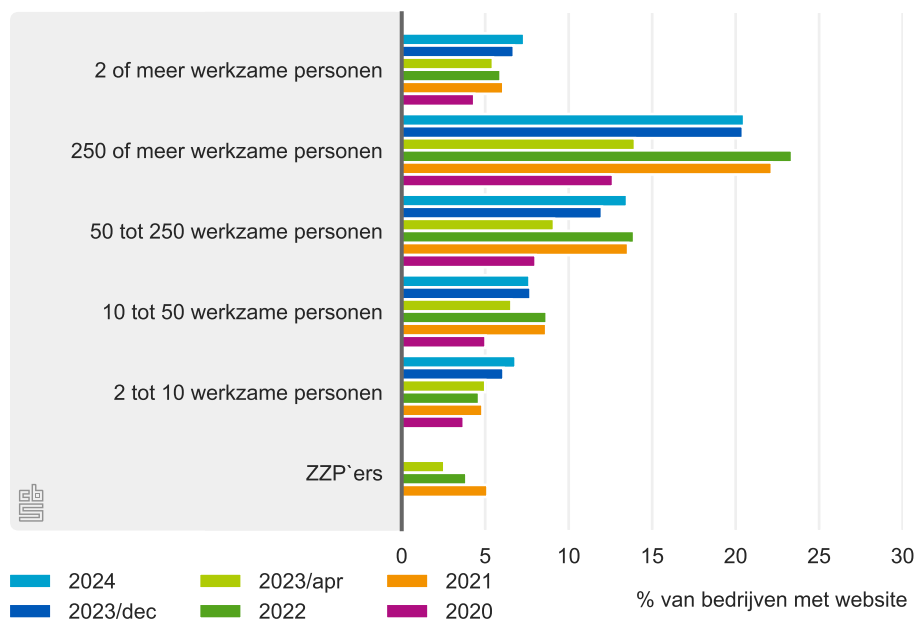


(b) Bedrijfstak

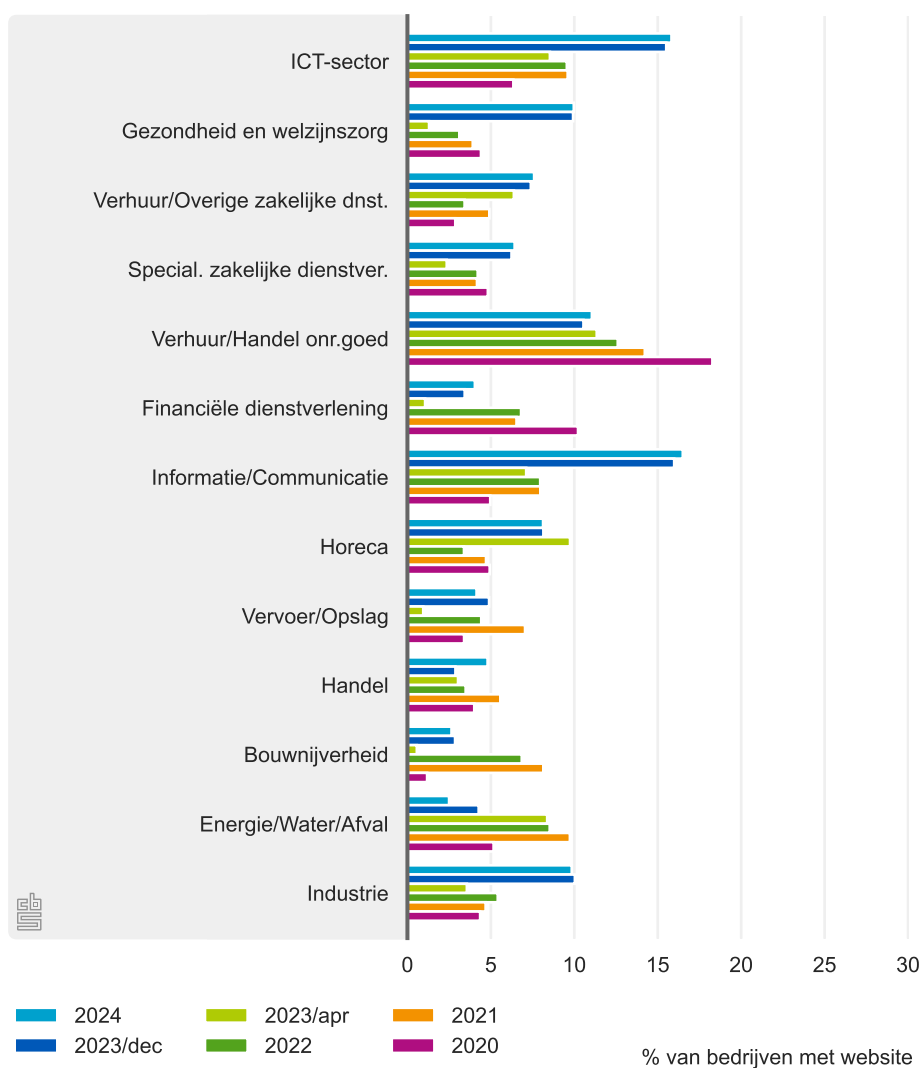


3.2.4 Percentage van bedrijven met website met geslaagde categorie 'HTTPS' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse



(b) Bedrijfstak

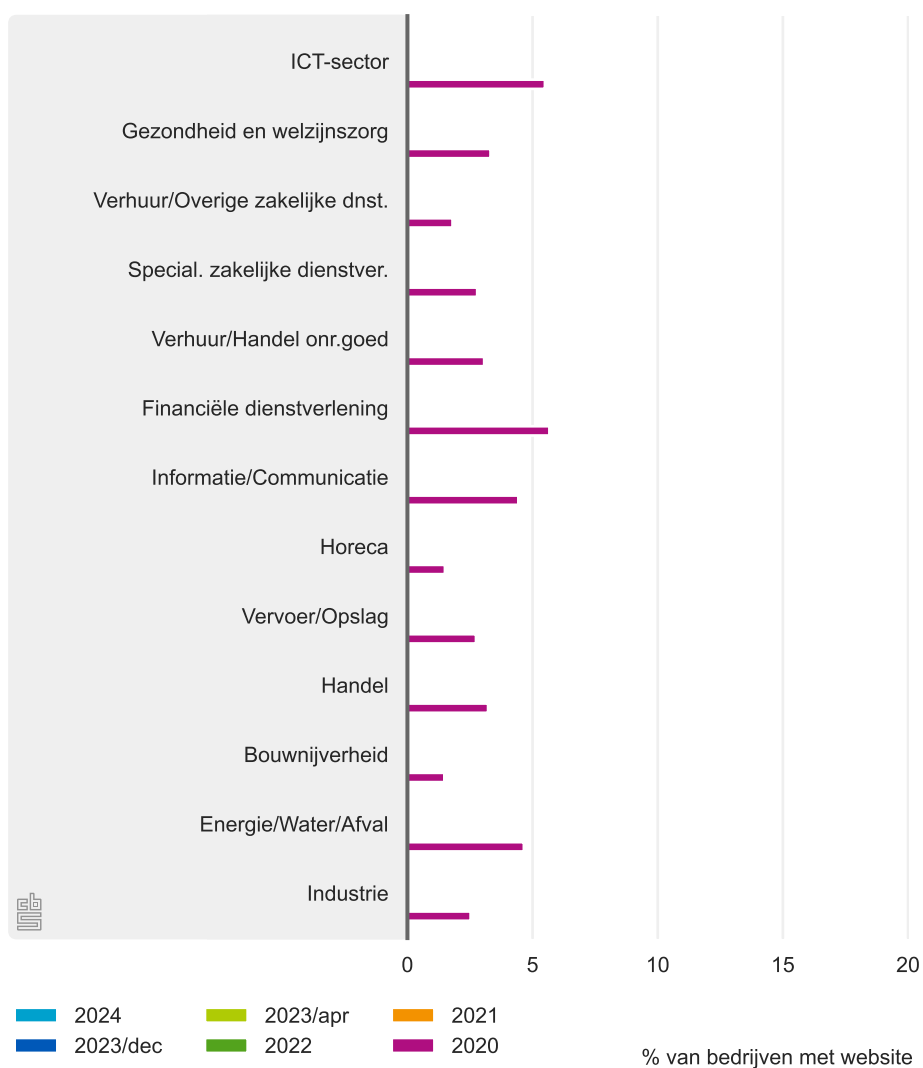


3.2.5 Percentage van bedrijven met website met geslaagde categorie 'Beveiligingsopties' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse

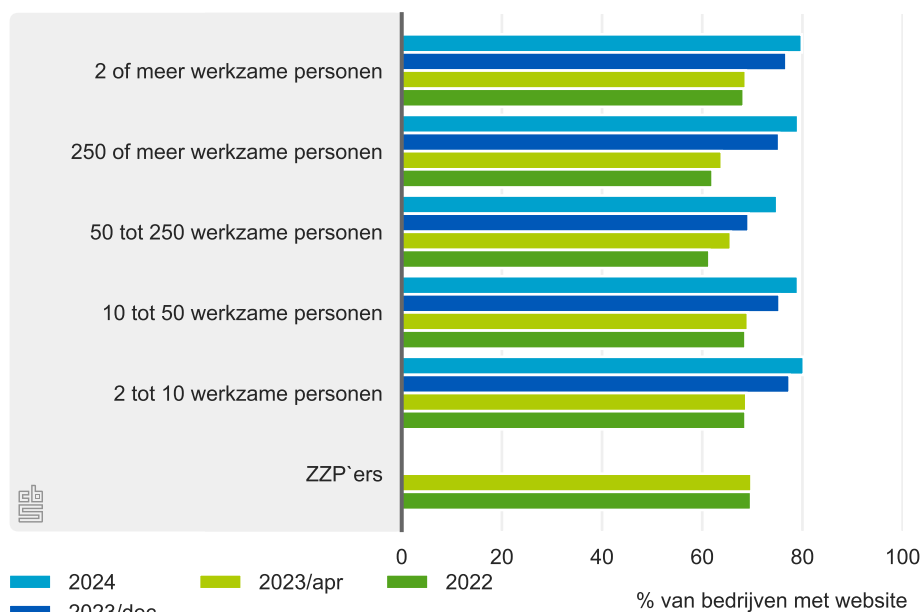


(b) Bedrijfstak

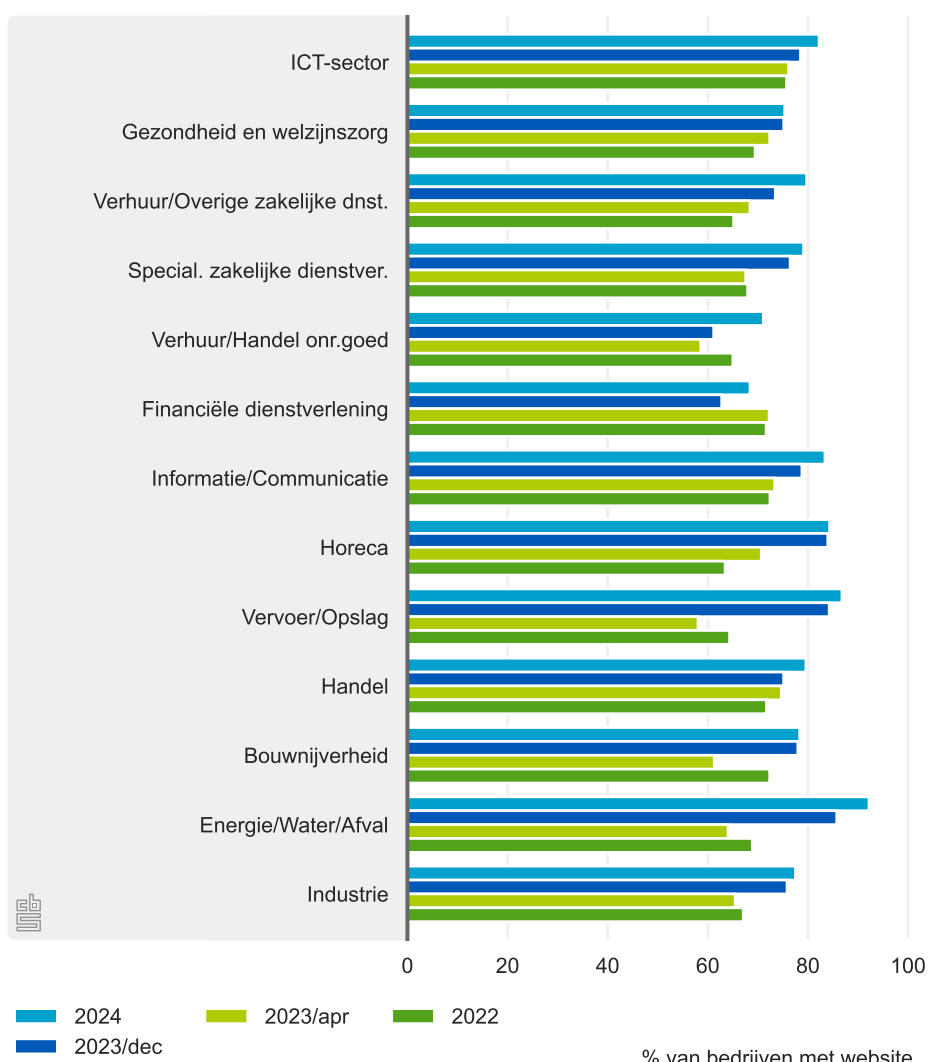


3.2.6 Percentage van bedrijven met website met geslaagde categorie 'Autorisatie voor routing (RPKI)' voor de Website-test per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse



(b) Bedrijfstak



3.3 Verdelingen van de eindscores van de websitescan van alle bedrijven

Alhoewel de gemiddelde score van alle websites van bedrijven in 2024 Nederland zo rond de 65 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 over alle bedrijven heen.

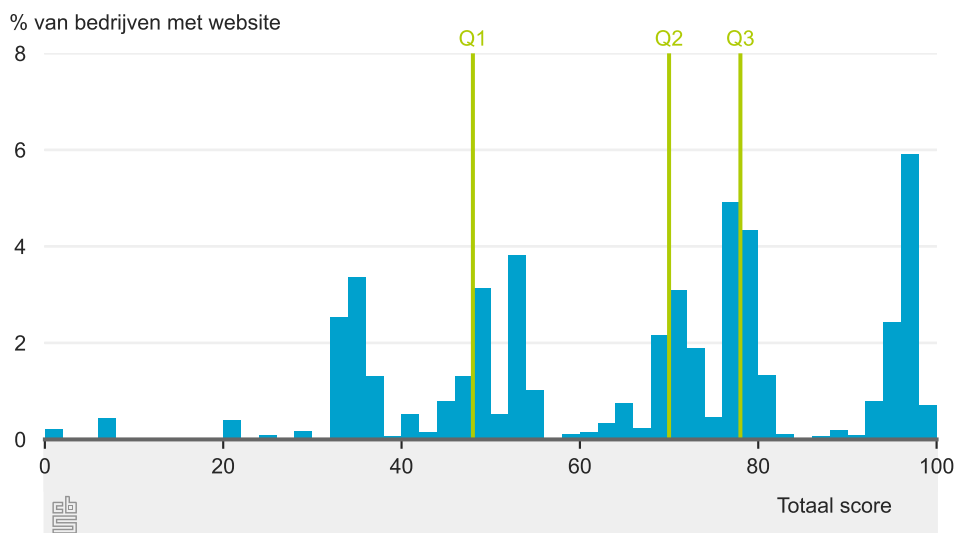
De verdeling van de eindscore voor alle bedrijven in Nederland is voor april 2024 te zien in figuur 3.3.1²⁾. De verdeling vertoont pieken rond de 30, 50, 70 en 90 procent. In figuur 3.3.1 zijn verder nog drie kwartielen Q1, Q2, en Q3 weergegeven. De verdeling van de overige jaren wordt in appendix B.6 gegeven (figuur B.6.1). In de verdeling van 2020 geeft het eerste kwartiel Q1 aan dat 25 procent van de bedrijven een eindscore lager dan 42 procent haalt. Het tweede kwartiel Q2 (de mediaan), geeft in 2020 aan dat de helft van alle bedrijven een score hoger dan 64 procent haalt. Het derde kwartiel geeft ten slotte aan dat 25 procent van de bedrijven een score hoger dan 76 procent haalt (in 2020).

In het voorgaand rapport (CBS, 2022c) werd aangetoond dat voor 2020 de pieken in de verdeling min of meer overeen komen met het aantal categorieën waarvoor een website geslaagd is. De spreiding rondom een piek wordt veroorzaakt door spreiding van het aantal geslaagde onderliggende subtesten. De scorebepaling is echter dynamisch en past zich aan aan de veiligheidseisen en bovendien is er een categorie bijgekomen. Inderdaad is te zien is dat de verdeling van de scores over de jaren daarom ook verandert. Meer bedrijven schuiven richting de 100 procent score op, wat blijkt dat de piek rond de 100 procent die toegenomen is.

Tabel 3.3.2 geeft de waardes voor de percentielen die in de figuren gevisualiseerd zijn. Inderdaad is te zien dat de 75 percentiel langzaam groter wordt; deze waarde geeft aan dat 75 procent van de bedrijven een score gelijk of lager dan dit percentiel heeft, of anders gezegd, dat 25 procent van de bedrijven een score hoger dan deze waarde heeft. In 2020 had 25 procent van de bedrijven een score die groter dan 76 was; in 2024 had 25 procent van de bedrijven een score die groter dan 78 was.

²⁾ De verdelingen van alle jaren worden in de appendix B.6 gegeven; de cijfers van de percentielen zijn wel in tabel 3.3.2 terug te vinden

3.3.1 Verdeling van de website-scan Internet.nl-score in april 2024



3.3.2 Percentielen van scoreverdelingen van de website-scans

Percentiel	2020	2021	2022	2023/apr	2024
25	42	48	48	48	48
50 (mediaan)	64	70	70	70	70
75	76	80	92	94	78

3.4 Welke bedrijven hebben de hoogste en laagste score voor de websitescan?

In figuur 3.4.1 en figuur 3.4.2 worden de bedrijven met hoogste scores voor de websitescan op Internet.nl weergegeven per bedrijfsgrootteklasse en bedrijfstak. Als gekeken wordt naar het percentage van bedrijven dat per bedrijfsgrootteklasse een eindscore van 90 procent of meer haalt (figuur 3.4.1(a)), dan is een duidelijke trend te zien: kleine bedrijven hebben vaker een eindscore van 90 procent of meer dan grote bedrijven. Naast deze constatering, kan ook geconcludeerd worden dat het aantal bedrijven met website met 2 of meer werknemers dat eindscore op Internet.nl haalt van 90 procent of meer gestaag toeneemt. In 2020 haalde maar 13,6 procent van de bedrijven een score van 90 of meer, terwijl dat in 2024 ondertussen al bijna 20 procent is: een relatieve toename van bijna 40 procent in vier jaar.

De verdeling over de bedrijfstakken van de bedrijven die een Internet.nl eindscore van 90 procent of meer halen (figuur 3.4.1(b)) laat zien dat voor de laatste twee scans, de Financiële dienstverlening de best scorende bedrijfstak is, waarbij bijna helft van de bedrijven in 2024 een website heeft met een Internet.nl-eindscore van 90 procent of meer. Daarentegen is er bij de bedrijfstakken ICT-sector en Bouwnijverheid, die in de jaren 2021 tot en met 2023 de

sterkste stijging kenden, juist sprake van een jaardaling van respectievelijk 12 en 19 procentpunten in 2024.

In figuur 3.4.2 wordt gekeken naar het percentage bedrijven met website die een eindscore op Internet.nl van 100 procent haalt. Waar in figuur 3.4.1(a) 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 3.4.2(a) te zien dat deze trend voor bedrijven met een 100 procent score precies andersom is. Van de bedrijven met een website met 250 of meer werknemers haalde in 2024 4,3 procent een score van 100 procent op Internet.nl. Dus hoewel kleine bedrijven wel vaker goed score (met een score van 90 procent of meer), is te concluderen dat *als* grote bedrijven boven de 90 procent score, ze relatief vaker ook direct een 100 procent score halen. Een verklaring zit hem misschien in het feit dat grote bedrijven hun website op hun eigen server hosten, terwijl kleine bedrijven een website vaker bij een externe service provider zetten. Van een aantal internetstandaarden is bekend dat je die niet helemaal in eigen hand hebt, omdat je afhankelijk van de netwerkinstellingen van de server bent. Dit zou misschien kunnen verklaren dat het voor grote bedrijven beter mogelijk is om die 100 procent score te halen.

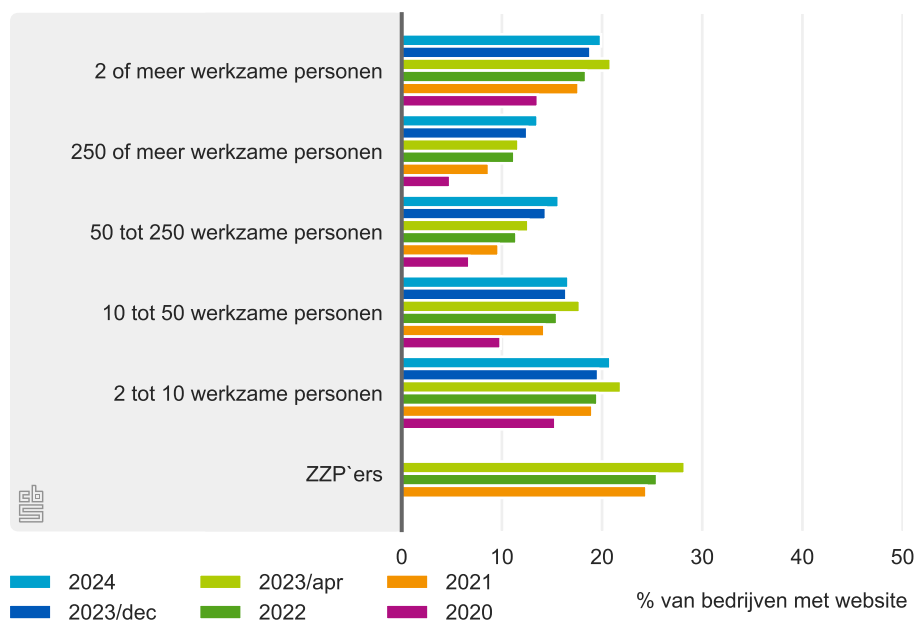
Figuur 3.4.2(b) laat de verdeling over de bedrijfstakken zien van de bedrijven met een website dat een Internet.nl eindscore van 100 procent haalt. Dit keer is te zien dat de verdeling niet te vergelijken is met de verdeling van de bedrijven die een score van 90 procent of meer halen. Waar vooral de bedrijven uit de Financiële dienstverlening goed vertegenwoordigd zijn bij 90 procent of meer, zijn juist de bedrijven uit de ICT-sector en Informatie/Communicatie die het meest prominent aanwezig zijn. Ruim 4 procent van de bedrijven met een website voldoet aan alle normen voor de internetstandaarden van Forum Standaardisatie.

Tot nu toe is aangetoond dat kleine bedrijven relatief vaker een score van 90 procent of meer halen dan grote bedrijven. Toch was eerder in figuur 3.2.1 geconstateerd dat de gemiddelde eindscore over alle bedrijfsgrootteklassen niet veel varieert, met gemiddelde eindscores voor alle bedrijfsgrootteklasse van rond de 65 procent. Dit impliceert dat kleine bedrijven ook vaker juiste een lagere score halen, zodat de gemiddelde eindscore voor grote en kleine bedrijven ongeveer gelijk is. In figuur 3.4.3(a) is te zien dat dit inderdaad het geval is: kleine bedrijven hebben relatief vaker een eindscore van 40 procent of minder dan grootte bedrijven. In 2024 had 19,2 procent van de bedrijven met website met 2 tot 10 werknemers een score onder de 40 procent tegen 8,4 procent van de grote bedrijven met website met 250 of meer werknemers. In de figuur is ook te zien dat voor bijna alle bedrijfsgrootteklassen het percentage bedrijven dat een score onder de 40 haalt zo goed als over de tijd afneemt. In ieder geval kan geconcludeerd worden dat de spreiding van de scores (die in figuur voor alle bedrijven in 3.3.1 getoond is) voor kleine bedrijven groter is dan voor grote bedrijven: kleine bedrijven hebben websites met zowel de laagste als de hoogste scores.

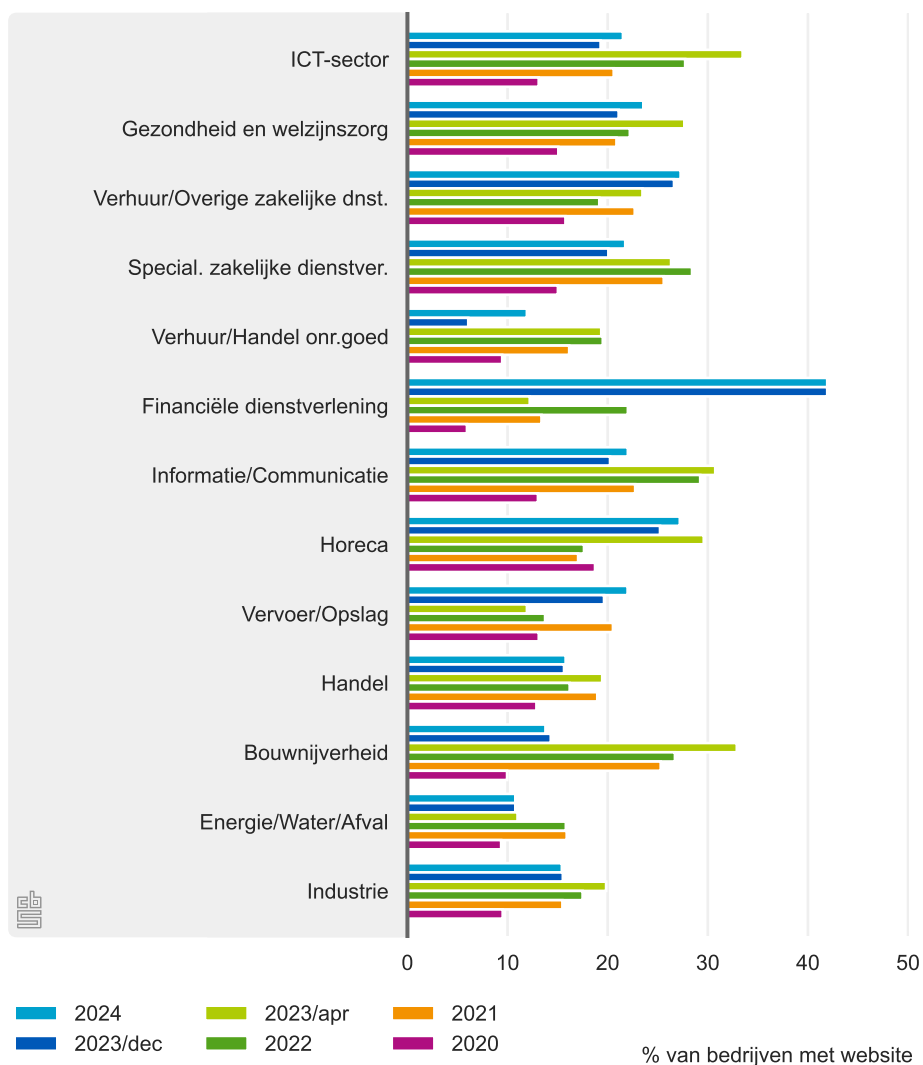
In figuur 3.4.3(b) laat zien dat per bedrijfstak er voor de Horeca zo'n zelfde conclusie te trekken is. Hoeveel de Horeca bij de groep met de hoogste scores zit, is de bedrijfstak ook hoog vertegenwoordigd met het aantal bedrijven met een website die een score van 40 of minder halen. Alleen voor de ICT-sector is te zien dat deze bedrijven niet alleen bij de best scorende bedrijfstak zitten, maar ook relatief minder vertegenwoordigd zijn in de groep van laag scorende bedrijven: slechts 14 procent van de bedrijven met een website uit de ICT-sector had een eindscore op Internet.nl van 40 procent of minder. Dit toont aan dat de spreiding van eindscores voor de ICT-sector klein is: bedrijven uit deze branche voldoen over het algemeen beter aan de normen voor de internetstandaarden voor websites dan gemiddeld, wat op zich niet gek is voor bedrijven die zich met ICT bezig houden.

3.4.1 Percentage van bedrijven met website met een eindscore op Internet.nl voor de websitescan van minimaal 90 procent per bedrijfsgrootteklasse (a) en bedrijfstak met 2 of meer werknemers (b).

(a) Bedrijfsgrootteklasse

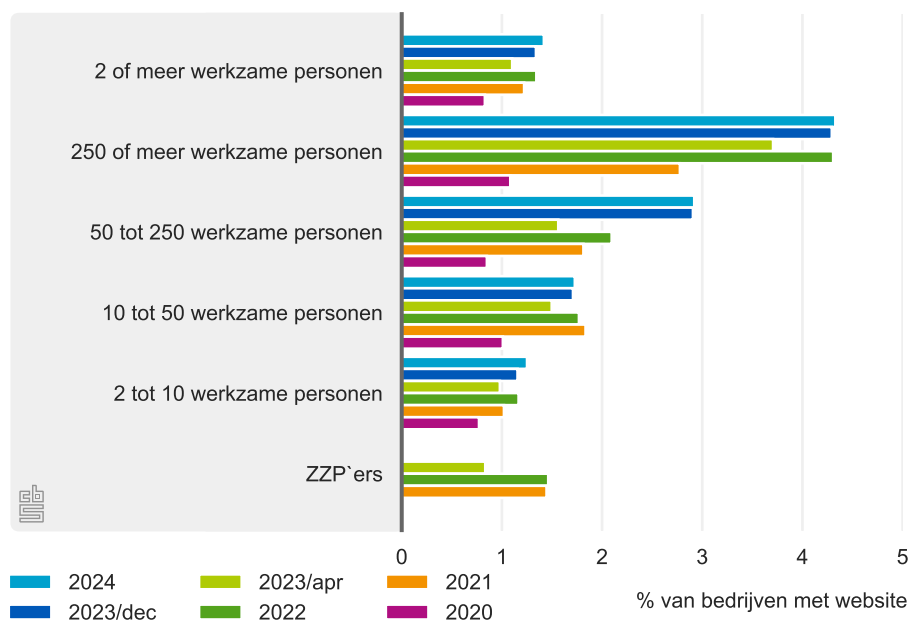


(b) Bedrijfstak

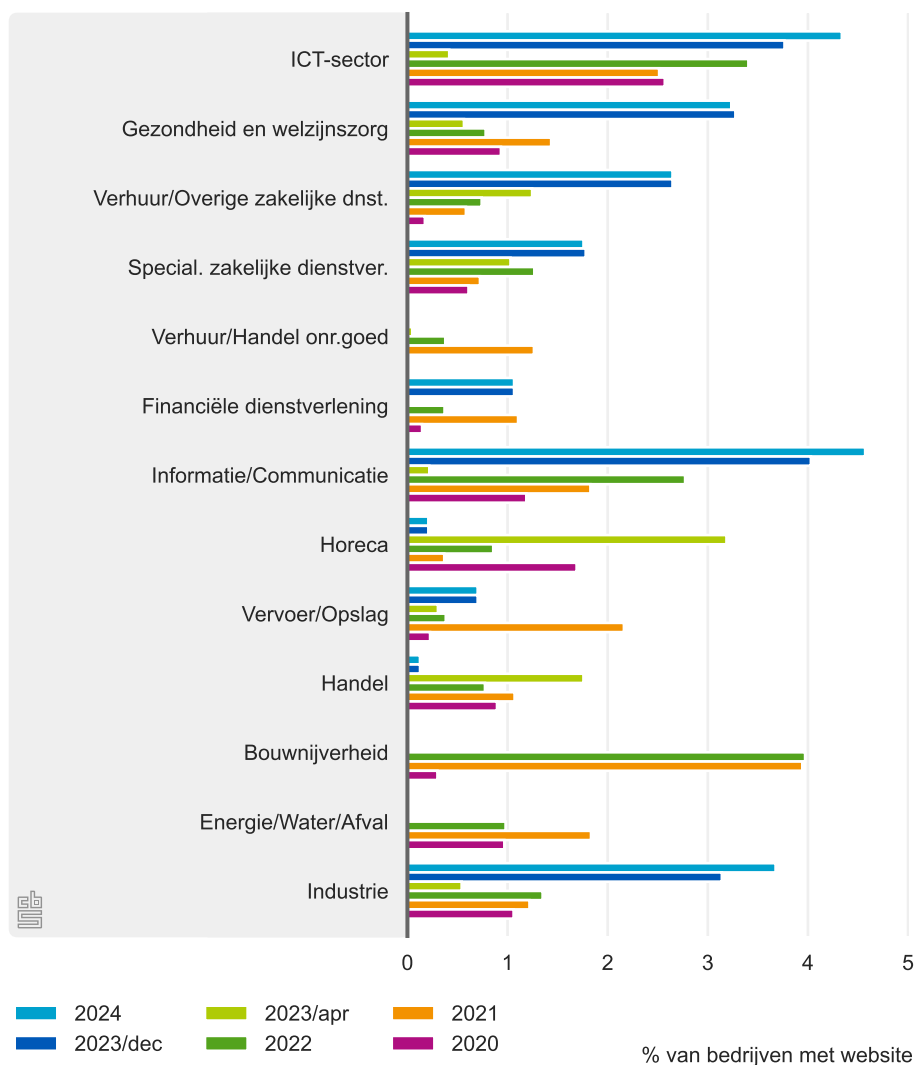


3.4.2 Percentage van bedrijven met website met een eindscore op Internet.nl voor de websitescan van 100 procent per bedrijfsgrootteklasse (a) en bedrijfstak met 2 of meer werknemers (b).

(a) Bedrijfsgrootteklasse

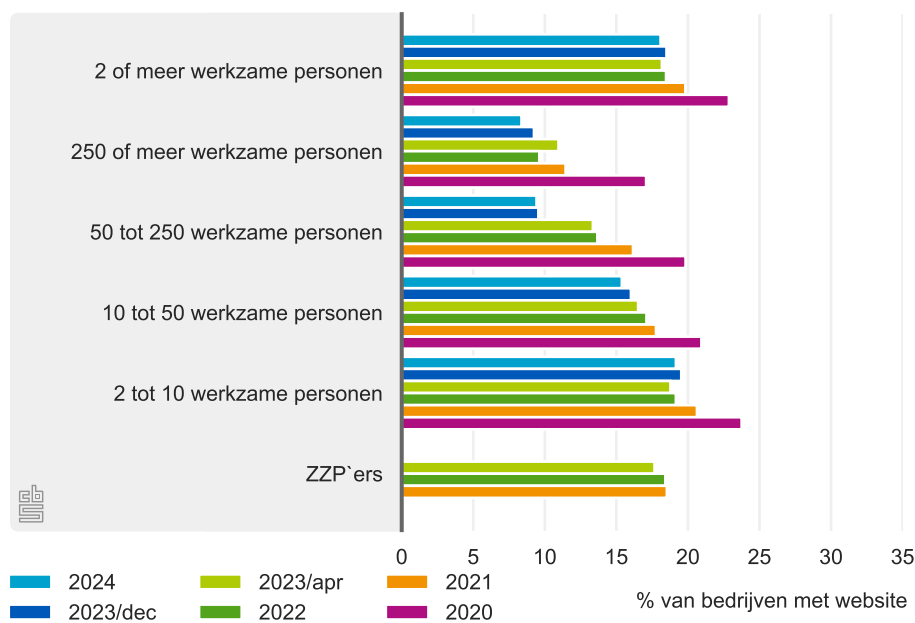


(b) Bedrijfstak

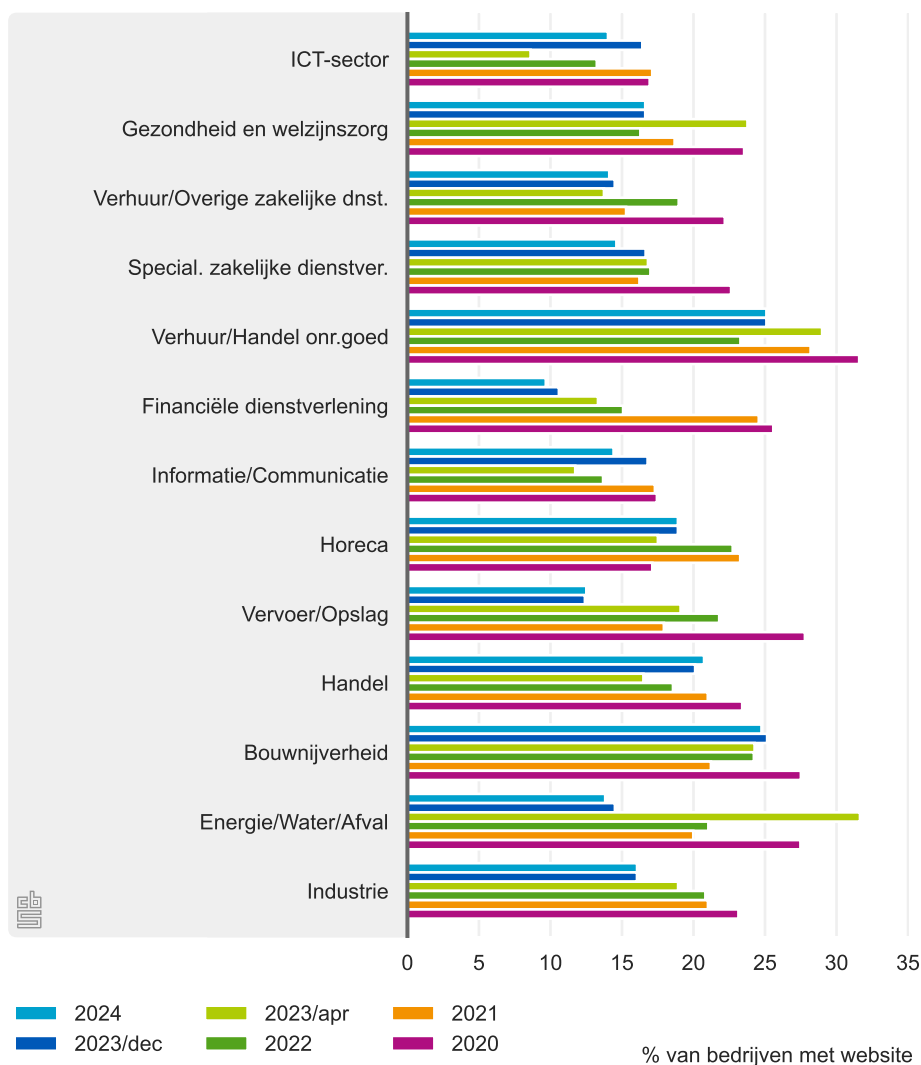


3.4.3 Percentage van bedrijven met website met een eindscore op Internet.nl voor de websitescan van 40 procent of minder per bedrijfsgrootteklasse (a) en bedrijfstak met 2 of meer werknemers (b).

(a) Bedrijfsgrootteklasse



(b) Bedrijfstak



4.

Resultaten

e-mailscans

4.1 Introductie

De scan van [Internet.nl](#) test of websites, mailservers en internetverbindingen aan de moderne internetstandaarden voldoen. In het vorige hoofdstuk is de analyse van de resultaten van de websitescans besproken. In dit hoofdstuk komen de resultaten van de e-mailscans aan bod. Van de e-mail zijn tot nu toe drie scans uitgevoerd, namelijk de scan van april en december 2023 en de scan van april 2024. Er kan daarom nog geen lange ontwikkeling besproken worden.

De e-mail-analyse van [Internet.nl](#) bevat vijf categorieën:

- [IPv6](#): bereikbaarheid via een modern internetadres.
- [DNSSEC](#): gebruik van een ondertekende domeinnaam.
- [Authenticiteit](#): protectie tegen e-mail phishing.
- [STARTTLS](#) en [DANE](#): beveiligde e-mail transport.
- [RPKI](#): Authenticiteit voor routing Applicatie-beveiligingsopties.

De laatste categorie is pas in 2022 toegevoegd. De score per categorie wordt bepaald met verschillende losse testen die binnen de categorie vallen. In dit hoofdstuk worden de resultaten per categorie gepresenteerd; in Appendix 4 worden de resultaten van alle onderliggende testen gegeven die per categorie uitgevoerd zijn. Een overzicht van de vijf categorieën met de bijbehorende subtesten kan in Tabel [A.3.1](#) gevonden worden.

In sectie [4.2](#) wordt eerst naar de gemiddelde Internet.nl-eindscores en de gemiddelde scores per categorie per bedrijfsgrootteklasse en bedrijfstak gekeken. Daarna wordt in paragraaf [4.3](#) nog de verdeling van alle eindscores laten zien.

4.2 Resultaten van Internet.nl per bedrijfsgrootteklasse en -tak

Eindscore niet afhankelijk van bedrijfsgrootte, wel van bedrijfstak

In figuren [4.2.1\(a\)](#) en [4.2.1\(b\)](#) wordt per bedrijfsgrootteklasse en bedrijfstak voor 2023 en 2024 de verdeling van de eindscores van e-mailscan via [Internet.nl](#) getoond. De gemiddelde eindscore per bedrijfsgrootte (figuur [4.2.1\(a\)](#)) is in beide jaren vrij constant over de bedrijfsgrootteklassen met een waarde van ronde de 60 procent. Figuur [4.2.1\(b\)](#) toont de gemiddelde eindscore per bedrijfstak. De gemiddelde eindscore varieert in 2024 van 58,1 procent voor de bedrijfstak 'Bouwnijverheid' tot 63,7 procent voor de bedrijfstak 'Horeca'. In meer dan de helft van de bedrijfstakken zijn de eindscores in 2024 gedaald in vergelijking met 2023, waarbij de grootste daling te zien is in de Bouwnijverheid.

Uitkomsten van de e-mailscan per categorie

De eindscore die nu bekeken is, wordt samengesteld uit de onderliggende testen zoals in tabel A.3.1 gegeven worden. Deze testen zijn in vijf categorieën opgedeeld: *IPv6*, *DNSSEC*, *STARTTLS Authenticiteit*, en *RPKI*. Als een bedrijf voldoende testen binnen een categorie goed heeft, zal de categorie van de e-mailscan door Internet.nl met 'geslaagd' aangeduid worden. In de figuren 4.2.2, 4.2.3, 4.2.5, 4.2.4 en 4.2.6 wordt voor de vijf categorieën het percentage van geslaagde bedrijven met website per bedrijfsgrootteklasse en bedrijfstak getoond. Terwijl de eindscores weinig per bedrijfsgrootteklasse en bedrijfstak variëren, is nu te zien dat er wel aanzienlijke verschillen per categorie zijn die we nu zullen bespreken.

De uitslag van een categorie wordt bepaald met de uitkomsten van de onderliggende testen die door een scan van Internet.nl uitgevoerd wordt. De uitkomsten van alle onderliggende testen worden in de appendix C gegeven in de figuren C.1.1 tot en met C.5.4. In deze figuren is terug te vinden voor welke testen de verschillen tussen de verschillende bedrijfsgrootteklassen ontstaan. Hieronder worden de resultaten per categorie besproken en waar nodig naar de belangrijkste subtesten verwezen.

Categorie IPv6

De categorie IPv6 geeft aan in hoeverre een mailserver bereikbaar is via een modern internetadres. Figuur 4.2.2(a). Gemiddeld slaagt 28,7 procent van de bedrijven met een website met 2 of meer werknemers voor de categorie IPv6. Opvallend is dat de score voor grotere bedrijfsgrootteklassen afneemt; zo slaagt van de bedrijven met 50 tot 250 werknemers nog maar 14,5 procent voor de categorie IPv6.

De uitsplitsing van de categorie IPv6 naar bedrijfstak, zoals weergegeven in figuur 4.2.2(b) laat zien dat Horeca de best scorende bedrijfstak is, met ruim 45 procent van de bedrijven die slagen voor deze categorie. Daarentegen presteert de Bouwnijverheid gemiddeld gezien aanzienlijk slechter op dit gebied, met slechts 10,2 procent van de bedrijven die slagen. In vergelijking met 2023 vertonen vrijwel alle bedrijfstakken in 2024 lagere scores, met uitzondering van de Financiële dienstverlening, die een stijging van ruim 7 procentpunten laat zien.

Categorie DNSSEC

De categorie DNSSEC geeft aan of het e-maildomein met een geldige handtekening ondertekend is. Figuur 4.2.3(a) laat zien dat 28,7 procent van de kleine bedrijven met 2 tot 10 werkzame personen slaagt voor de categorie DNSSEC. Bedrijven met website met 50 tot 250 werknemers zitten daar behoorlijk onder: 8,2 procent van deze groep slaagt in 2024 voor de categorie DNSSEC.

De categorie wordt in het geval van DNSSEC bepaald door maar vier onderliggende testen: DNSSEC aanwezig voor het e-maildomein (figuur C.2.1), DNSSEC geldig voor e-maildomein (figuur C.2.2), DNSSEC aanwezig voor mailserver (figuur C.2.3) en DNSSEC geldig voor mailserver (figuur C.2.4). Aan de subtesten is te zien dat voornamelijk laag gescoord wordt op de aanwezigheid van DNSSEC voor de mailserver.

Categorie Authenticiteit

Bij de categorie Authenticiteit wordt gekeken hoe goed bedrijven e-mailoplichting proberen te voorkomen door het toepassen van de juiste authenticatie mechanismes zoals DMARC, DKIM en SPF. Voor de categorie 'Authenticiteit', getoond in figuur 4.2.4, is het opvallend dat grote bedrijven een stuk beter scoren dan kleine bedrijven. Van alle bedrijven met website met 2 of meer werknemers slaagde 13,2 procent voor deze categorie. Dit lage percentage wordt voornamelijk veroorzaakt door de lage score voor kleine bedrijven. Zo slaagde slechts 11,2 procent van de bedrijven met website met 2 tot 10 werknemers voor de categorie 'Authenticate'. Grote bedrijven scoren in dit geval een stuk beter: 44,8 procent van de bedrijven met website met 250 of meer werknemers slaagt voor de categorie 'Authenticiteit'. De slagingspercentages per bedrijfstak getoond in figuur 4.2.4(b) laat dezelfde omkering zien; zo scoort de bedrijfstak 'Vervoer/Opslag' voor de categorieën IPv6 en DNSSEC relatief slecht (ten opzicht van de andere bedrijfstakken), terwijl het voor de categorie 'Authenticiteit' met 23,5 procent geslaagde bedrijven de beste scorende bedrijfstak is.

De onderliggende subtesten van de categorie Authenticiteit worden gegeven in de bijlage C sectie C.3. Per subtest wordt een stuk beter gescoord dan het resultaat van de hele categorie. Figuur C.3.1 en C.3.2 rapporteren hoeveel bedrijven DMARC (*Domain-based Message Authentication, Reporting, and Conformance*) toepassen. Met DMARC kunnen ontvangende e-mailsystemen mails vertrouwen die door het bedrijf verstuurd worden. Het is te zien dat 50,3 procent van de bedrijven met website met twee of meer werknemers DMARC heeft (figuur C.3.1), maar slechts 13,6 procent van de bedrijven met website met twee werknemers heeft DMARC met een voldoende strikt beleid (figuur C.3.2). Grote bedrijven met 250 of meer werknemers hebben DMARC het best op orde, met 44,1 procent van de grote bedrijven met website die DMARC hebben met een voldoende strikt beleid.

Ook DKIM (*DomainKeys Identified Mail*) wordt gebruikt om e-mails te authenticeren. Figuur C.3.3(a) laat zien dat 78,5 procent van de bedrijven met website met 2 of meer werknemers DKIM op hun mailserver heeft. Verder is te zien dat de verschillen tussen grote en kleine bedrijven klein zijn: Figuur C.3.3(b) laat zien dat de 'ICT-sector' voorop loopt met het gebruik van DKIM, alhoewel de verschillen per bedrijfstak verder ook bijna niet groot zijn.

Ten slotte laten figuur C.3.4 en C.3.5 zien welke bedrijven SPF gebruiken. SPF (*Sender Policy Framework*) wordt gebruikt om te valideren of uitgaande e-mails die vanaf het aangepaste domein verzonden worden, daadwerkelijk afkomstig zijn van de persoon die het zegt te zijn. Deze test valt ook in de categorie authenticiteit. Van de bedrijven met website met 2 of meer werknemers heeft 86,6 procent SPF op de server (figuur C.3.4(a)). De verschillen tussen de bedrijfsgrootteklassen zijn weer niet groot: van de kleine bedrijven slaagt 84,8 procent voor deze test, terwijl dat voor de grote bedrijven (250 of meer werknemers) 97,4 procent is. Figuur C.3.4(b) laat zien dat de sector 'Energie/water/afval' weer het meest van SPF gebruik maakt, met alle bedrijven met website die SPF gebruiken.

Figuur C.3.5 geeft weer aan welke deel van de bedrijven SPF ook met een voldoende strikt beleid gebruiken. Het gaat om dit geval om 79,6 procent van de bedrijven met website met 2 of meer werknemers die hier aan voldoet.

Dat grote bedrijven beter scoren op de categorie beveiligde e-mailtransport is goed te

begrijpen, omdat *e-mailspoofing*¹⁾ 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 ook meer imagoschade tot gevolg hebben, dus er is veel aan gelegen om zich hier zo goed mogelijk tegen te beschermen.

Categorie beveiligde e-mailtransport (STARTTLS en DANE)

Bij de categorie 'Beveiligde e-mailtransport' wordt gekeken in hoeverre verzendende mailservers die versleutelde e-mails versturen ook een beveiligde connectie met de mailserver van het bedrijf kunnen maken. STARTTLS voorkomt dat passieve aanvallers mails kunnen lezen terwijl de naar de mailserver onderweg is. Met DANE wordt bescherming tegen actieve aanvallers die proberen de STARTTLS te omzeilen door het e-mailverkeer te manipuleren. Figuur 4.2.5 toont per grootteklasse en bedrijfstak het percentage bedrijven dat slaagt voor deze categorie. In figuur 4.2.5(a) is te zien dat de van de bedrijven met website met 2 of meer werknemers 14,7 procent slaagt voor de categorie 'Beveiligde e-mailtransport'. Dit keer zijn de kleine bedrijven weer beste scorende bedrijfstagrootteklasse: 16,7 procent van de bedrijven met website met 2 tot 10 werknemers slaagt voor deze test. Van de grote bedrijven met website met 50 tot 250 werknemers slaagt slechts 3,1 procent van de bedrijven.

De onderliggende subtesten van deze categorie worden in bijlage C.4 gegeven. Zoals hiervoor bepaalt de slechts scorende subtest weer de uitslag van de categorie zelf. De testen die samenhangen met STARTTLS zijn niet beperkend: in figuur C.4.1 is bijvoorbeeld te zien dat rond de 91 procent slaagt voor de test 'STARTTLS beschikbaar voor de ontvangende mailserver'. De beperking wordt door de testen op DANE opgelegd. Figuur C.4.13 laat bijvoorbeeld zien dat maar 16 procent van de bedrijven met website met 2 of meer werknemers slaagt voor de STARTTLS test 'DANE bestaat' en dat dit voor bedrijven met 50 tot 250 werknemers zelfs slechts 4,6 procent is.

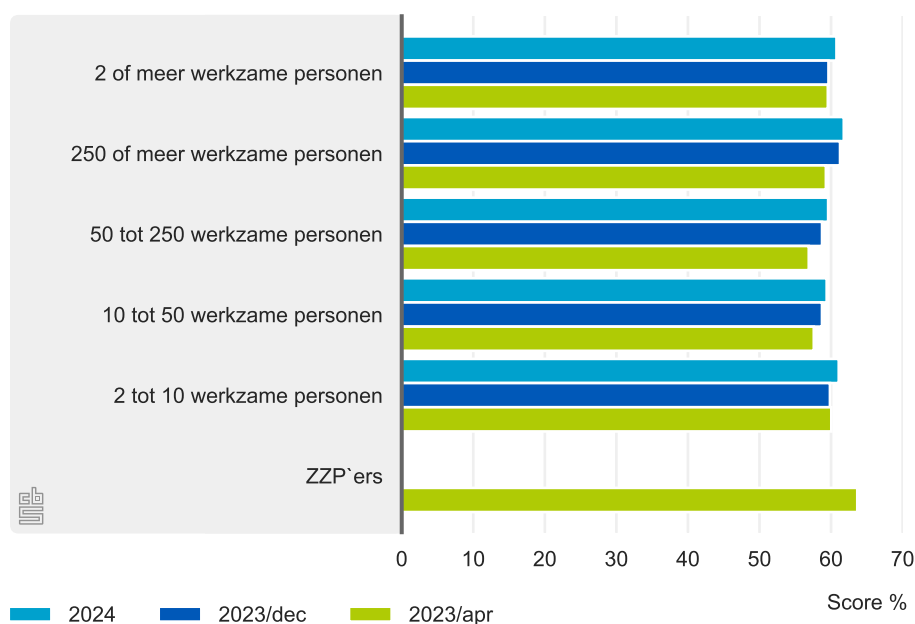
Categorie autorisatie voor Routing (RPKI)

Als laatste wordt naar de categorie RPKI gekeken in figuur 4.2.6. Deze categorie test of een website een route-aankondiging heeft die kan worden gematcht aan de gepubliceerde route-autorisatie (RPKI). Van alle bedrijven met website met 2 of meer werknemers slaagt 80,5 procent voor deze categorie (zie figuur 4.2.6(a)). Figuur 4.2.6(b) laat zien dat de 'Vervoer/Opslag' met 91,6 procent het meeste voor deze categorie slaagt. Geen van de bedrijfstakken komt onder de 60 procent.

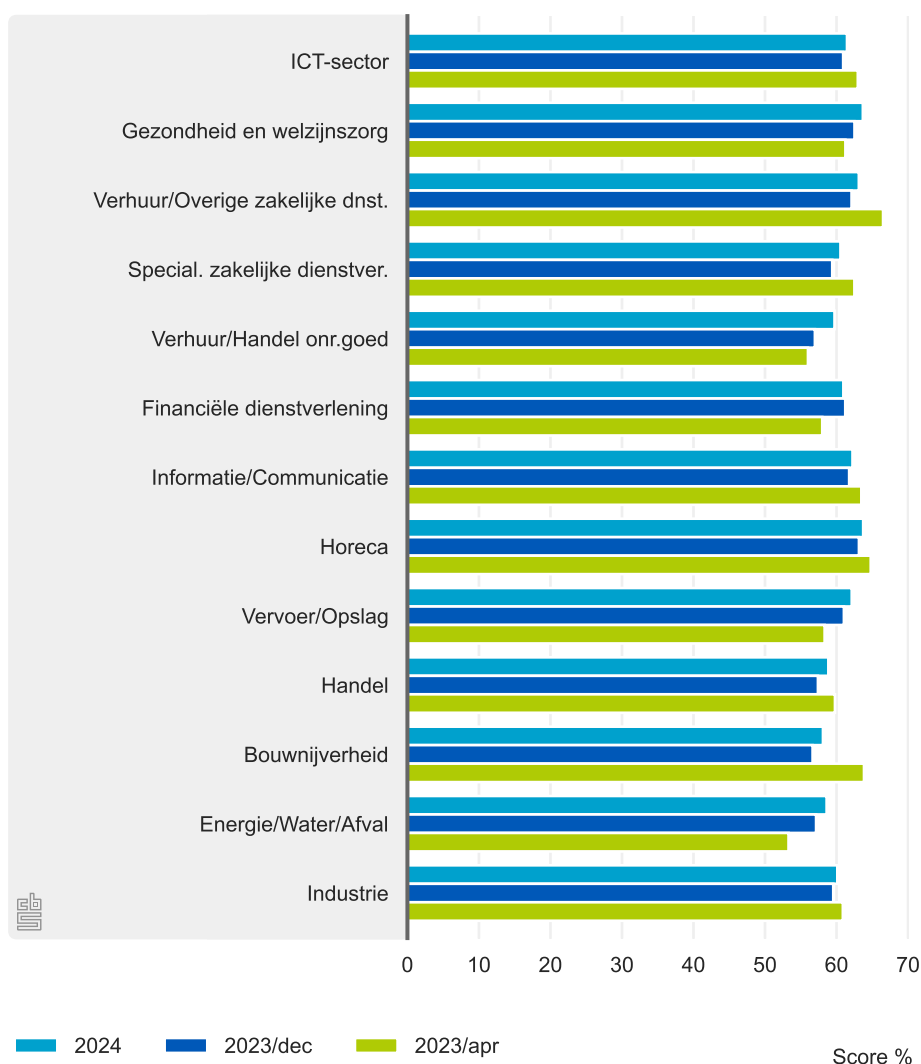
¹⁾ E-mailspoofing is een techniek gebruikt voor *spammail* en *phishing*-aanvallen om de e-mail van de verzender te vervalsen, zodat het lijkt alsof de mail door een ander bedrijf verstuurd is.

4.2.1 Gemiddelde eindscore op Internet.nl voor de e-mailtest per bedrijfsgrootteklasse (a) en bedrijfstak met 2 of meer werknemers (b).

(a) Bedrijfsgrootteklasse

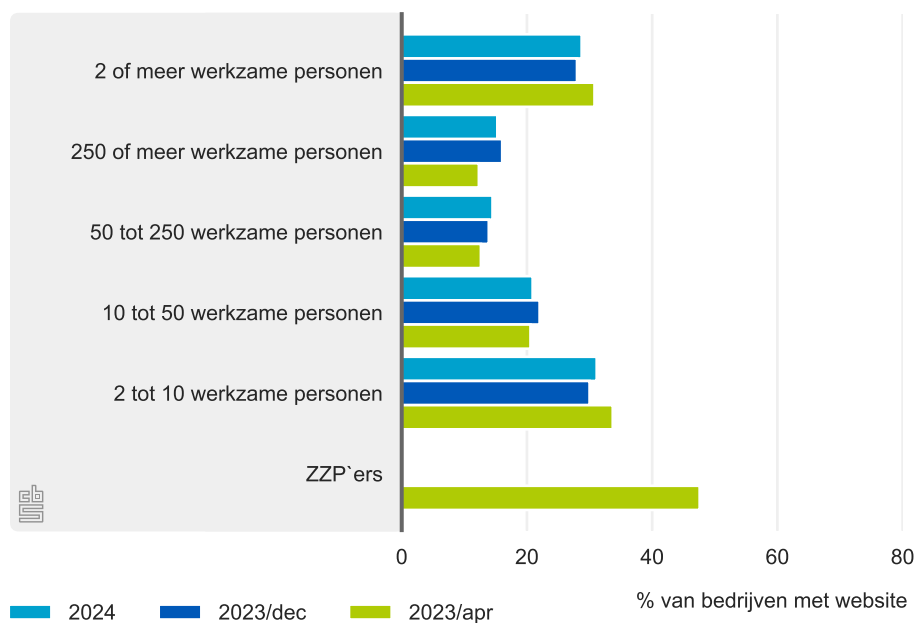


(b) Bedrijfstak

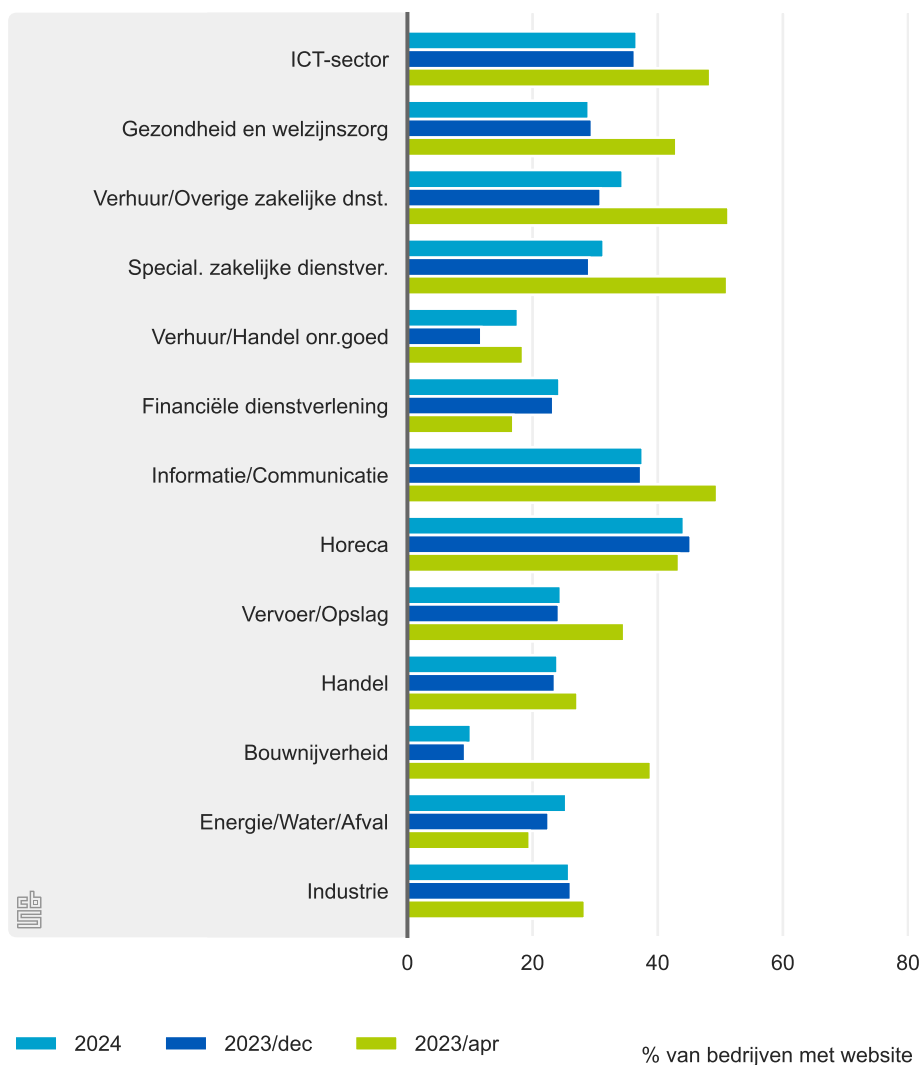


4.2.2 Percentage van bedrijven met website met geslaagde categorie 'Modern adres (IPv6)' voor de e-mailtest per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse

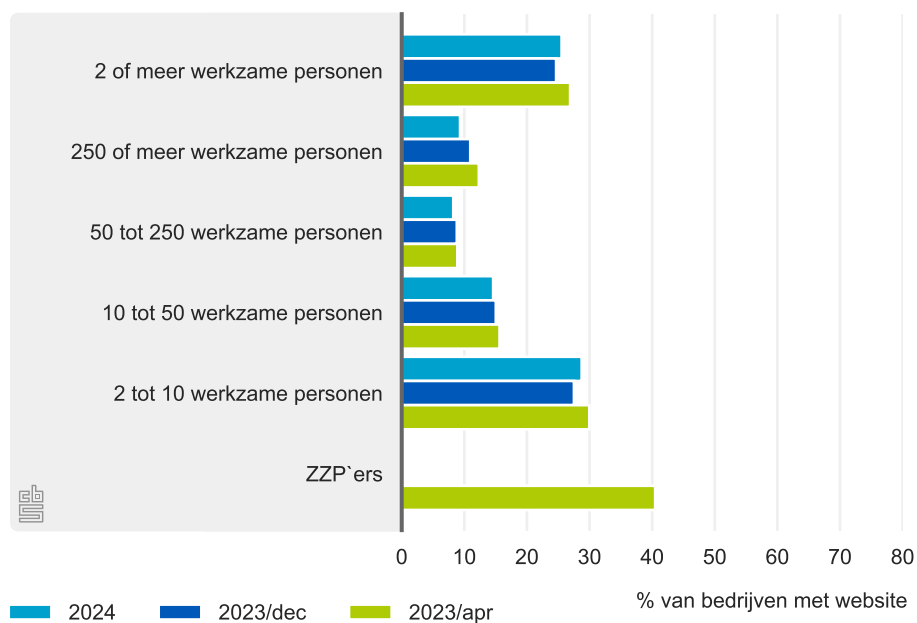


(b) Bedrijfstak

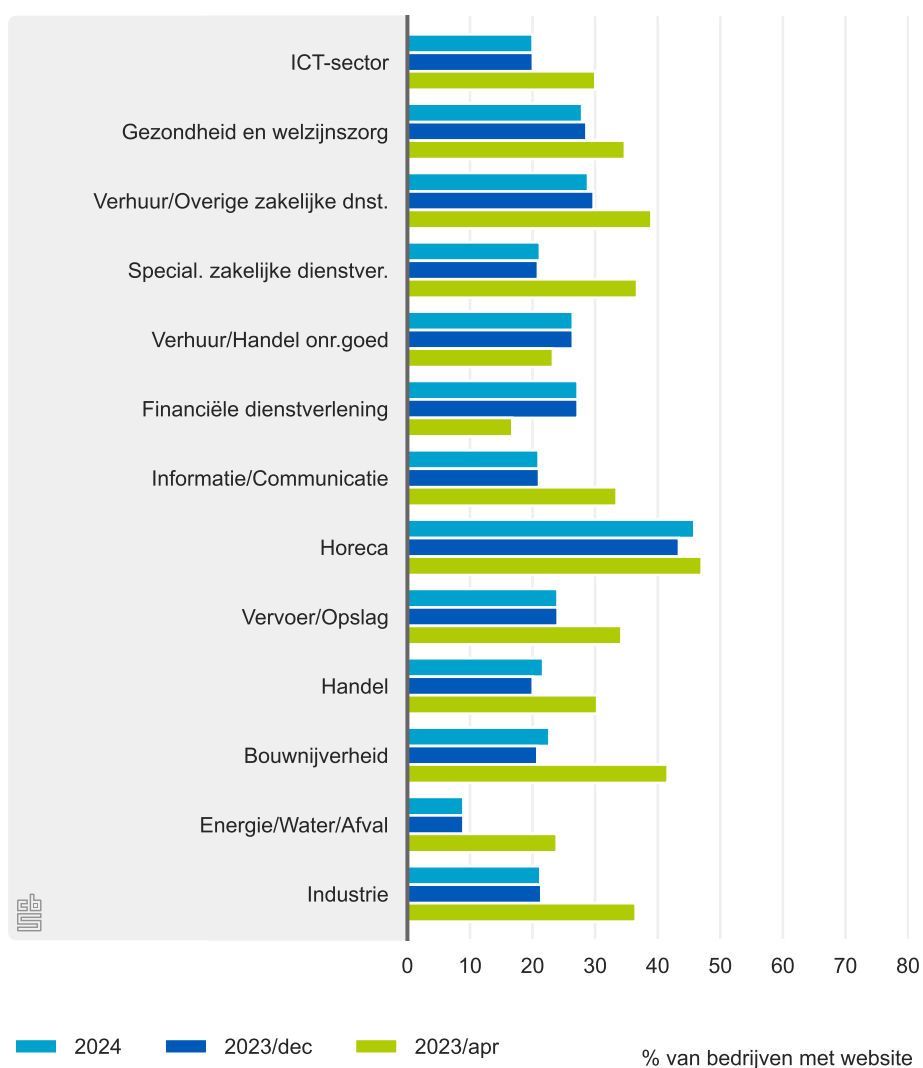


4.2.3 Percentage van bedrijven met website met geslaagde categorie 'Domeinnaamhandtekening (DNSSEC)' voor de e-mailtest per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse

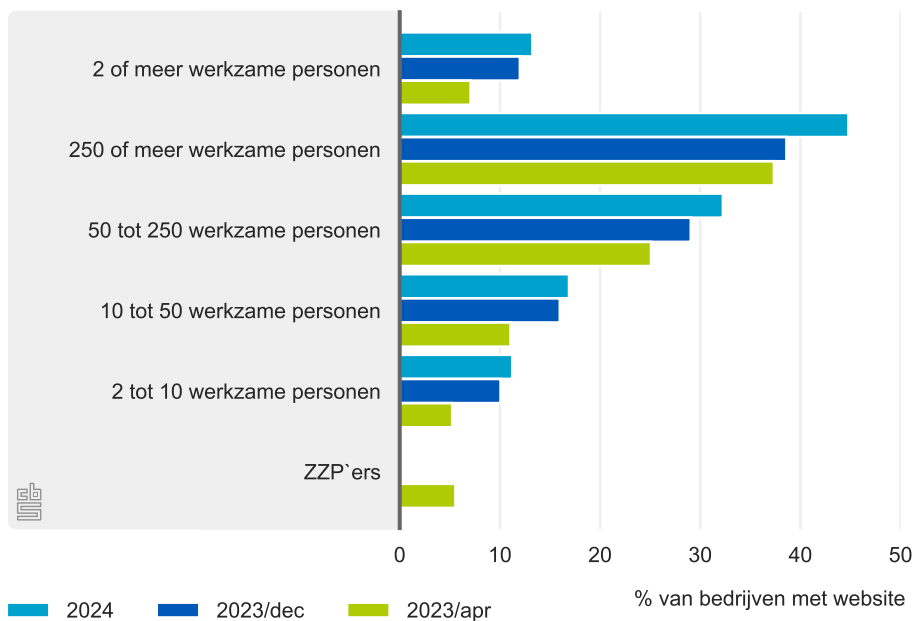


(b) Bedrijfstak

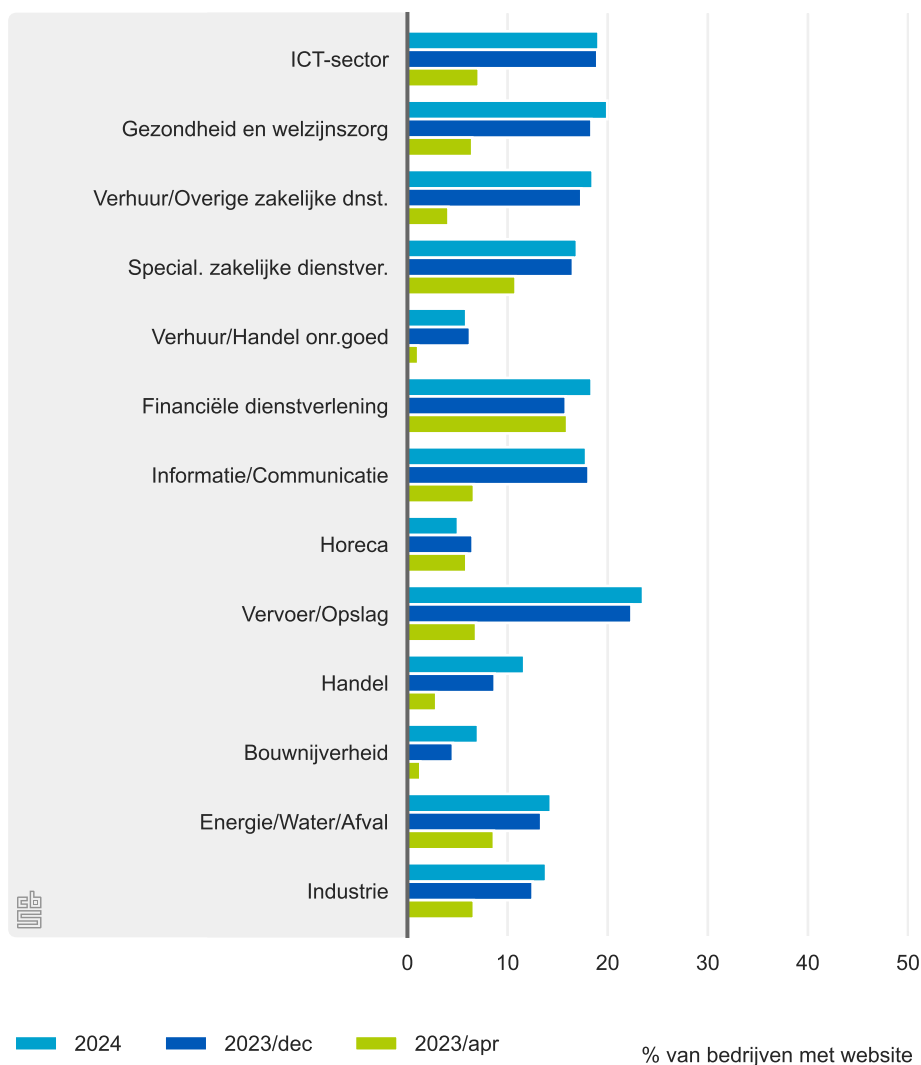


4.2.4 Percentage van bedrijven met website met geslaagde categorie 'Authenticatie' (DMARC, DKIM, SPF) voor de e-mailtest per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse

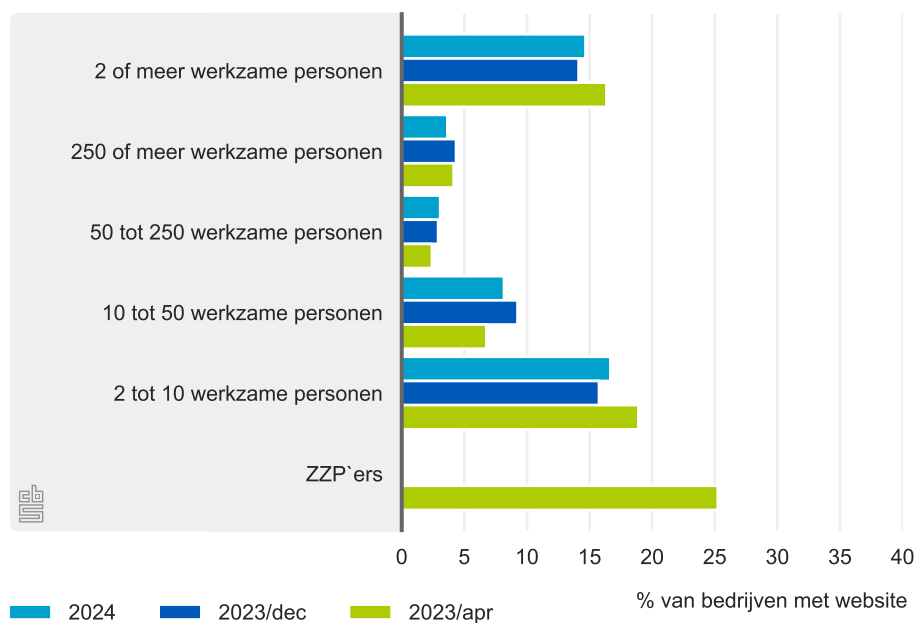


(b) Bedrijfstak

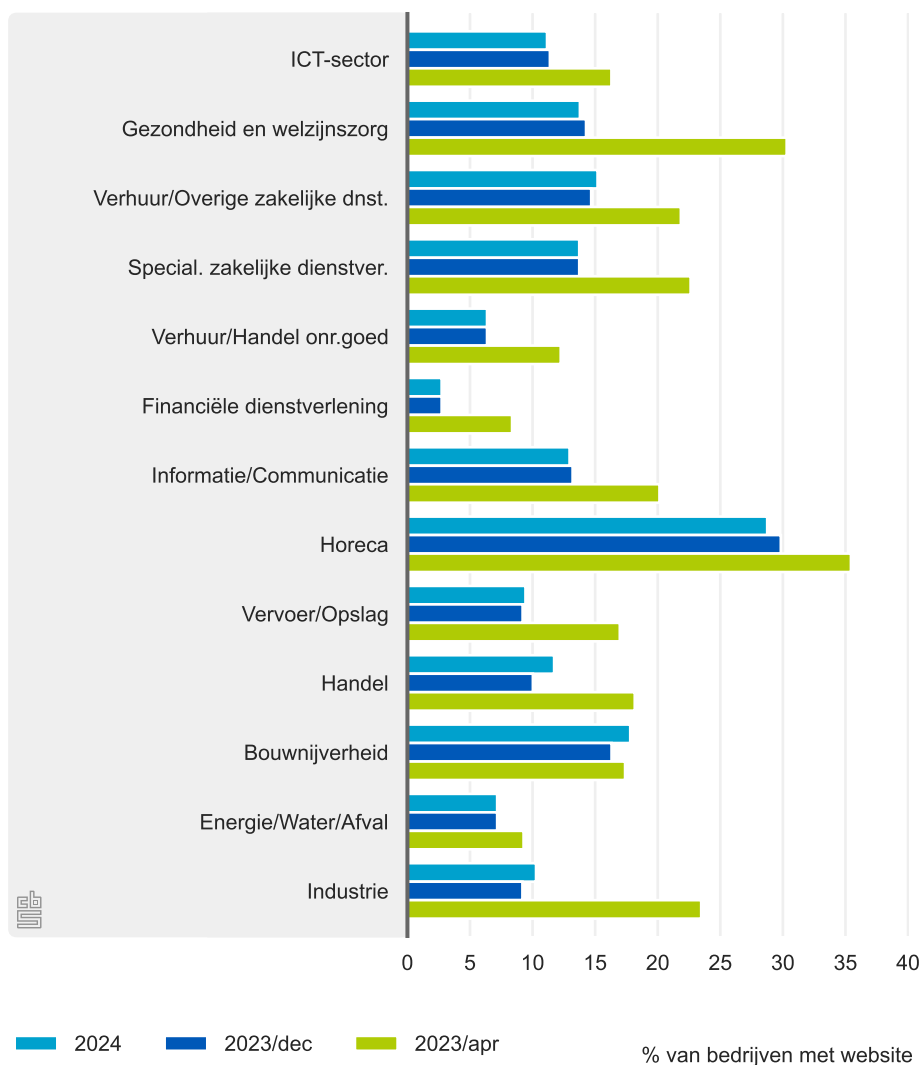


4.2.5 Percentage van bedrijven met website met geslaagde categorie `Beveiligde e-mailtransport (STARTTLS en DANE)` voor de e-mailtest per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse

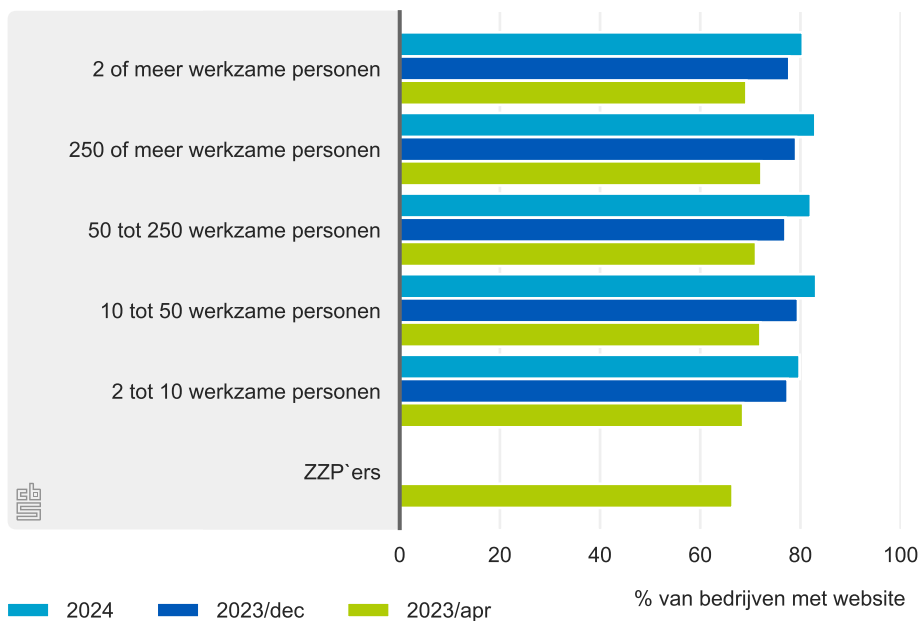


(b) Bedrijfstak

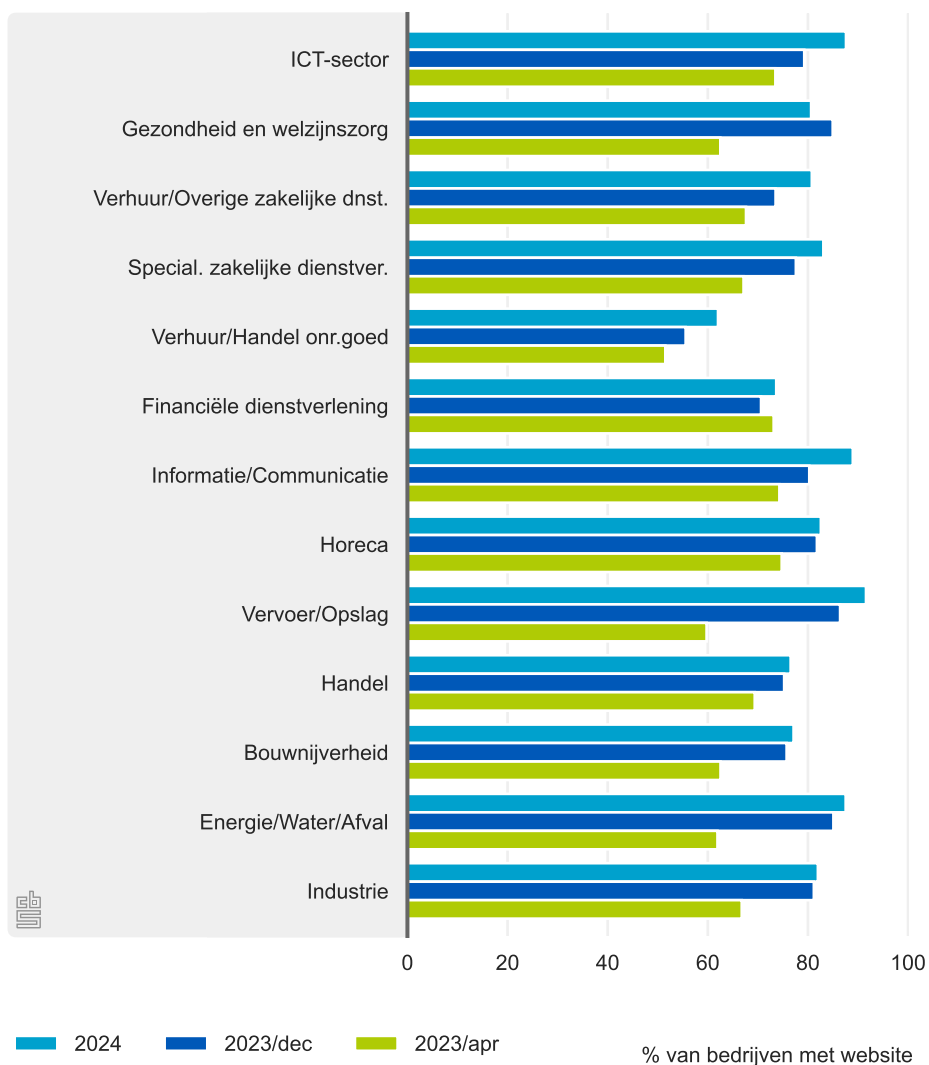


4.2.6 Percentage van bedrijven met website met geslaagde categorie 'Autorisatie voor routing (RPKI)' voor de e-mailtest per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse

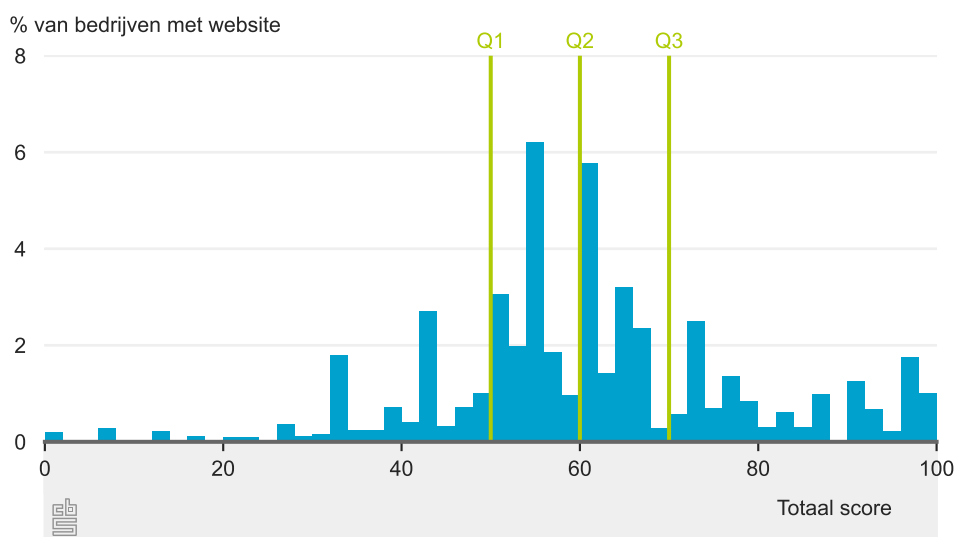


(b) Bedrijfstak



4.3 Verdelingen van de eindscores van de e-mailscan van alle bedrijven

4.3.1 Verdeling van de email-scan Internet.nl-score voor april 2024.



Alhoewel de gemiddelde score voor de e-mailscan van alle websites van bedrijven in Nederland zo rond de 60 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 van de e-mailscan over alle bedrijven heen.

4.3.2 Perctielen van scoreverdelingen van de Email-scans getoond in Fig. 4.3.1

Percentiel	2023/apr	2024
25	48	50
50 (mediaan)	70	60
75	94	72

De verdeling van de eindscores van de mail-scan van april 2024 wordt voor alle bedrijven in Nederland in figuur 4.3.1 getoond²⁾. In figuur 3.3.1 zijn verder nog drie kwartielen Q1, Q2, en Q3 weergegeven. De verdeling van de overige jaren wordt in appendix C.6 gegeven (figuur B.6.1).

4.4 Welke bedrijven hebben de hoogste en laagste score voor de e-mailscan?

In figuur 4.4.1 en figuur 4.4.2 worden tenslotte de bedrijven met hoogste eindscores voor de e-mails per bedrijfsgrootteklasse en bedrijfstak weergegeven. Net als bij de websitescan in sectie 3.4 is weer te zien dat kleine bedrijven vaker een score van 90 procent of hoger halen dan grote bedrijven (figuur 4.4.1(a)). Ruim één op de tien (11,0 procent) van de bedrijven met 2 tot 10 werknemers heeft een website met een eindscore voor de e-mailscan van 90 procent of meer, terwijl dat voor bedrijven met 50 tot 250 werknemers slechts 2,1 procent is. De verdeling over de bedrijfstakken van de bedrijven die een Internet.nl eindscore van 90 procent of meer halen (figuur 4.4.1(b)) laat zien dat de Horeca de best scorende bedrijfstak is, met 20,2 procent van de bedrijven met een website die een Internet.nl-eindscore voor de e-mailtest van 90 procent of meer halen.

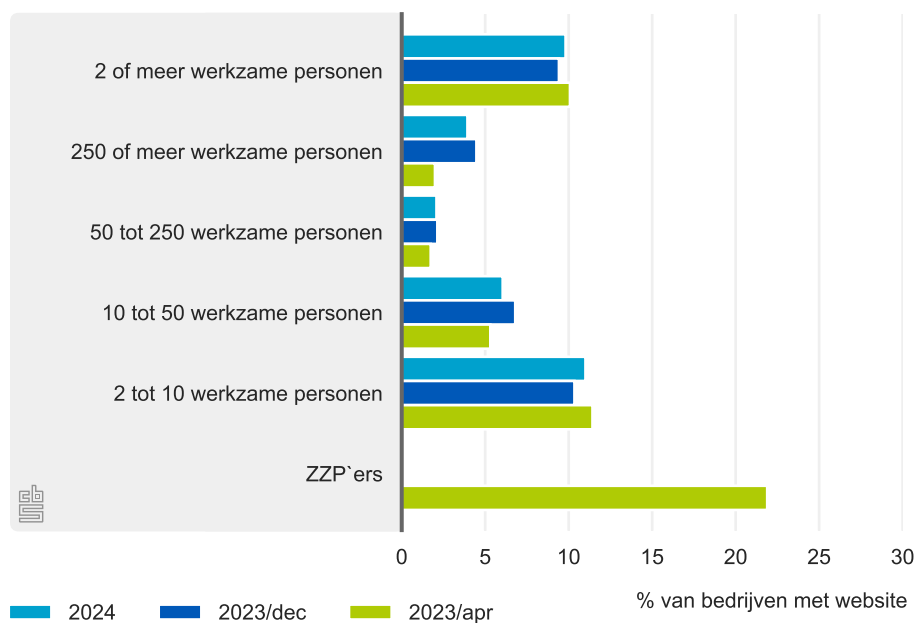
In figuur 4.4.2 wordt gekeken naar het percentage bedrijven dat een eindscore voor de e-mailtest op Internet.nl van 100 procent haalt. Per bedrijfsgrootteklasse (figuur 4.4.2(a)) is te zien dat nog maar heel weinig bedrijven een 100 procent score voor de e-mail server halen. Bedrijven met 10 tot 50 werknemers doen het met 2,4 procent van de bedrijven met een 100 procent score nog het best, maar gemiddeld haalt maar 0,5 procent van de bedrijven met een website met 50 tot 250 werknemers een 100 procent score voor de e-mailscan. Als naar de verdeling per bedrijfstak gekeken wordt (figuur 4.4.2(b)), is te zien dat met name de Vervoerssector hier nog het beste scoort: 4,4 procent van de bedrijven met een website in de 'Vervoer en opslag' halen een 100 procent score voor de e-mailtest op Internet.nl.

Ten slotte wordt in figuur 4.4.3(a) gekeken naar de bedrijven die juist laag scoren voor de e-mailtest op Internet.nl. Bijna 10 procent van de bedrijven met een website met 2 of meer werknemers heeft een eindscore voor de e-mailtest van 40 procent of minder. De groep is iets kleiner voor grote bedrijven, met maar 4,6 procent van de bedrijven met een website die een eindscore van 40 procent of minder halen voor de e-mail test. In figuur 4.4.3(b) is te zien dat 12,8 procent van de bedrijven met een website in de Financiële dienstverlening een eindscore van 40 procent of minder behaalt. Deze groep is niet alleen goed vertegenwoordigd bij de bedrijven met een 90 procent score of hoger, maar ook vrij ruim vertegenwoordigd bij de bedrijven met een lage score voor de e-mailtest.

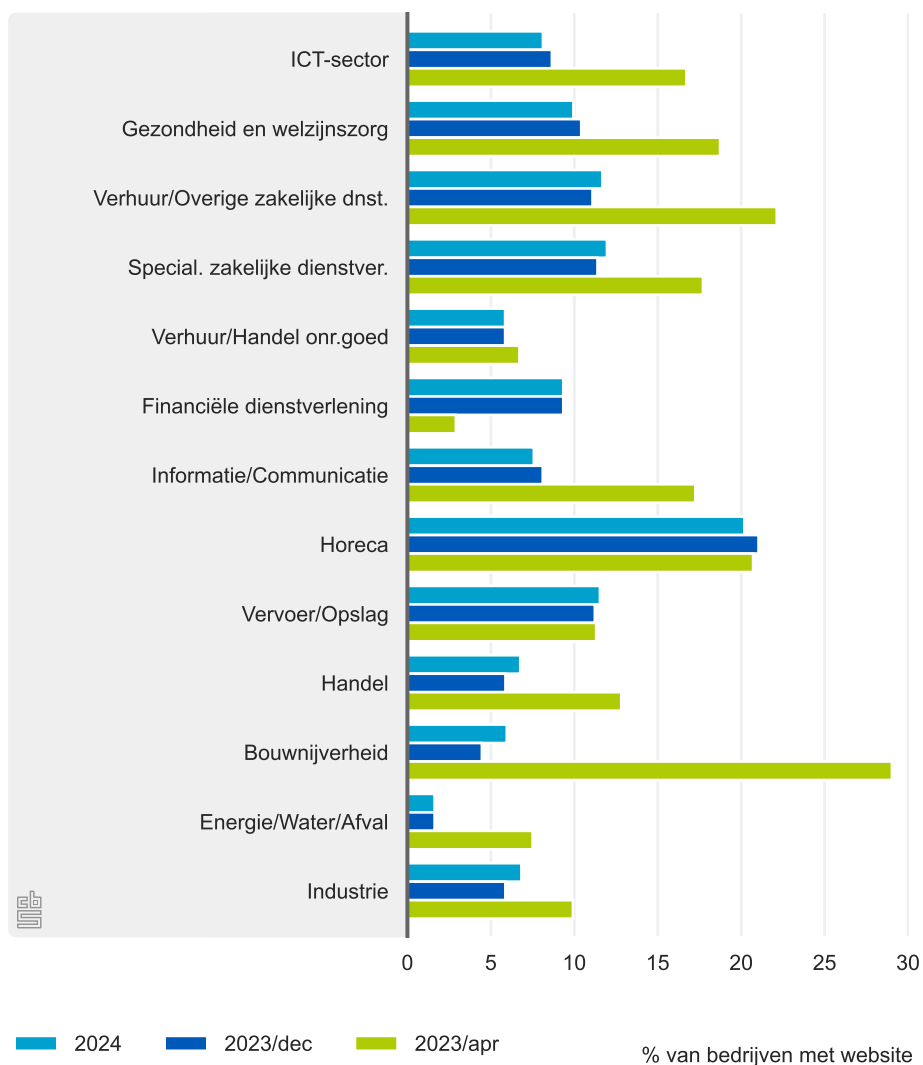
²⁾ De verdelingen van alle jaren worden in de appendix 4.3 gegeven; de cijfers van de percentielen zijn wel in tabel 4.3.2 terug te vinden

4.4.1 Percentage van bedrijven met website met een eindscore op Internet.nl voor de e-mailtest van minimaal 90 procent per bedrijfsgrootteklasse (a) en bedrijfstak met 2 of meer werknemers (b).

(a) Bedrijfsgrootteklasse

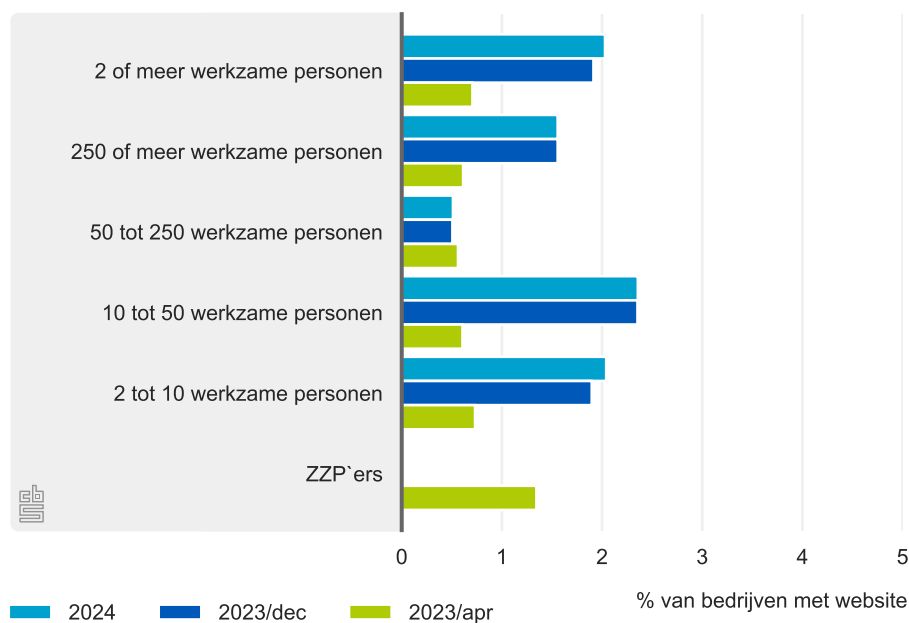


(b) Bedrijfstak

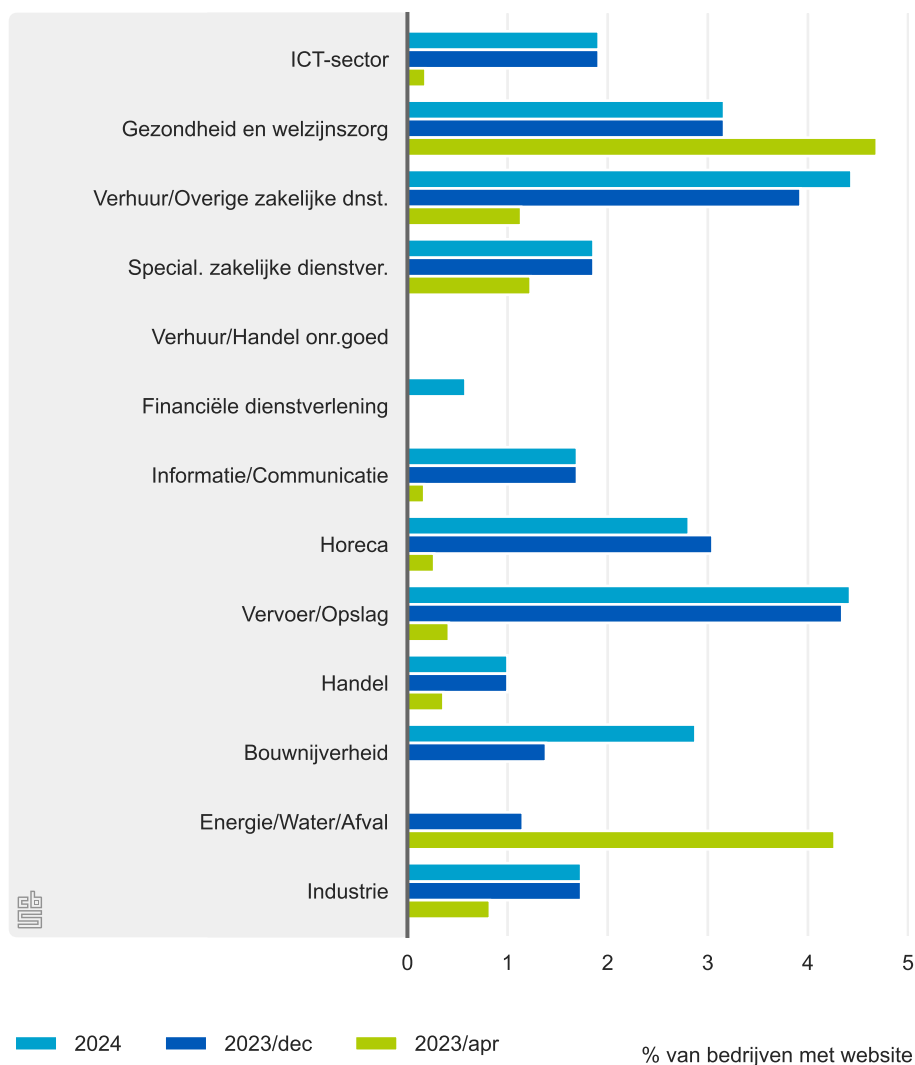


4.4.2 Percentage van bedrijven met website met een eindscore op Internet.nl voor de e-mailtest van 100 procent per bedrijfsgrootteklasse (a) en bedrijfstak met 2 of meer werknemers (b).

(a) Bedrijfsgrootteklasse

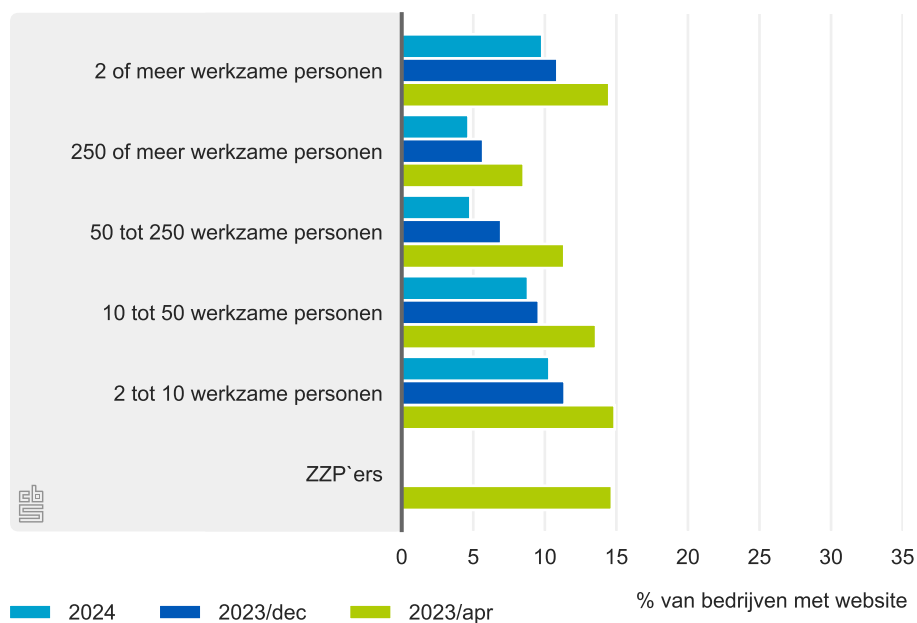


(b) Bedrijfstak

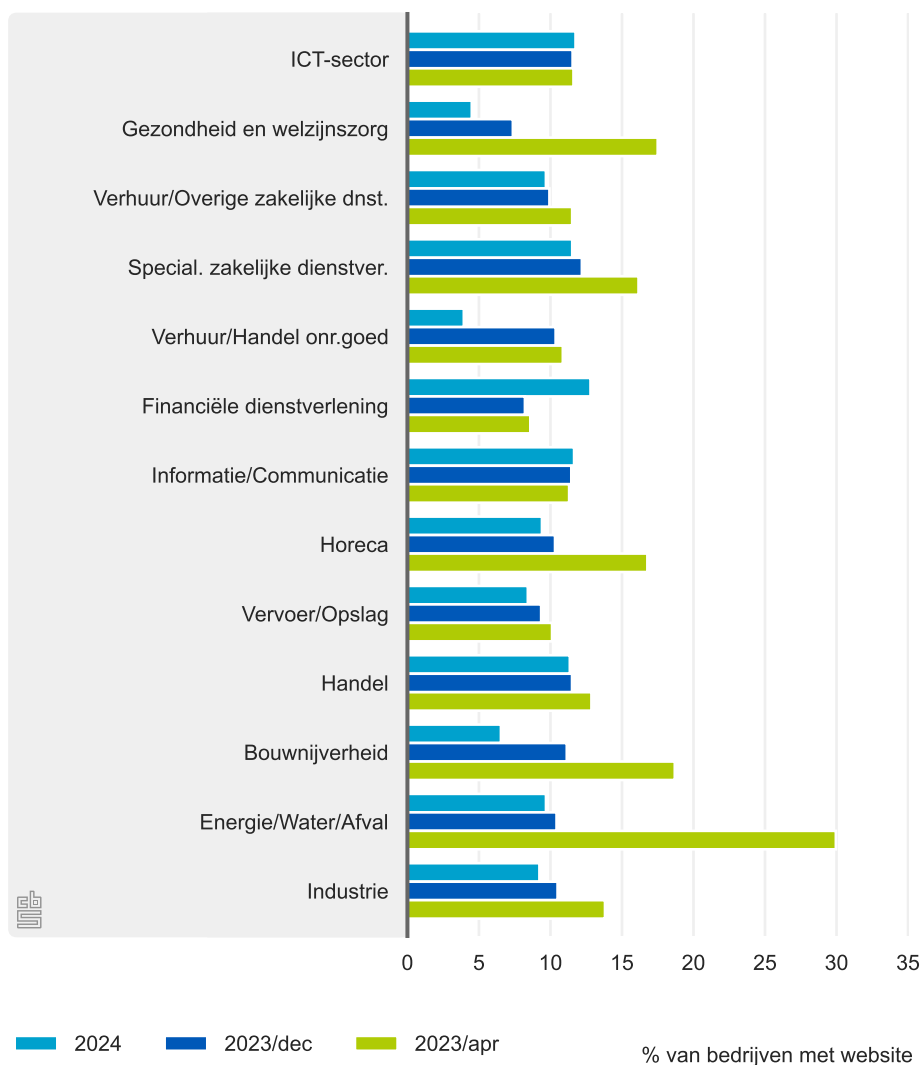


4.4.3 Percentage van bedrijven met website met een eindscore op Internet.nl voor de e-mailtest van 40 procent of minder per bedrijfsgrootteklasse (a) en bedrijfstak met 2 of meer werknemers (b).

(a) Bedrijfsgrootteklasse



(b) Bedrijfstak



5.

Conclusies

In dit onderzoek is samen met [Platform Internetstandaarden \(2023\)](#) een analyse gemaakt van de veiligheid van websites van Nederlands bedrijven. Hiertoe is de CBS-enquête 'ICT-gebruik bij bedrijven' gebruikt om voor vier achtereenvolgende jaren de website die door bedrijven ingevuld is met de webtool [Internet.nl](#) te scannen. Op deze manier is er voor een representatieve steekproef van bedrijven de URL van de website met de meeste bezoekers van het bedrijf gescand. Voor alle jaren is een websitescan uitgevoerd; de e-mailscan is vanaf april 2023 gedaan. Op basis van de websitescans is het mogelijk om per bedrijfsgrootteklasse en bedrijfstak de ontwikkeling van het toepassen van internetstandaarden te volgen.

Geconcludeerd kan worden dat:

- Ongeveer 71 procent van de Nederlandse bedrijven met twee of meer werknemers heeft in 2023 een website; dat is iets minder dan het jaar ervoor.
- Ruim 80 procent bedrijven met website met 2 of meer werknemers heeft *.nl* als domeinextensie voor de hoofdwebsite, *.com* komt met ruim 13 procent op de tweede plaatst.
- Bedrijven gebruiken steeds vaker correcte internetstandaarden, niet alleen voor de eindscore van Internet.nl, maar ook voor alle onderliggende subtesten die aan de eindscore ten grondslag liggen.
- De gemiddelde eindscore van de websitescan van alle bedrijven met website met 2 of meer werknemers is tussen oktober 2020 en april 2024 met 5,2 procentpunt toegenomen, van 60,3 naar 65,5 procent; een toename van ruim 8 procent.
- De eindscoreverdeling van de Internet.nl web- en mailscan vertoont weinig variatie over de bedrijfsgrootteklassen en bedrijfstakken.
- De eindscore wordt samengesteld uit de scores van meerdere onderliggende subtesten; voor deze subtesten zijn wel duidelijke verschillen tussen kleine en grote bedrijven waar te nemen.
- Kleine bedrijven scoren relatief vaker beter op de categorie IPv6, grote bedrijven score juist vaker goed op de categorie HTTPS en de categorie Authenticate als protectie tegen *e-mail phishing*.

Bibliografie

CBS (2020). [ICT-gebruik bij kleine bedrijven; bedrijfstak en bedrijfsgrootte, 2020](#).

CBS (2021). [ICT-gebruik bij kleine bedrijven; bedrijfstak en bedrijfsgrootte, 2021](#).

CBS (2022a). [ICT-gebruik bij kleine bedrijven; bedrijfstak en bedrijfsgrootte, 2022](#).

CBS (2022b). [Cybersecuritymonitor 2022](#).

CBS (2022c). [Veiligheid van website van bedrijven, 2020](#).

CBS (2023a). [ICT-gebruik bij kleine bedrijven; bedrijfstak en bedrijfsgrootte, 2023](#).

CBS (2023b). [Toepassing van internetstandaarden voor websites van bedrijven](#).

Platform Internetstandaarden (2021, Mar). [Nieuwe Internet.nl met verbeterde testen voor TLS en CSP](#).

Platform Internetstandaarden (2023). .

SIDN (2024). [Stichting Internet Domeinregistratie Nederland](#).

SIDN Lab (2024). [stat.sidnlabs.nl](#).

Bijlagen

Bijlage A

Tabellen

A.1 Overzicht Bedrijfsgrootteklassen en bedrijfstakken

A.1.1 Overzicht van de bedrijfsgrootteklassen

Code	Bedrijfsgrootte
2–10	2 tot 10 werkzame personen
10–50	10 tot 50 werkzame personen
50–250	50 tot 250 werkzame personen
100–250	100 tot 250 werkzame personen
250+	250 of meer werkzame personen

A.1.2 Overzicht van de bedrijfstakken

Code	Bedrijfsklasse
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

A.2 Kenmerken websitescans Internet.nl

A.2.1 Vijf categorieën met de subtesten voor de websitescans

Categorie	Subgroep	Testomschrijving	Testuitkomsten	Variabelenaam
HTTPS	https	HTTPS beschikbaar	<i>good/bad/other</i>	tests_web_https_http_available_verdict
		HTTPS-doorverwijzing	<i>good/bad/other/not tested</i>	tests_web_https_http_redirect_verdict
		HTTPS-compressie	<i>good/bad/not tested</i>	tests_web_https_http_compress_verdict
		HSTS aangeboden	<i>good/bad/other/not tested</i>	tests_web_https_http_hsts_verdict
	cert	Vertrouwensketen van certificaat	<i>good/bad/not tested</i>	tests_web_https_cert_chain_verdict
		Publieke sleutel van certificaat	<i>good/bad/not tested</i>	tests_web_https_cert_pubkey_verdict
		Handtekening van certificaat	<i>good/bad/not tested</i>	tests_web_https_cert_sig_verdict
		Domeinnaam op certificaat	<i>good/bad/not tested</i>	tests_web_https_cert_domain_verdict
	tls	TLS Versie	<i>good/bad/phase out/not tested</i>	tests_web_https_tls_version_verdict
		TLS ciphers	<i>good/bad/phase out/not tested</i>	tests_web_https_tls_ciphers_verdict
		TLS cipher-volgorde	<i>good/bad/other/not tested</i>	tests_web_https_tls_cipherorder_verdict
		TLS sleuteluitwisselingsparameters	<i>good/bad/phase out/not tested</i>	tests_web_https_tls_keyexchange_verdict
		Hashfunctie voor sleuteluitwisseling	<i>good/bad/phase out/not tested</i>	tests_web_https_tls_keyexchangehash_verdict
		TLS-compressie	<i>good/bad/not tested</i>	tests_web_https_tls_compress_verdict
		<i>Secure renegotiation</i>	<i>good/bad/not tested</i>	tests_web_https_tls_seceneg_verdict
		<i>Client initiated renegotiation</i>	<i>good/bad/not tested</i>	tests_web_https_tls_clientreneg_verdict
		O-RTT	<i>good/bad/N.A./not tested</i>	tests_web_https_tls_Ortt_verdict
		TLS OCSP-stapeling	<i>good/ok/bad/not tested</i>	tests_web_https_tls_ocsp_verdict
	dane	DANE aanwezig	<i>good/bad/not tested</i>	tests_web_https_dane_exist_verdict
		DANE geldigheid	<i>good/bad/not tested</i>	tests_web_https_dane_valid_verdict
IPv6	ipv6	IPv6-adressen voor <i>nameservers</i>	<i>good/bad/other</i>	tests_web_ipv6_ns_address_verdict
		IPv6-bereikbaarheid van <i>nameservers</i>	<i>good/bad/not tested</i>	tests_web_ipv6_ns_reach_verdict
		IPv6-adressen voor <i>webserver</i>	<i>good/bad</i>	tests_web_ipv6_ws_address_verdict
		IPv6-bereikbaarheid van <i>webserver</i> s	<i>good/bad/not tested</i>	tests_web_ipv6_ws_reach_verdict
		Gelijke website op IPv6 en IPv4	<i>good/bad/not tested</i>	tests_web_ipv6_ws_similar_verdict
DNSSEC	dnssec	DNSSEC aanwezig	<i>good/bad/server failed</i>	tests_web_dnssec_exist_verdict
		DNSSEC geldigheid	<i>good/bad/not tested</i>	tests_web_dnssec_valid_verdict
Beveiligings-opties	appsec	<i>X-Frame-options</i>	<i>good/bad/phase out/not tested</i>	tests_web_appsecpriv_x_frame_options_verdict
		<i>X-Content-Type-Options</i>	<i>good/bad/phase out/not tested</i>	tests_web_appsecpriv_x_content_type_options_verdict
		<i>Content-Security-Policy</i>	<i>good/bad/not tested</i>	tests_web_appsecpriv_csp_verdict
		<i>Referrer-Policy</i> aanwezig	<i>good/bad/not tested</i>	tests_web_appsecpriv_referrer_policy_verdict
RPKI	rpki	Route Oorsprong Autorisatie bestaat	<i>good/bad/no address/not tested</i>	tests_web_rpki_exists_verdict
		Route Oorsprong Autorisatie is geldig	<i>good/bad/not routed/not tested</i>	tests_web_rpki_valid_verdict
		RPKI voor nameserver bestaat	<i>good/bad/no address/not tested</i>	tests_web_ns_rpki_exists_verdict
		RPKI voor nameserver is geldig	<i>good/bad/invalid/not tested</i>	tests_web_ns_rpki_valid_verdict

A.3 Kenmerken e-mailscan Internet.nl

A.3.1 Vijf categorieën met de subtesten voor de E-mailscans

Categorie	Subgroep	Testomschrijving	Testuitkomsten	Variabelenaam
IPv6	ipv6	IPv6-adressen voor nameservers	<i>good/bad/other</i>	tests_mail_ipv6_ns_address_verdict
		IPv6-bereikbaarheid nameservers	<i>good/bad/other/not tested</i>	tests_mail_ipv6_ns_reach_verdict
		IPv6 voor mailservers	<i>good/bad/null mx</i>	tests_mail_ipv6_mx_address_verdict
		IPv6 mailservers bereikbaarheid	<i>good/bad/other/not tested</i>	tests_mail_ipv6_mx_reach_verdict
DNSSEC	dnssec	Email-adres heeft DNSSEC	<i>good/bad/null mx</i>	tests_mail_dnssec_mailto_exist_verdict
		Email-adres DNSSEC geldig	<i>good/bad/other/not tested</i>	tests_mail_dnssec_mailto_valid_verdict
		Ontvangende mailserver DNSSEC	<i>good/bad/null mx</i>	tests_mail_dnssec_mx_exist_verdict
		Ontv. mailserver DNSSEC geldig	<i>good/bad/other/not tested</i>	tests_mail_dnssec_mx_valid_verdict
Authenticati	auth	DMARC bestaat	<i>good/bad/other/not tested</i>	tests_mail_auth_dmarc_exist_verdict
		DMARC strict	<i>good/bad/policy</i>	tests_mail_auth_dmarc_policy_verdict
		DKIM bestaat	<i>good/bad/no email</i>	tests_mail_auth_dkim_exist_verdict
		SPF bestaat	<i>good/bad/other/not tested</i>	tests_mail_auth_spf_exist_verdict
		SPF beleid	<i>good/bad/not tested</i>	tests_mail_auth_spf_policy_verdict
STARTTLS	starttls	beschikbaar	<i>good/bad/null mx</i>	tests_mail_starttls_tls_available_verdict
		sleuteluitwisselingsparameters	<i>good/bad/phase out/not tested</i>	tests_mail_starttls_tls_keyexchange_verdict
		Alleen veilige algoritmeselecties	<i>good/bad/phase out/not tested</i>	tests_mail_starttls_tls_ciphers_verdict
		Volgorde Algoritmeselectie	<i>good/bad/not tested</i>	tests_mail_starttls_tls_cipherorder_verdict
	tls	alleen veilige TLS versies	<i>good/bad/phase out/not tested</i>	tests_mail_starttls_tls_version_verdict
		geen TLS-compressie	<i>good/bad/other/not tested</i>	tests_mail_starttls_tls_compress_verdict
		secure renegotiation	<i>good/bad/other/not tested</i>	tests_mail_starttls_tls_secureneg_verdict
		client-initiated renegotiation	<i>good/bad/other/not tested</i>	tests_mail_starttls_tls_clientreneg_verdict
		0-RTT	<i>good/bad/not tested</i>	tests_mail_starttls_tls_0rtt_verdict
		Hashfunctie voor sleuteluitwisseling	<i>good/bad/phase out/not tested</i>	tests_mail_starttls_tls_keyexchangehash_verdict
	certificaat	Vertrouwensketen	<i>good/bad/not tested</i>	tests_mail_starttls_cert_chain_verdict
		Publieke sleutel	<i>good/bad/other/not tested</i>	tests_mail_starttls_cert_pubkey_verdict
		Handtekening van certificaat	<i>good/bad/other/not tested</i>	tests_mail_starttls_cert_sig_verdict
		Domein op certificaat	<i>good/bad/other/not tested</i>	tests_mail_starttls_cert_domain_verdict
	dane	DANE bestaat	<i>good/bad/other/not tested</i>	tests_mail_starttls_dane_exist_verdict
		DANE geldigheid	<i>good/bad/other/not tested</i>	tests_mail_starttls_dane_valid_verdict
		DANE Rollover-schema	<i>good/bad/other/not tested</i>	tests_mail_starttls_dane_rollover_verdict
RPKI	rpki	Route Oorsprong Autorisatie bestaat	<i>good/bad/not tested</i>	tests_mail_rpki_exists_verdict
		Route Oorsprong Autorisatie is geldig	<i>good/bad/not routed/not tested</i>	tests_mail_rpki_valid_verdict
		nameserver bestaat	<i>good/bad/not tested</i>	tests_mail_ns_rpki_exists_verdict
		Geldigheid voor nameserver	<i>good/bad/not tested</i>	tests_mail_ns_rpki_valid_verdict
	Mx	voor ontvangende mailserver bestaat	<i>good/bad/not tested</i>	tests_mail_mx_ns_rpki_exists_verdict
		Geldigheid voor mail-servers	<i>good/bad/other/not tested</i>	tests_mail_mx_ns_rpki_valid_verdict

Bijlage B

Alle websitetestuitslagen

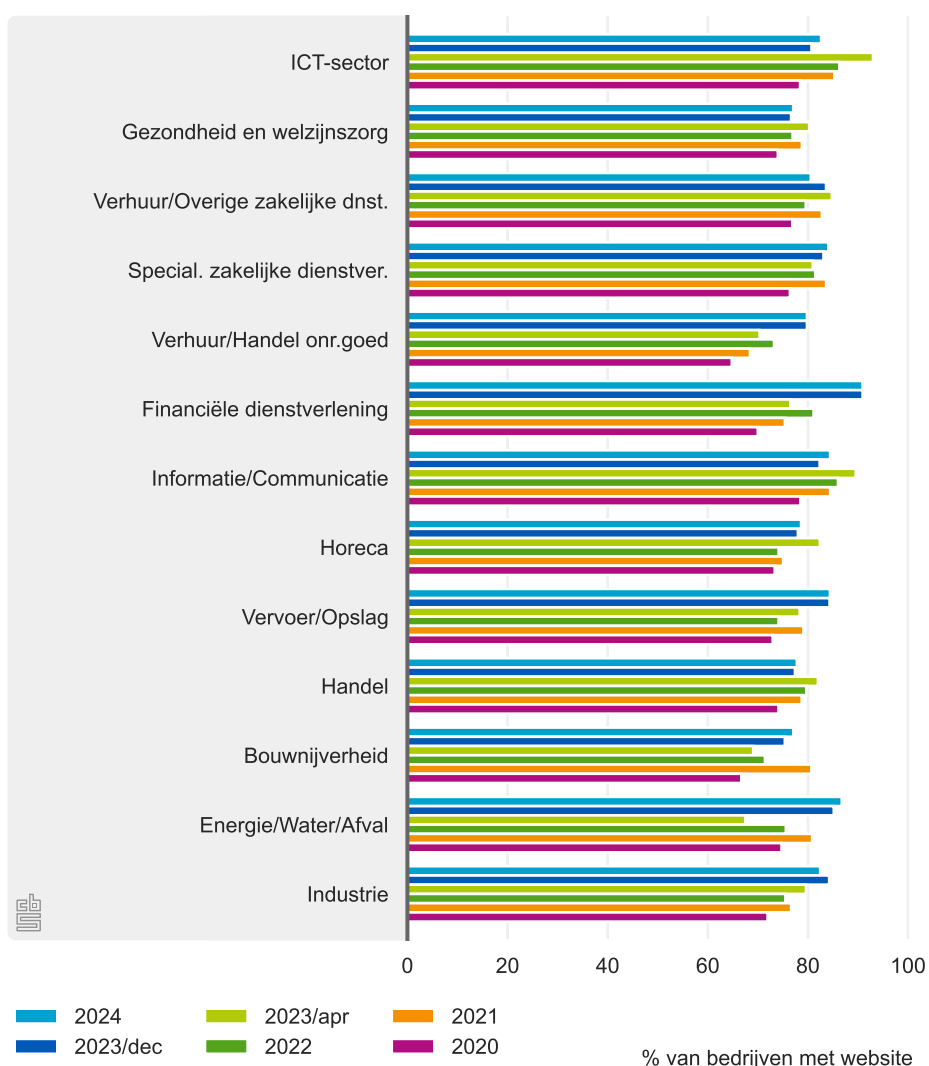
B.1 Website-testuitslagen voor categorie `IPv6`

**B.1.1 Percentage van bedrijven met website met geslaagde website-test
'IPv6-adressen voor nameservers' per bedrijfsgrootteklasse (a) en bedrijfstak
(b).**

(a) Bedrijfsgrootteklasse



(b) Bedrijfstak

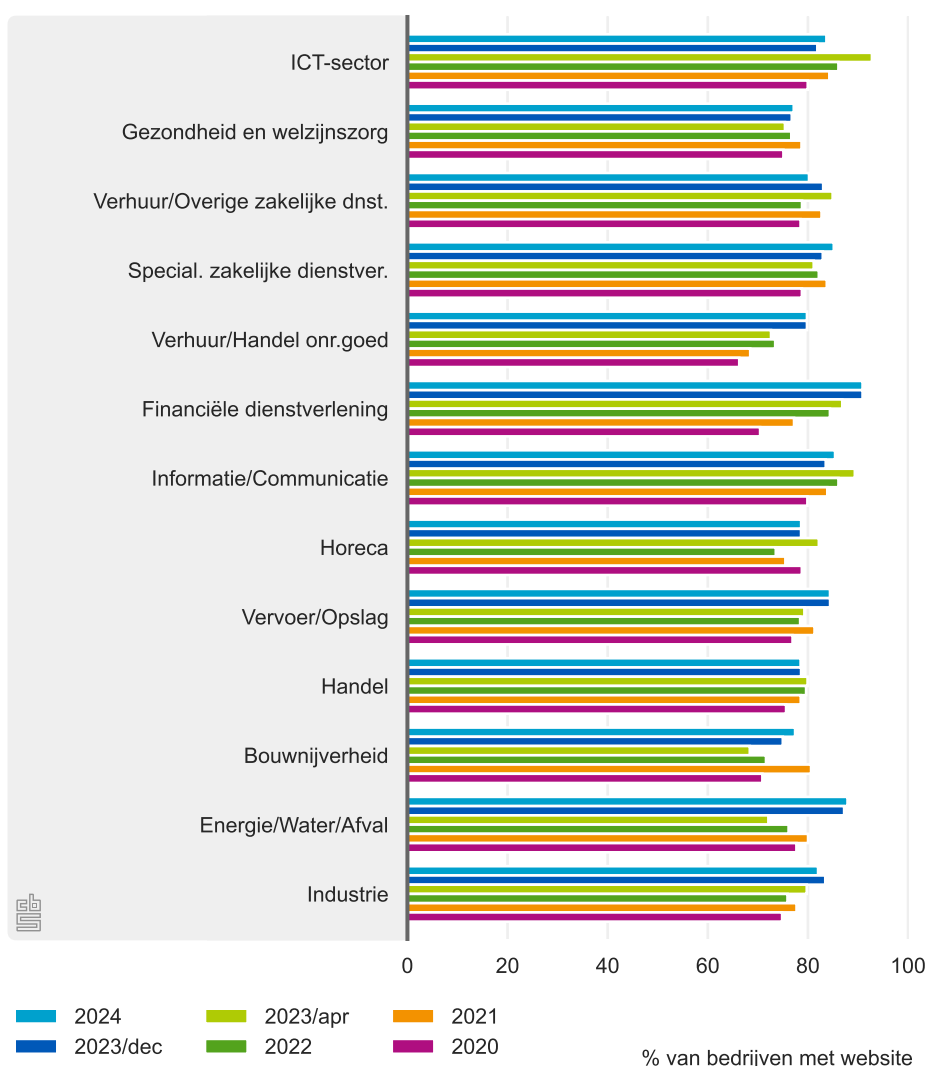


**B.1.2 Percentage van bedrijven met website met geslaagde website-test
'IPv6-bereikbaarheid van nameservers' per bedrijfsgrootteklasse (a) en
bedrijfstak (b).**

(a) Bedrijfsgrootteklasse

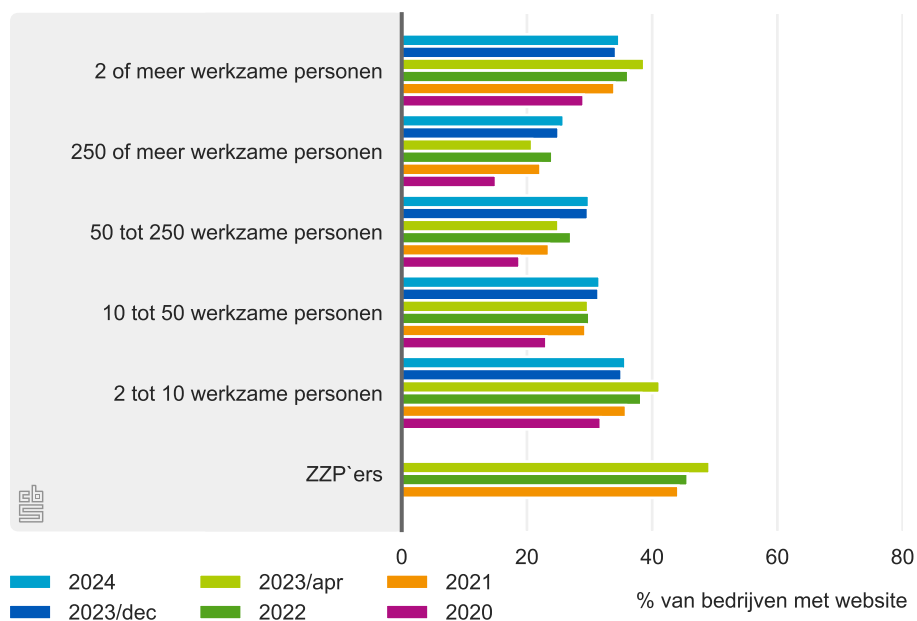


(b) Bedrijfstak

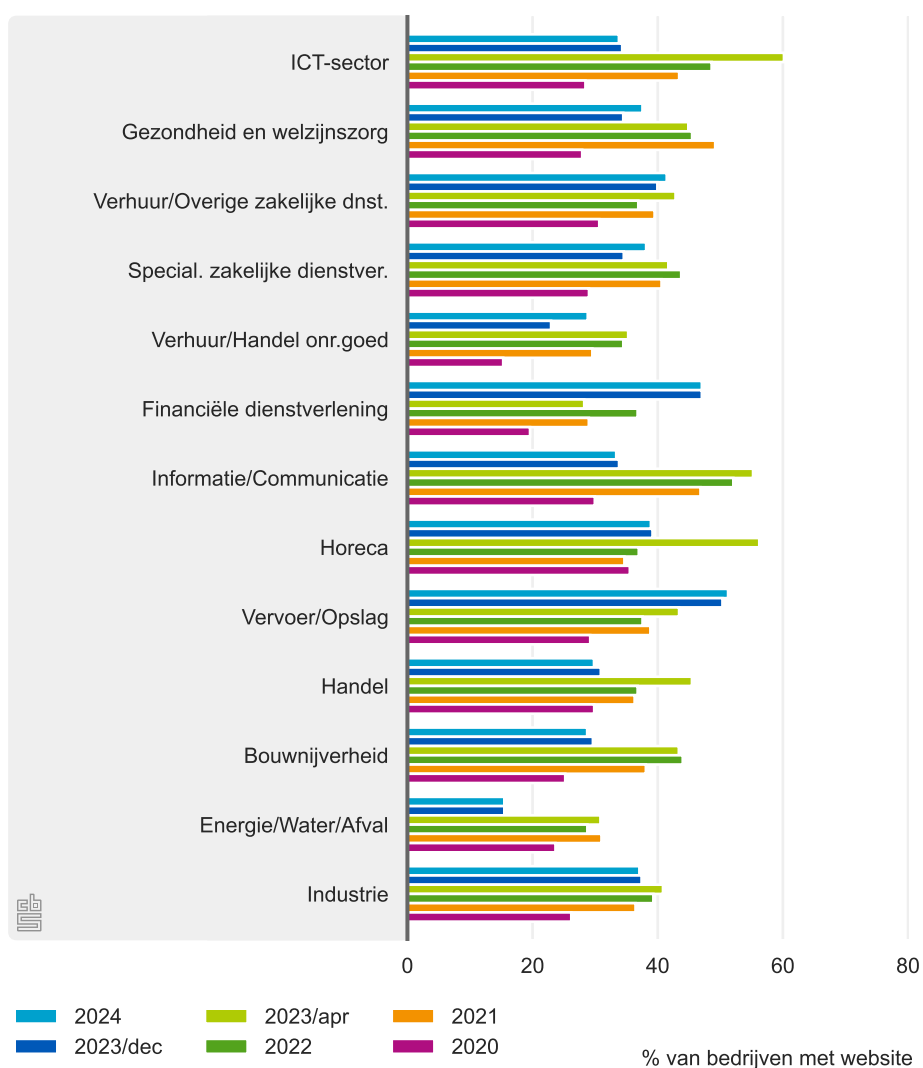


B.1.3 Percentage van bedrijven met website met geslaagde website-test 'IPv6-adressen voor webserver' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse

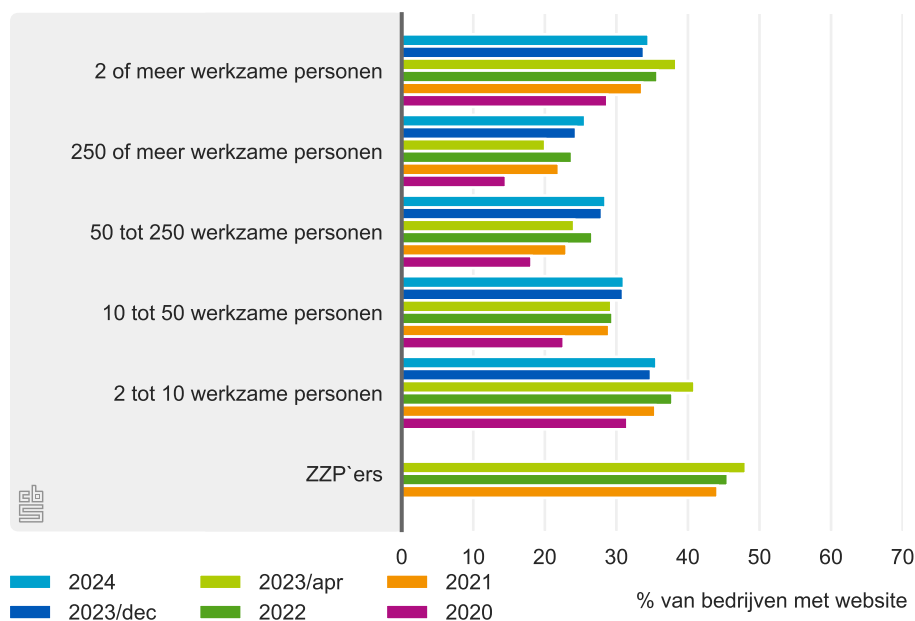


(b) Bedrijfstak

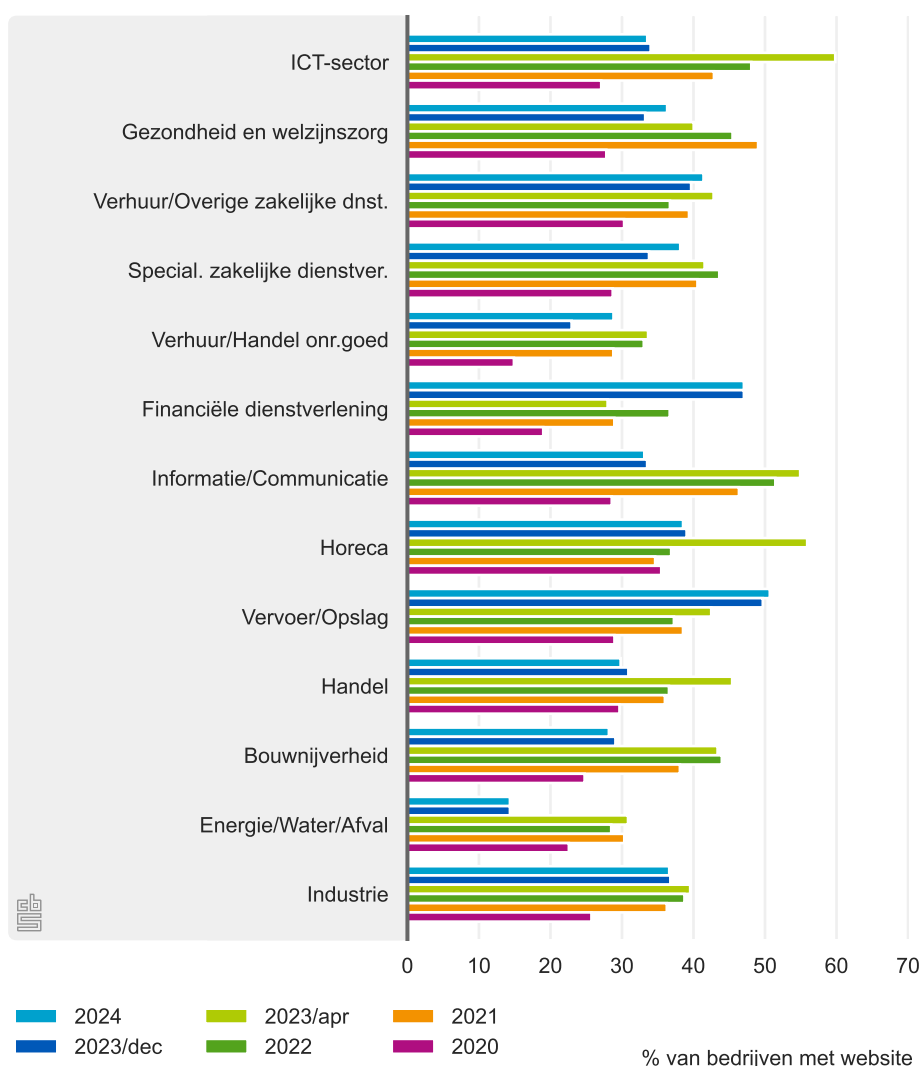


B.1.4 Percentage van bedrijven met website met geslaagde website-test 'IPv6-bereikbaarheid van webserver' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse

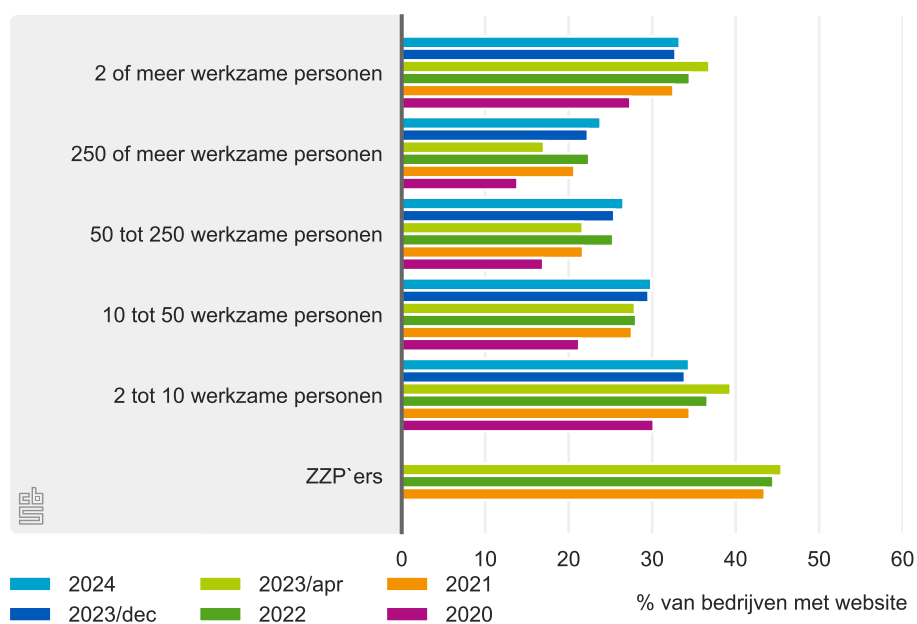


(b) Bedrijfstak

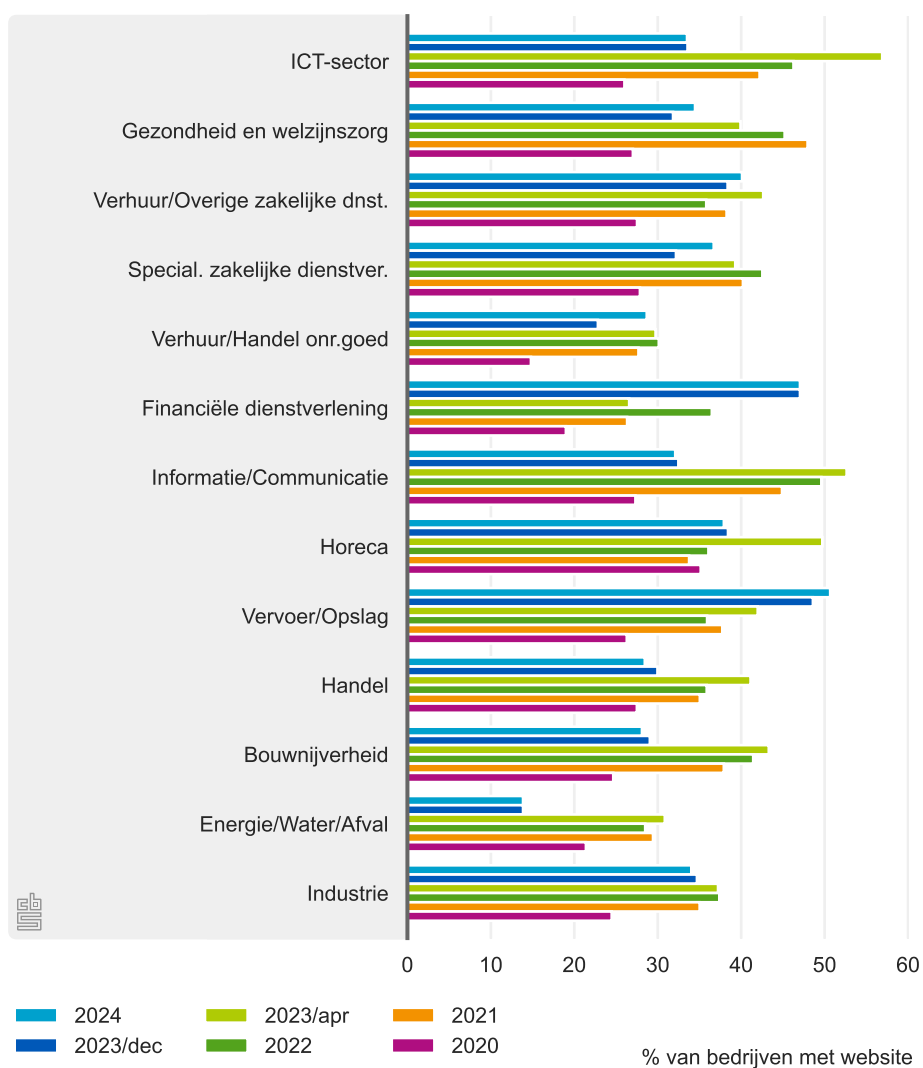


B.1.5 Percentage van bedrijven met website met geslaagde website-test `Gelijke website op IPv6 en IPv4` per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse



(b) Bedrijfstak



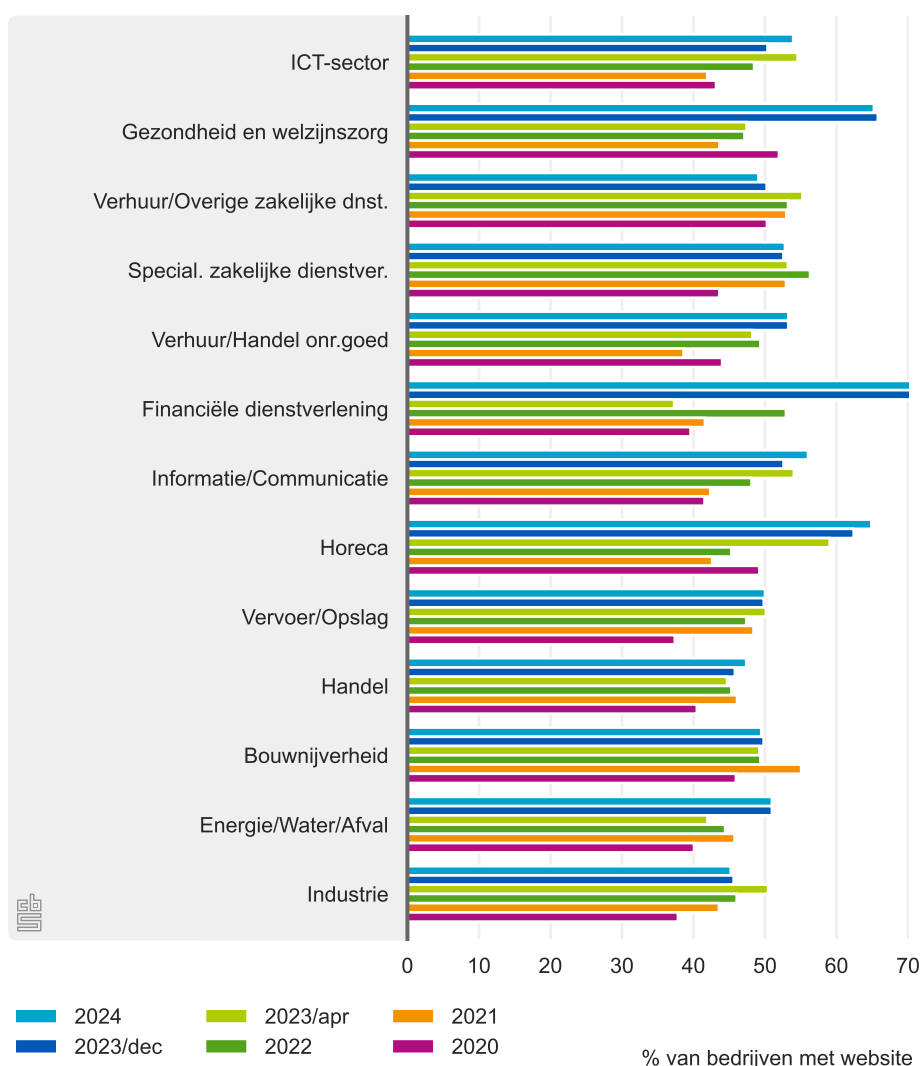
B.2 Website-testuitslagen voor categorie `Domeinnaamhandtekening' (DNSSEC)

**B.2.1 Percentage van bedrijven met website met geslaagde website-test
'Domeinnaamhandtekening aanwezig' per bedrijfsgrootteklasse (a) en
bedrijfstak (b).**

(a) Bedrijfsgrootteklasse



(b) Bedrijfstak

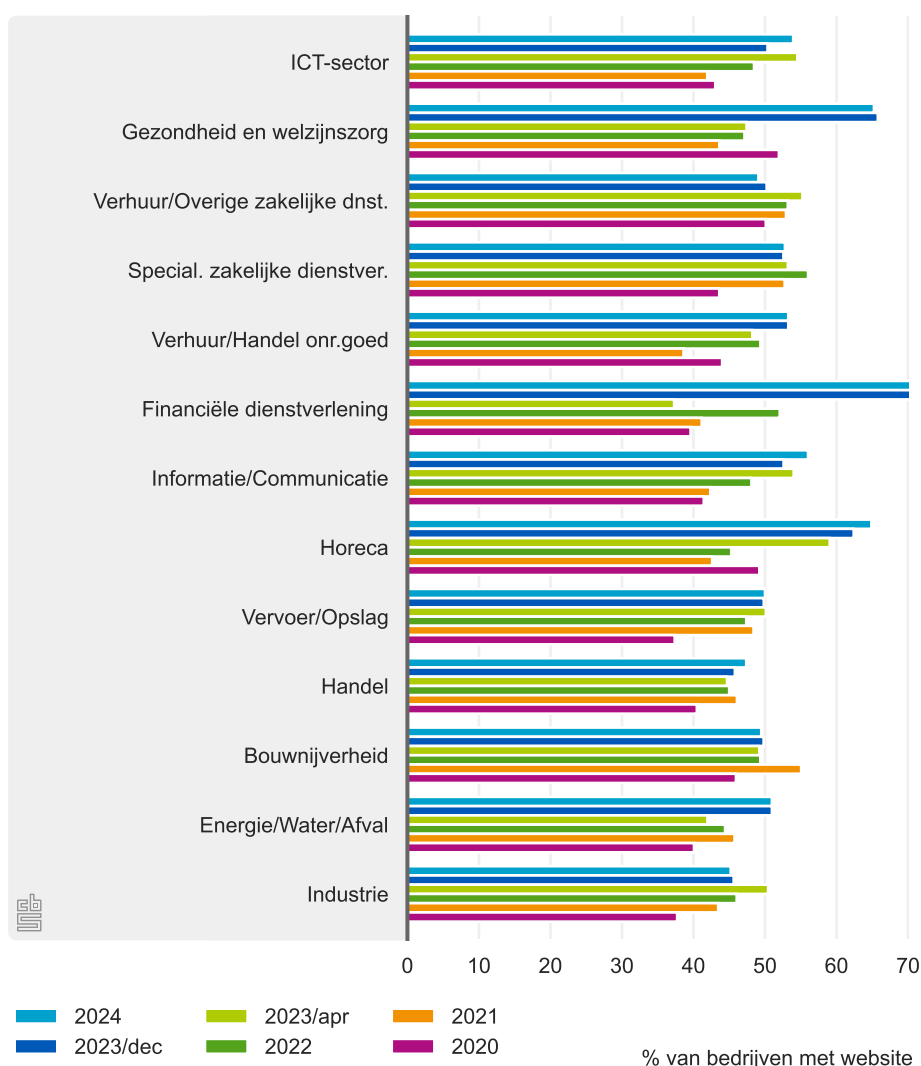


B.2.2 Percentage van bedrijven met website met geslaagde website-test 'Domeinnaamhandtekening geldigheid' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse



(b) Bedrijfstak



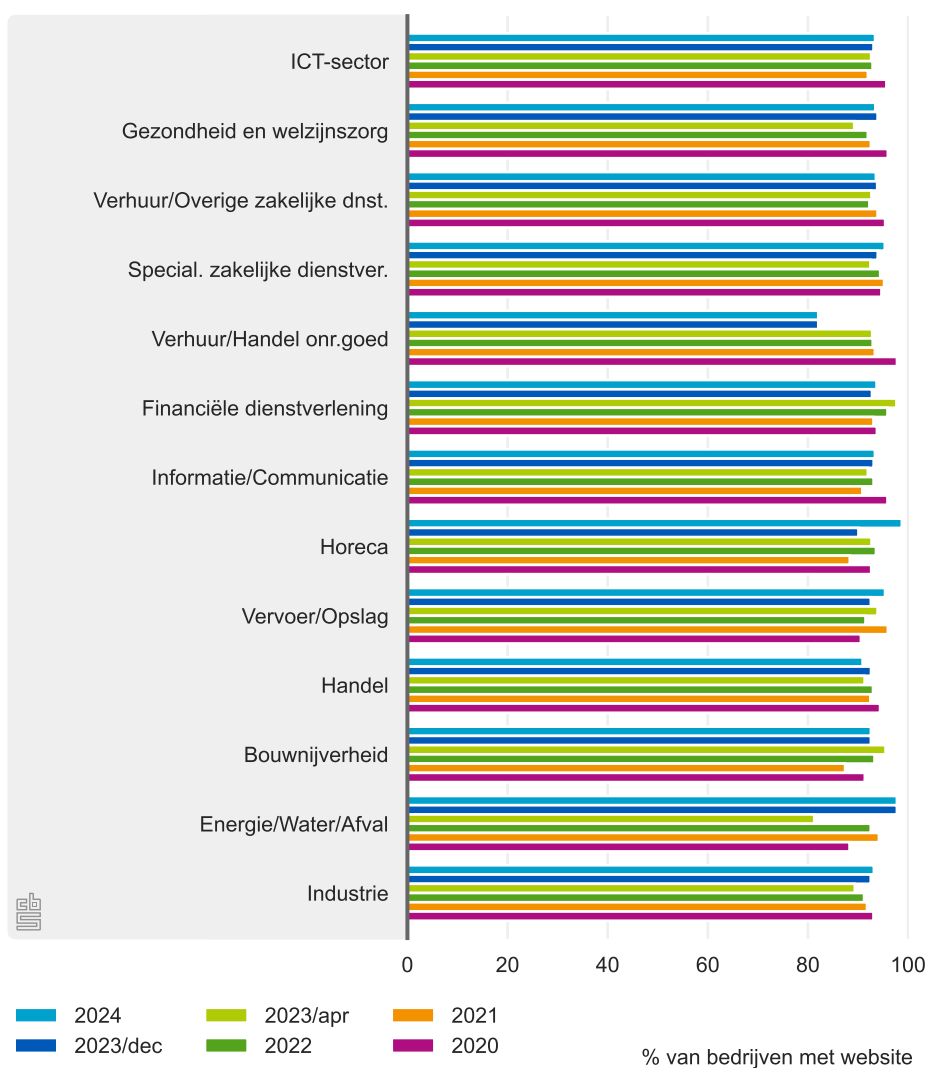
B.3 Website-testuitslagen voor categorie 'HTTPS'

B.3.1 Percentage van bedrijven met website met geslaagde website-test 'HTTPS beschikbaar' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse



(b) Bedrijfstak

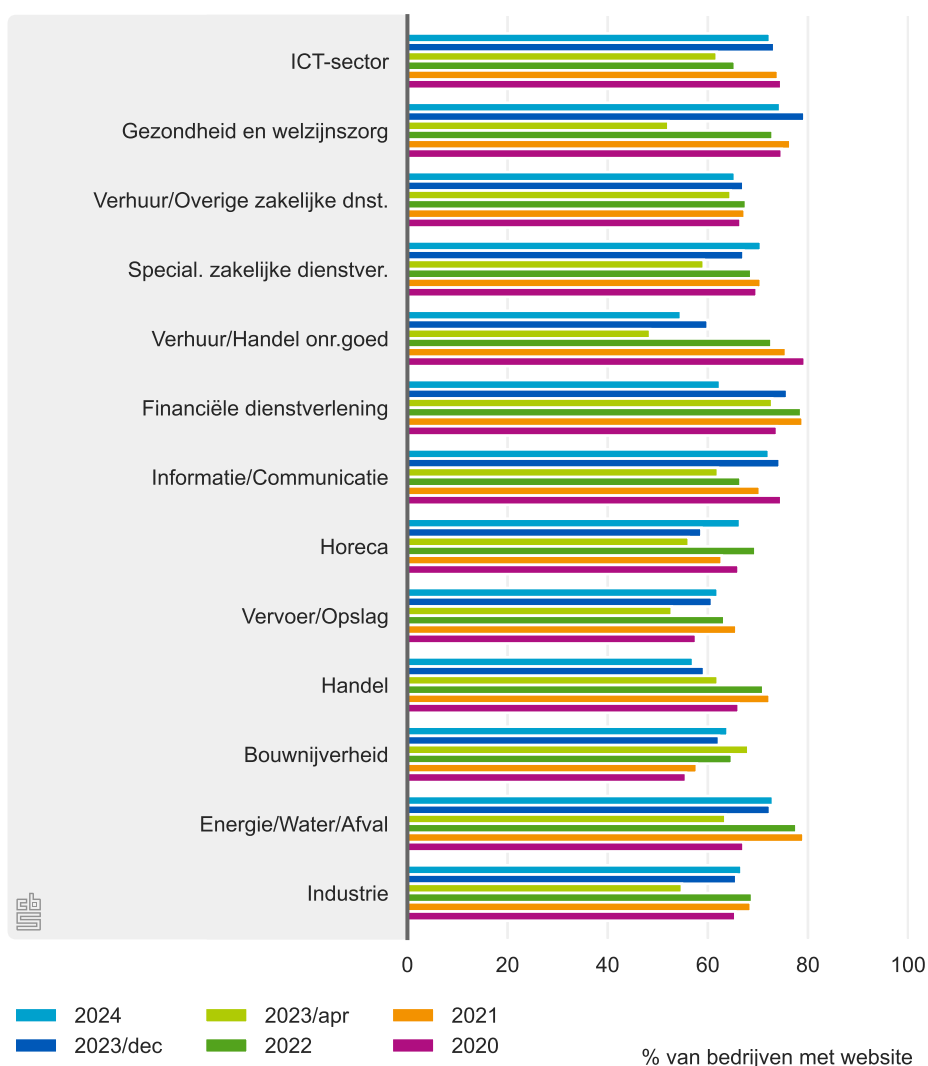


B.3.2 Percentage van bedrijven met website met geslaagde website-test 'HTTPS-doorverwijzing' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse



(b) Bedrijfstak

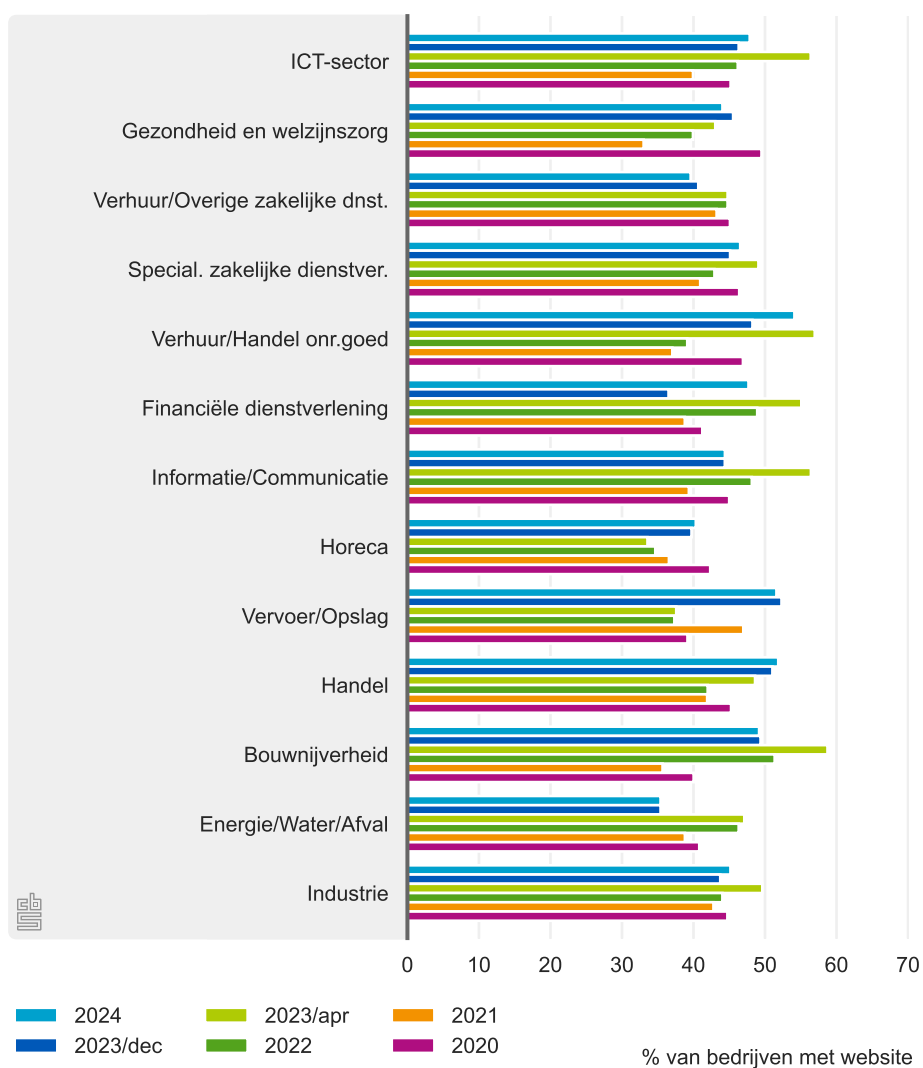


B.3.3 Percentage van bedrijven met website met geslaagde website-test `HTTPS compressie niet ondersteund' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse

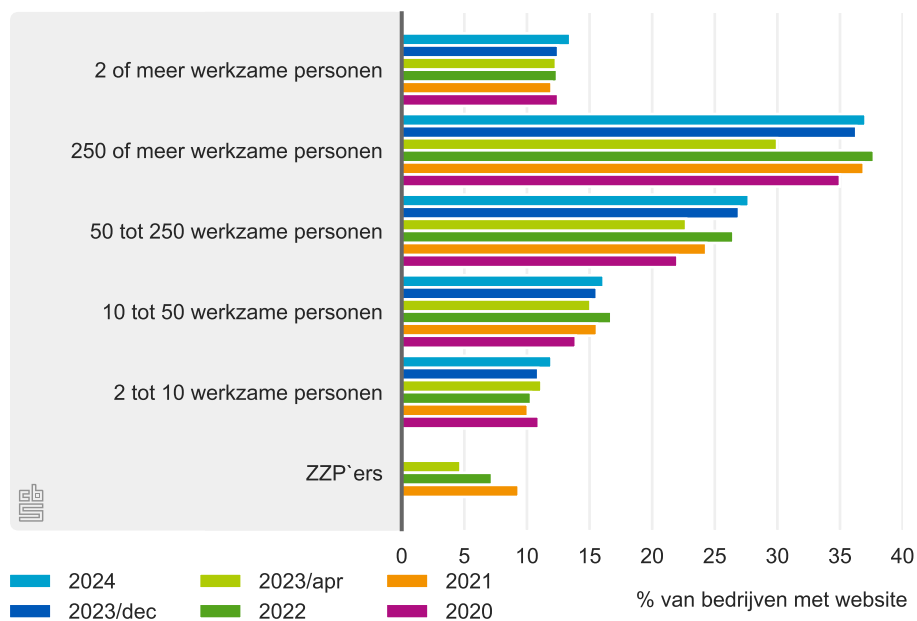


(b) Bedrijfstak

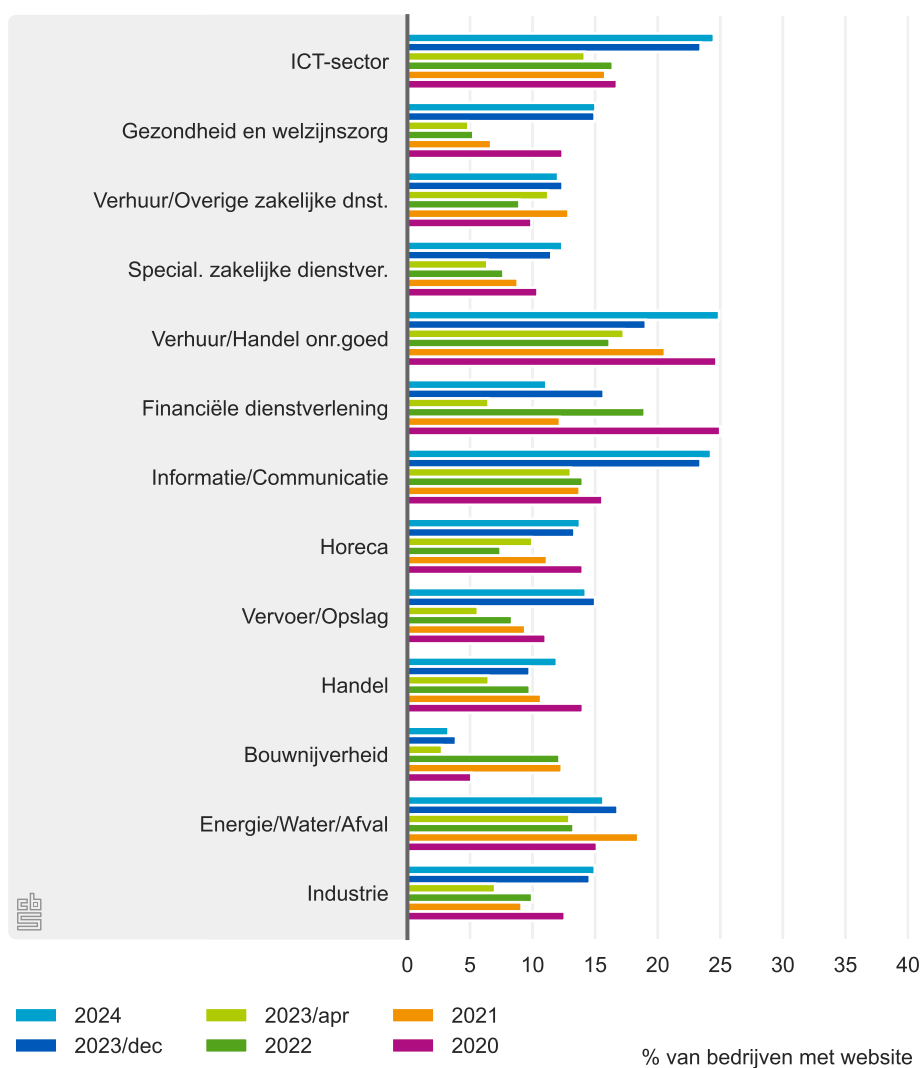


B.3.4 Percentage van bedrijven met website met geslaagde website-test 'HSTS policy aangeboden' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse



(b) Bedrijfstak

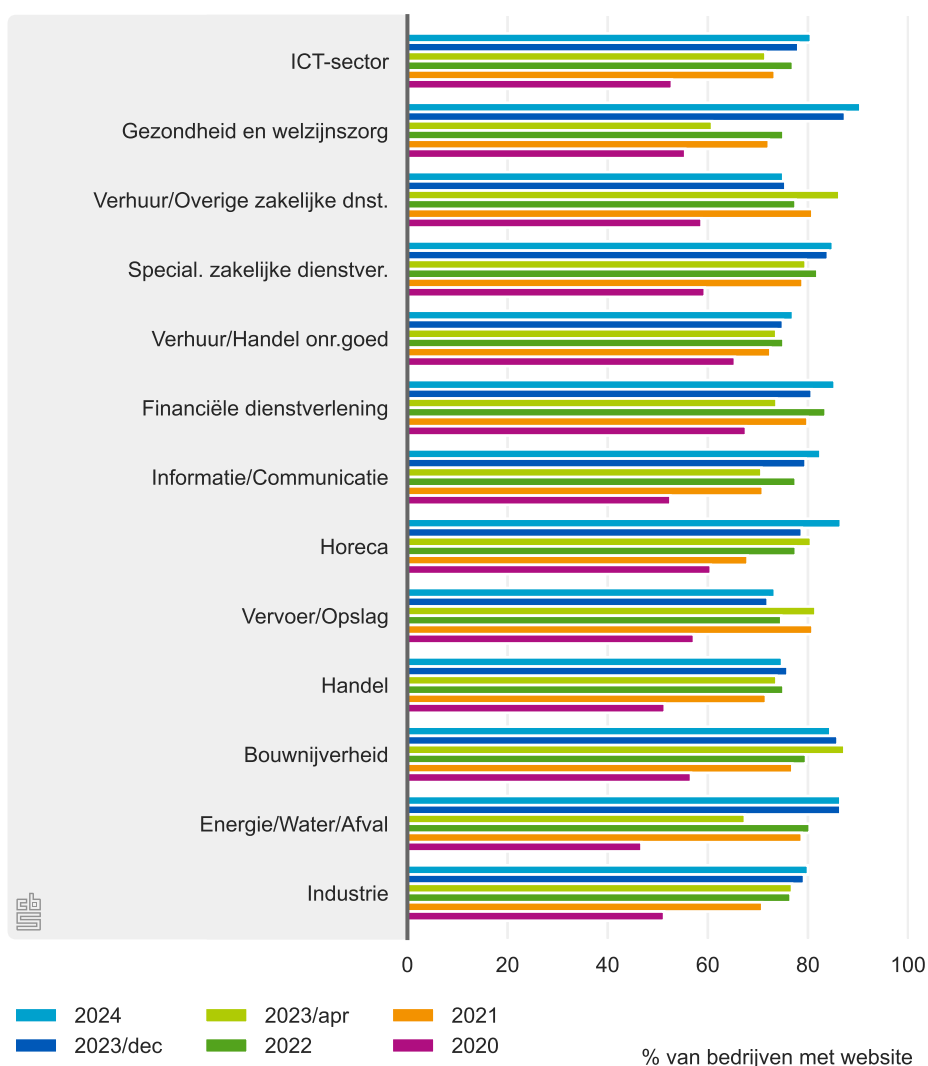


B.3.5 Percentage van bedrijven met website met geslaagde website-test 'TLS versie' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse



(b) Bedrijfstak

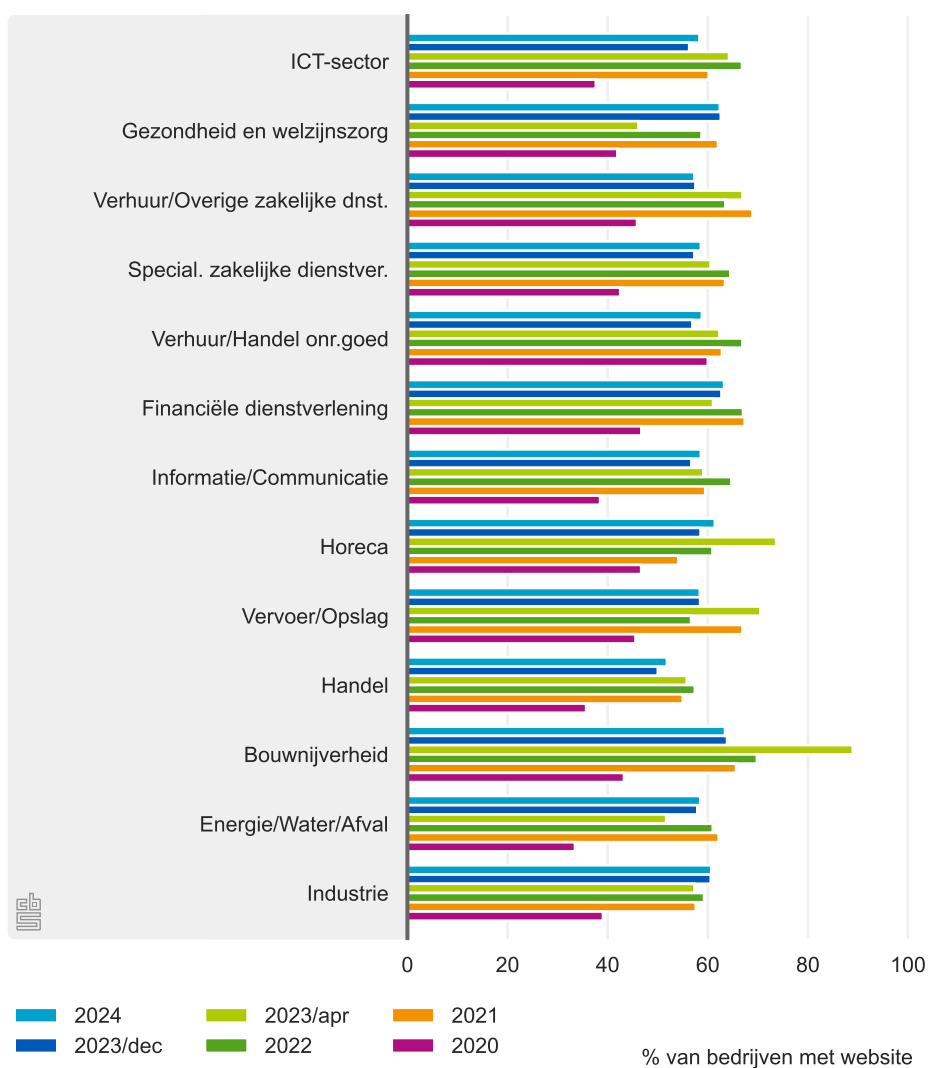


B.3.6 Percentage van bedrijven met website met geslaagde website-test `TLS ciphers' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse



(b) Bedrijfstak

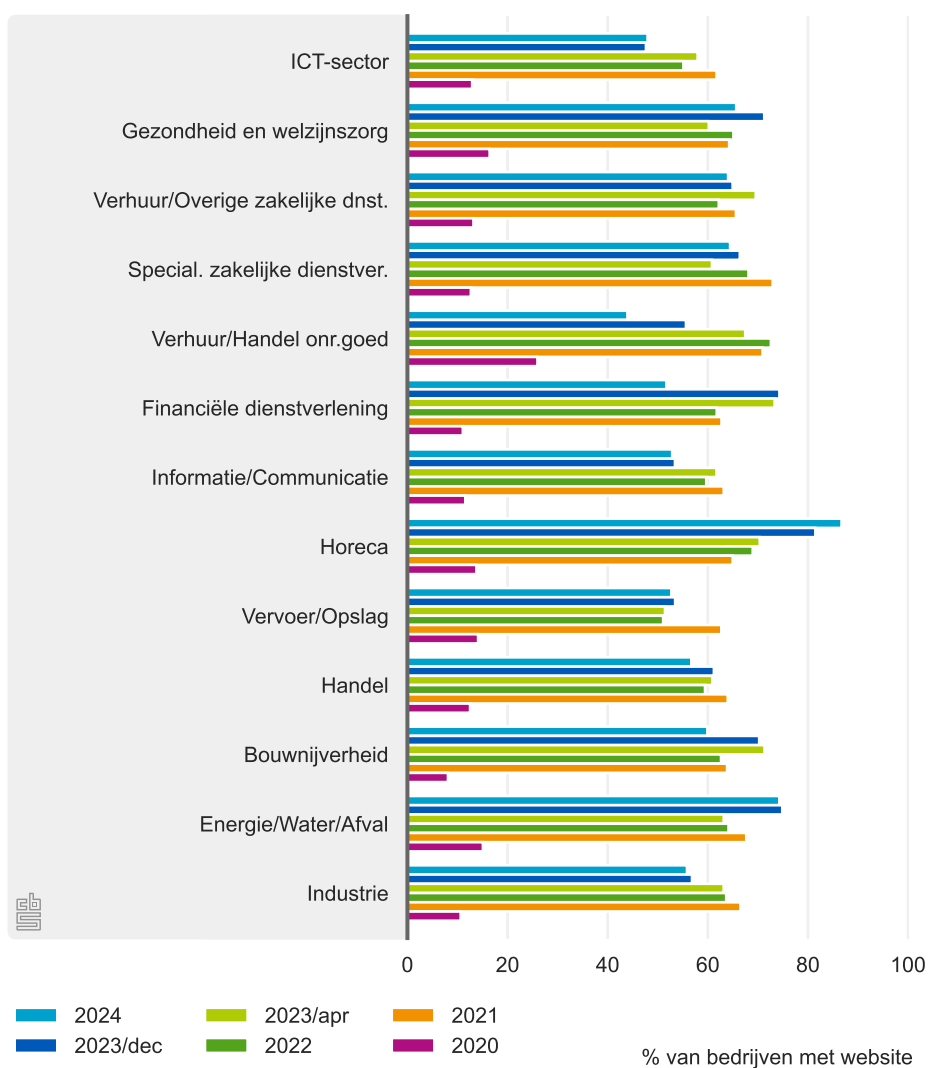


B.3.7 Percentage van bedrijven met website met geslaagde website-test 'TLS-cijfervolgorde' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse



(b) Bedrijfstak

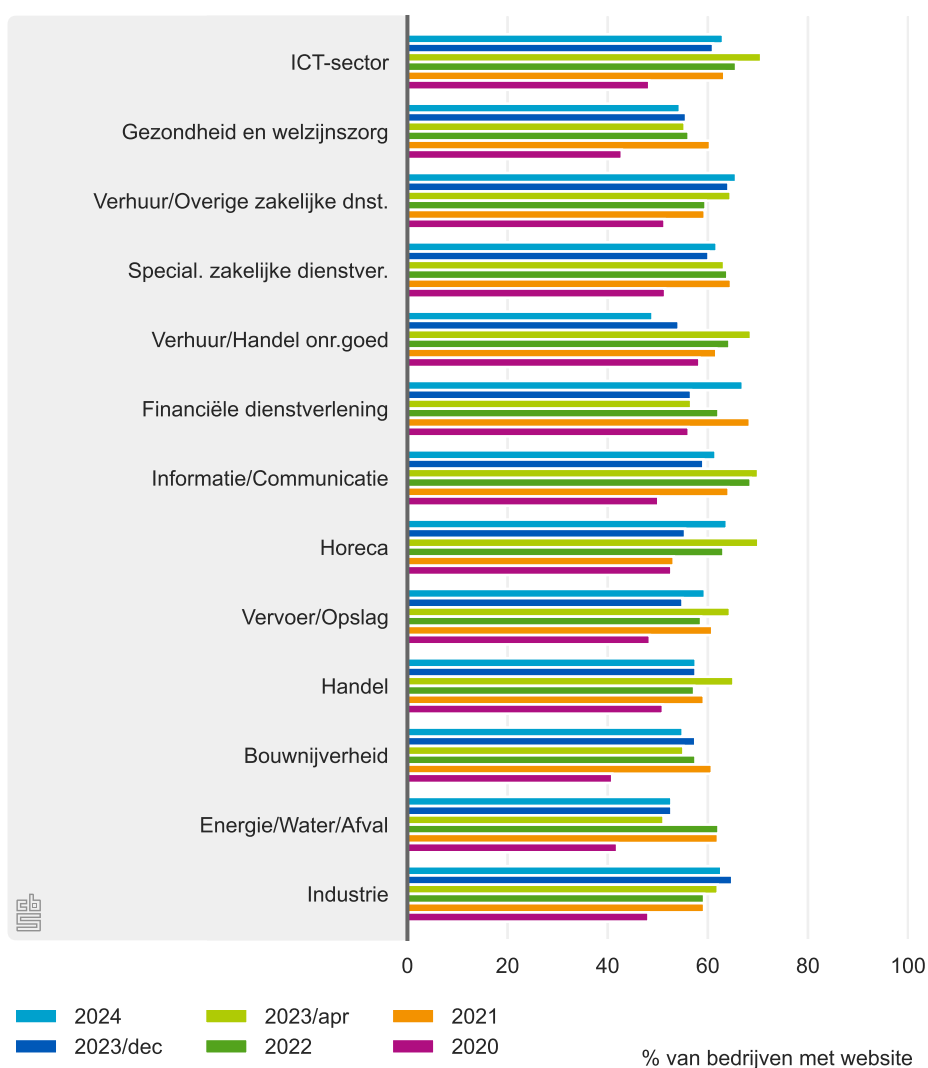


B.3.8 Percentage van bedrijven met website met geslaagde website-test `TLS sleutелuitwisselingsparameters' per bedrijfsgrootteklasse (a) en bedrijfstak(b).

(a) Bedrijfsgrootteklasse



(b) Bedrijfstak

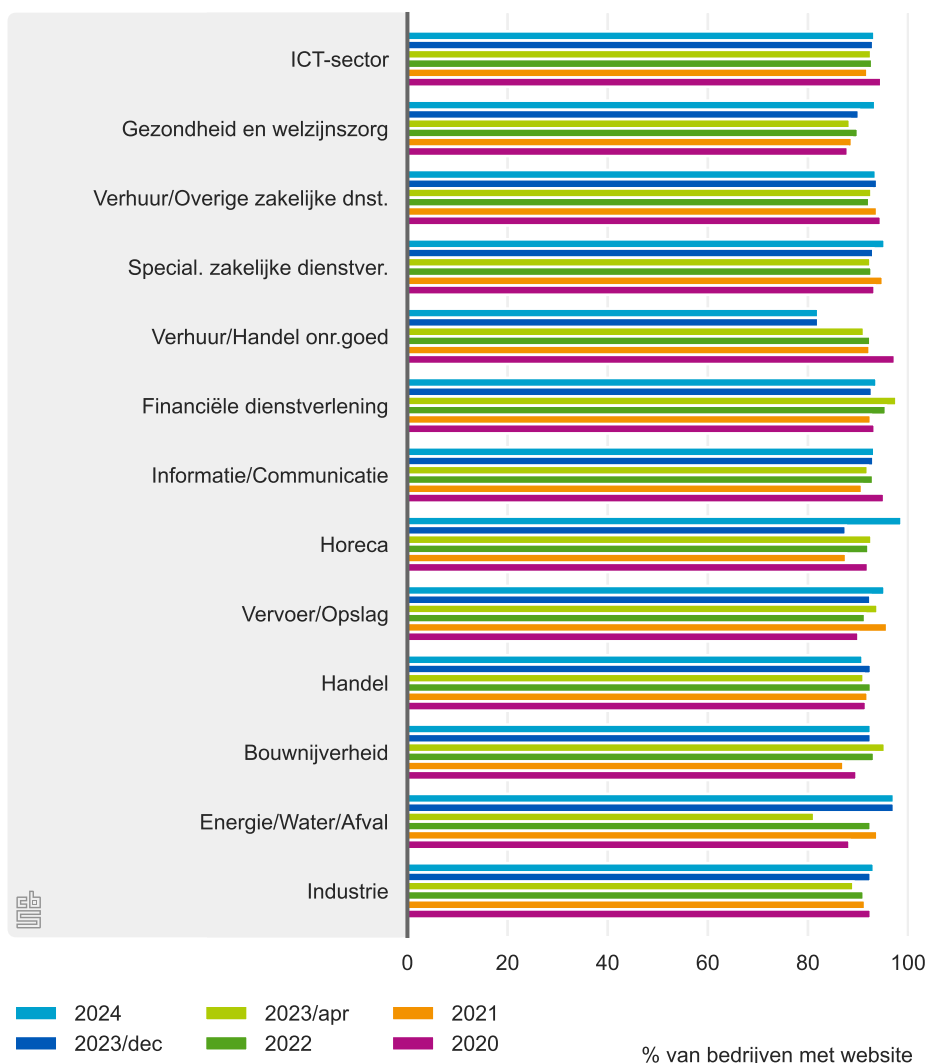


B.3.9 Percentage van bedrijven met website met geslaagde website-test 'Hashfunctie voor sleuteluitwisseling' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse



(b) Bedrijfstak

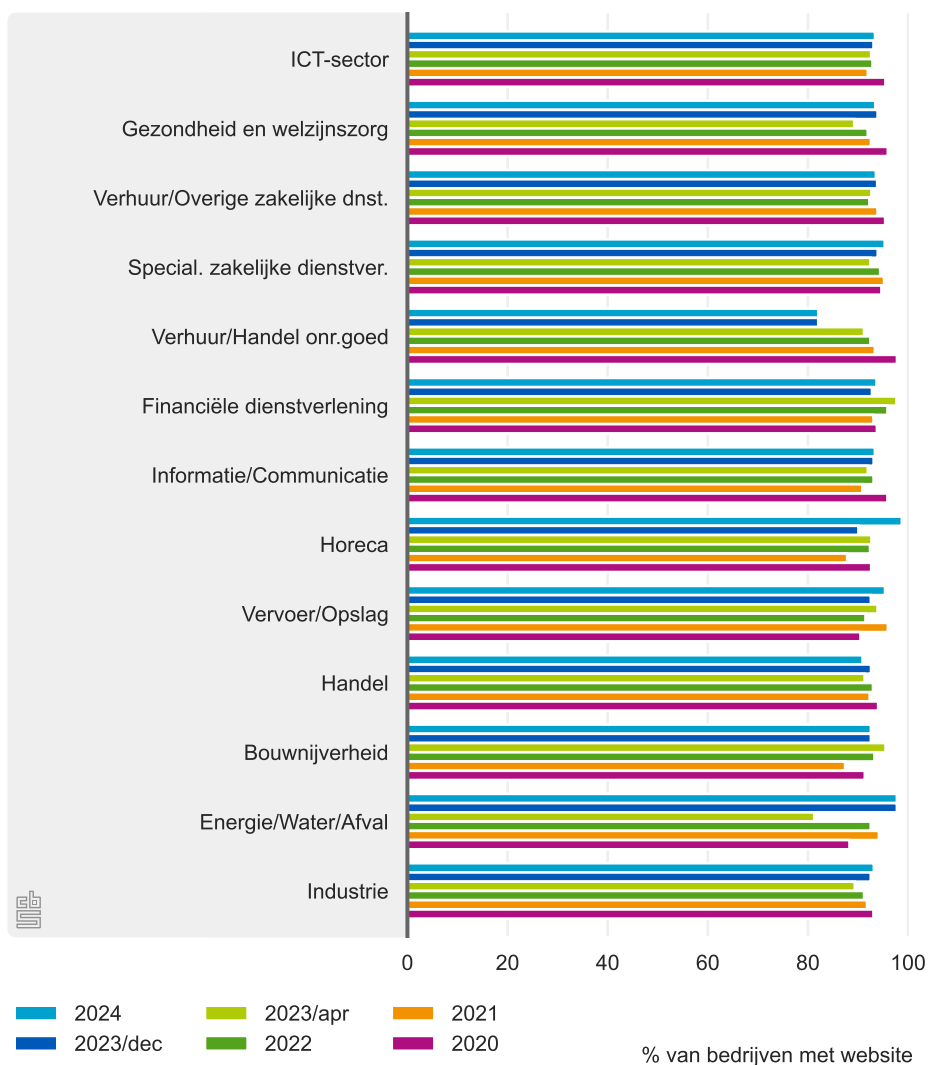


B.3.10 Percentage van bedrijven met website met geslaagde website-test 'TLS-compressie niet ondersteund' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse



(b) Bedrijfstak

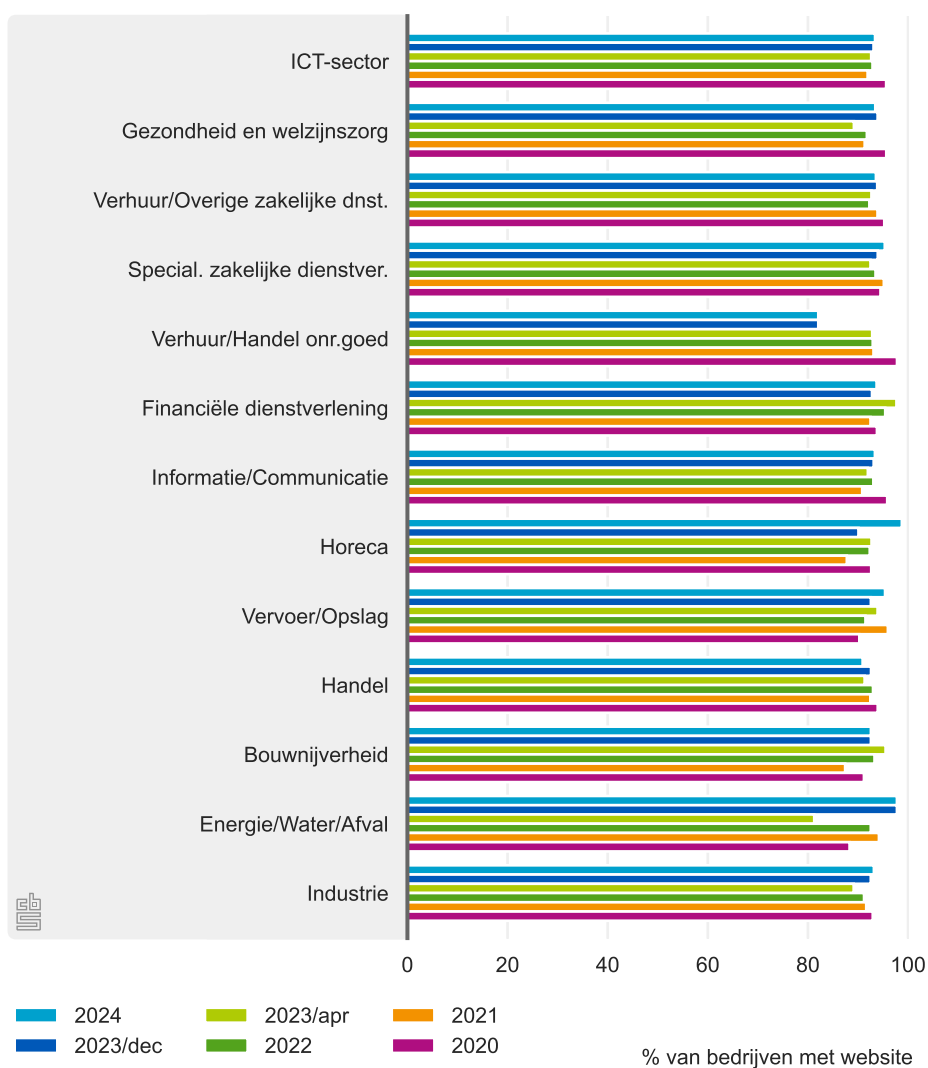


B.3.11 Percentage van bedrijven met website met geslaagde website-test 'TLS secure renegotiation' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse



(b) Bedrijfstak

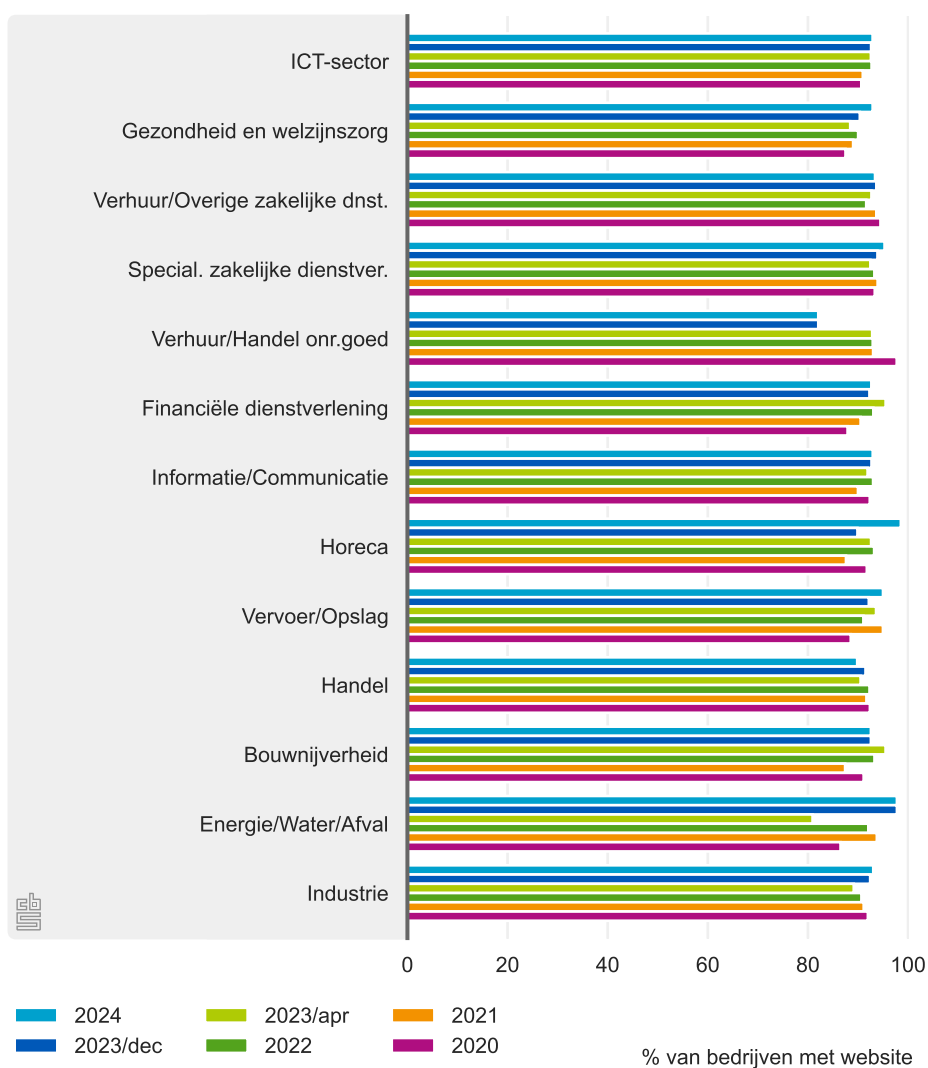


B.3.12 Percentage van bedrijven met website met geslaagde website-test 'TLS client-initiated renegotiation' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse



(b) Bedrijfstak

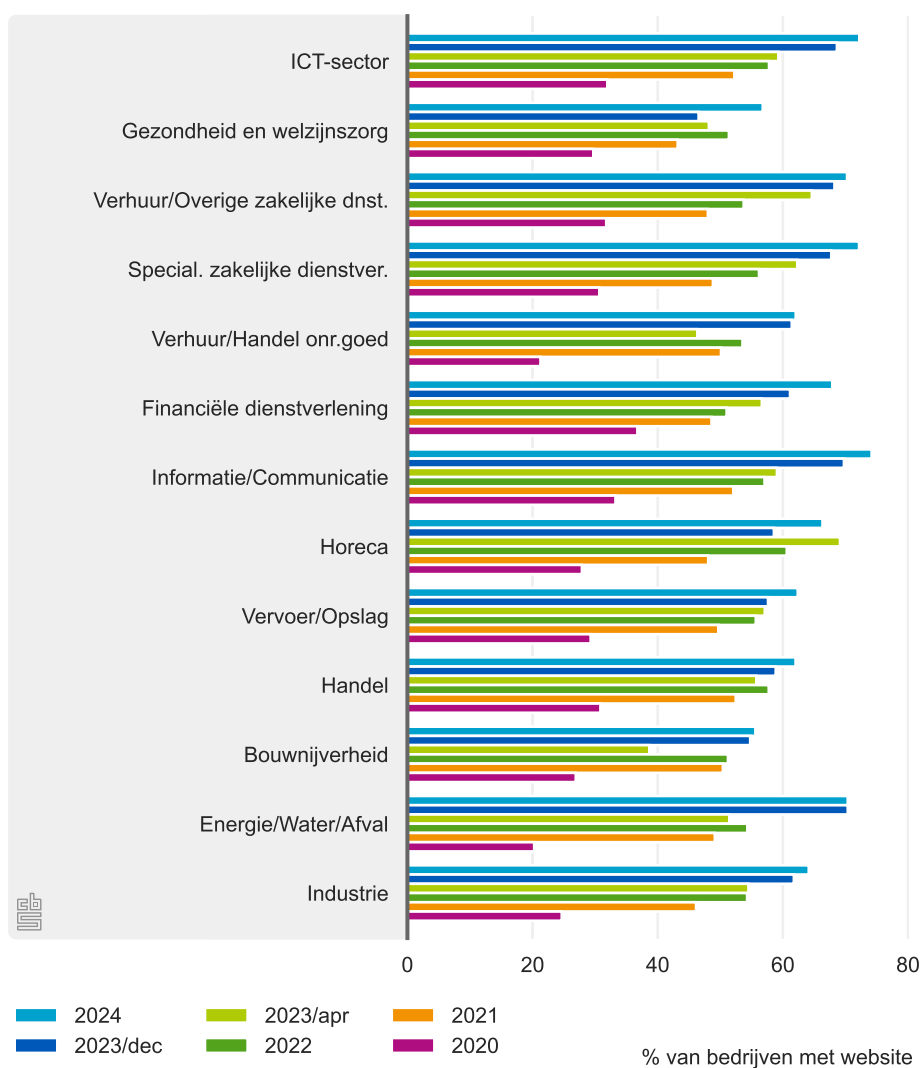


B.3.13 Percentage van bedrijven met website met geslaagde website-test `TLS 0-RTT` per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse



(b) Bedrijfstak

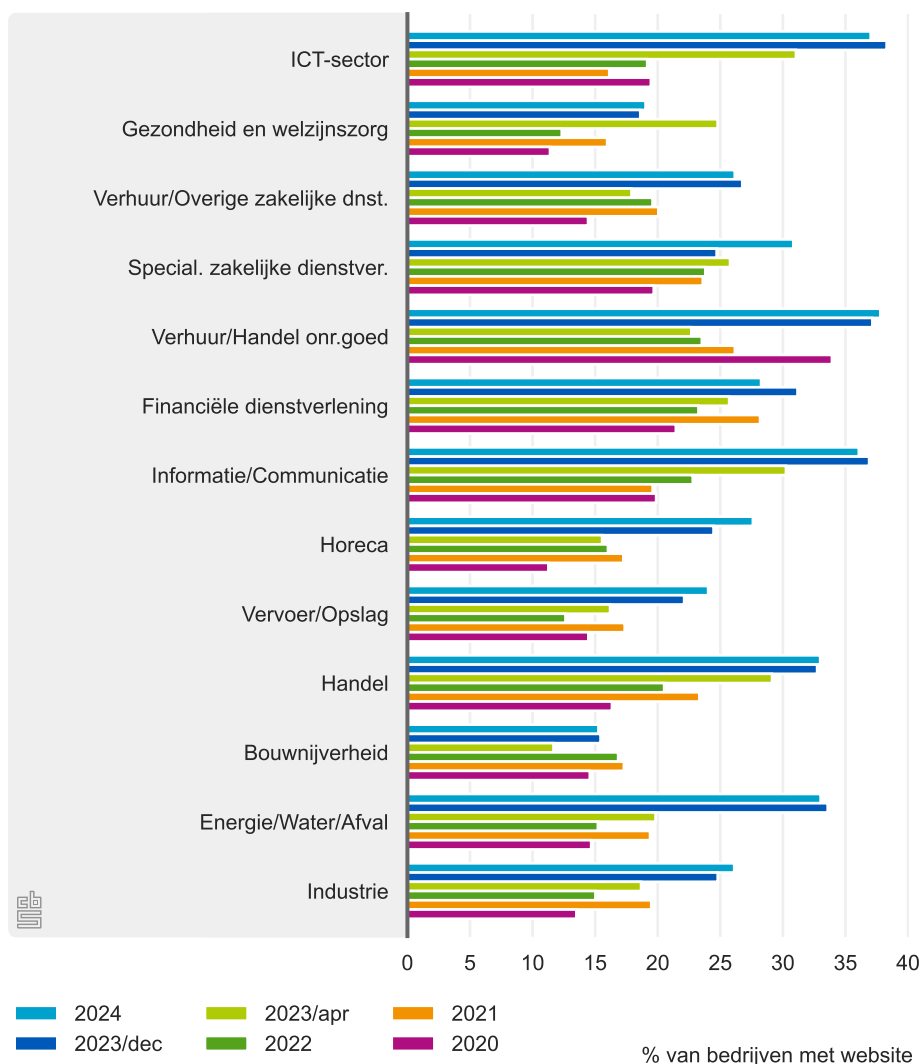


B.3.14 Percentage van bedrijven met website met geslaagde website-test `TLS OSCP-stapeling' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse



(b) Bedrijfstak

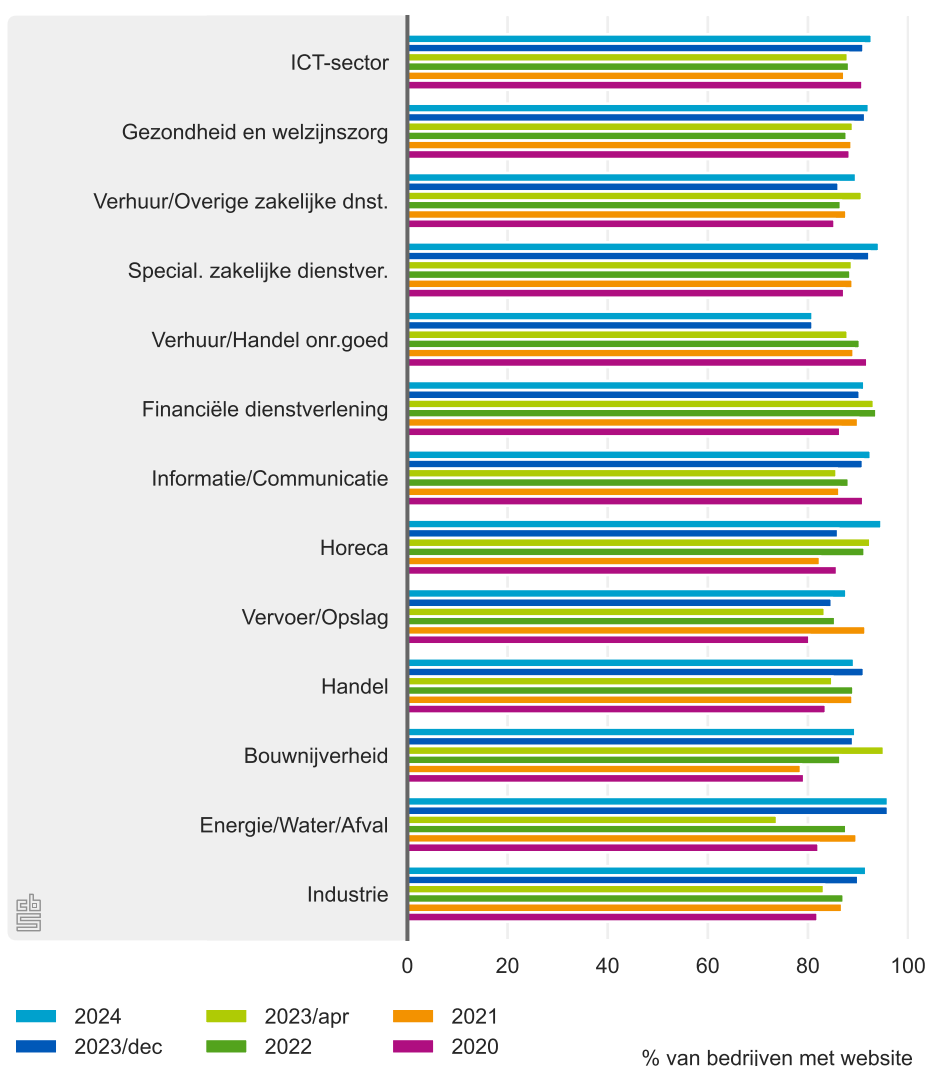


**B.3.15 Percentage van bedrijven met website met geslaagde website-test
`Vertrouwensketen van certificaat' per bedrijfsgrootteklasse (a) en
bedrijfstak (b).**

(a) Bedrijfsgrootteklasse



(b) Bedrijfstak

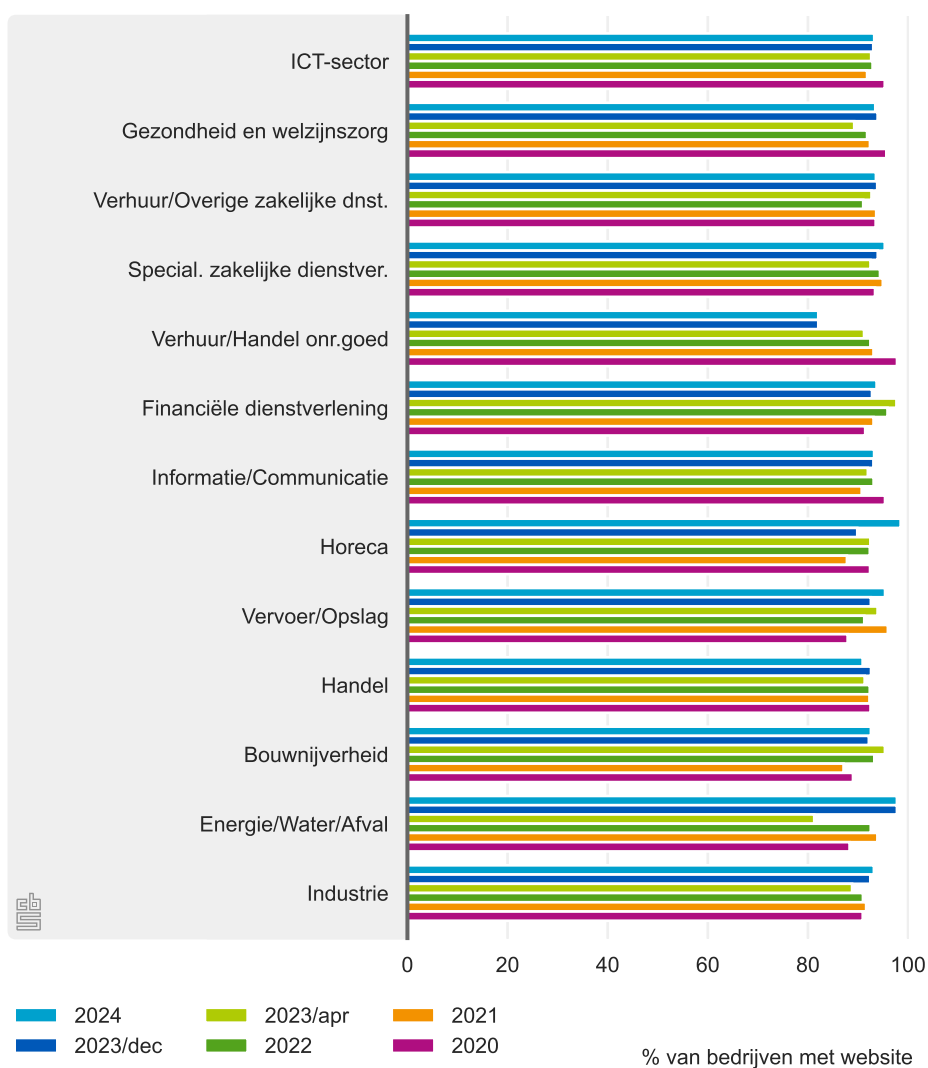


B.3.16 Percentage van bedrijven met website met geslaagde website-test 'Publieke sleutel van certificaat' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse



(b) Bedrijfstak

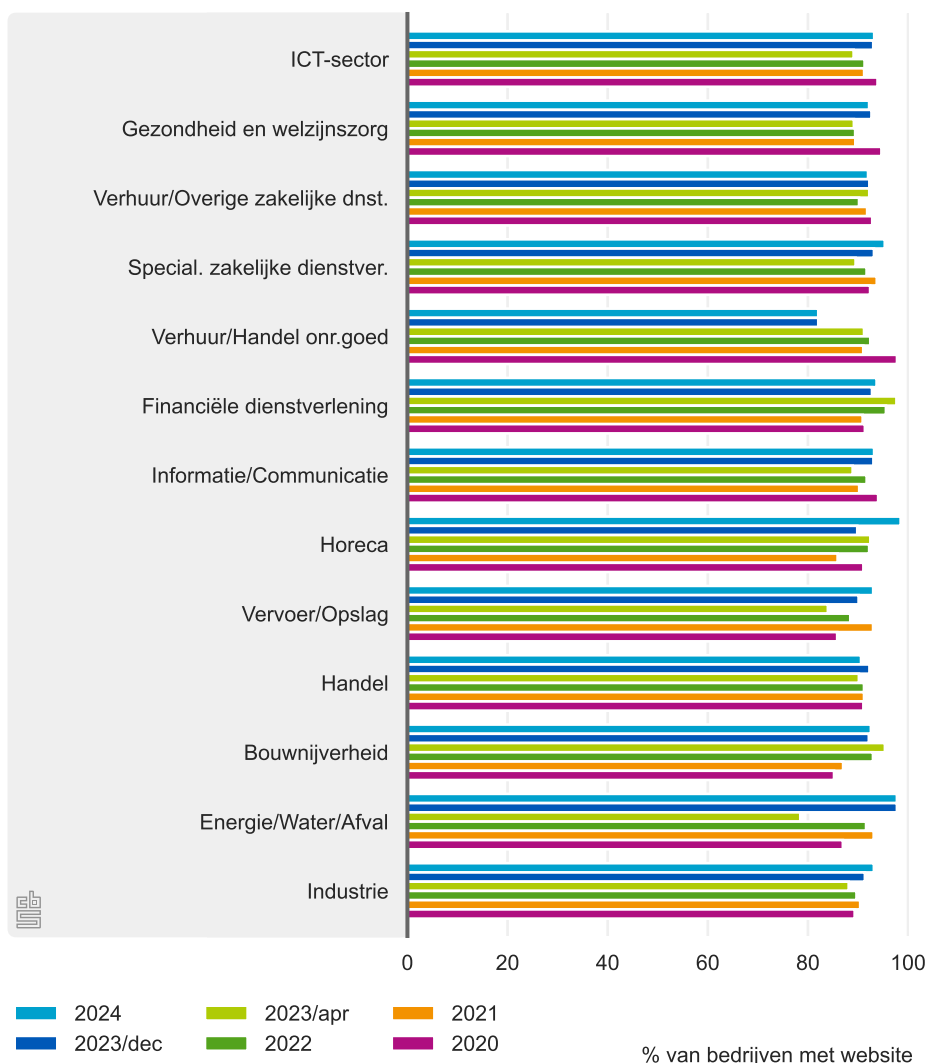


**B.3.17 Percentage van bedrijven met website met geslaagde website-test
'Handtekening van certificaat' per bedrijfsgrootteklasse (a) en bedrijfstak
(b).**

(a) Bedrijfsgrootteklasse



(b) Bedrijfstak

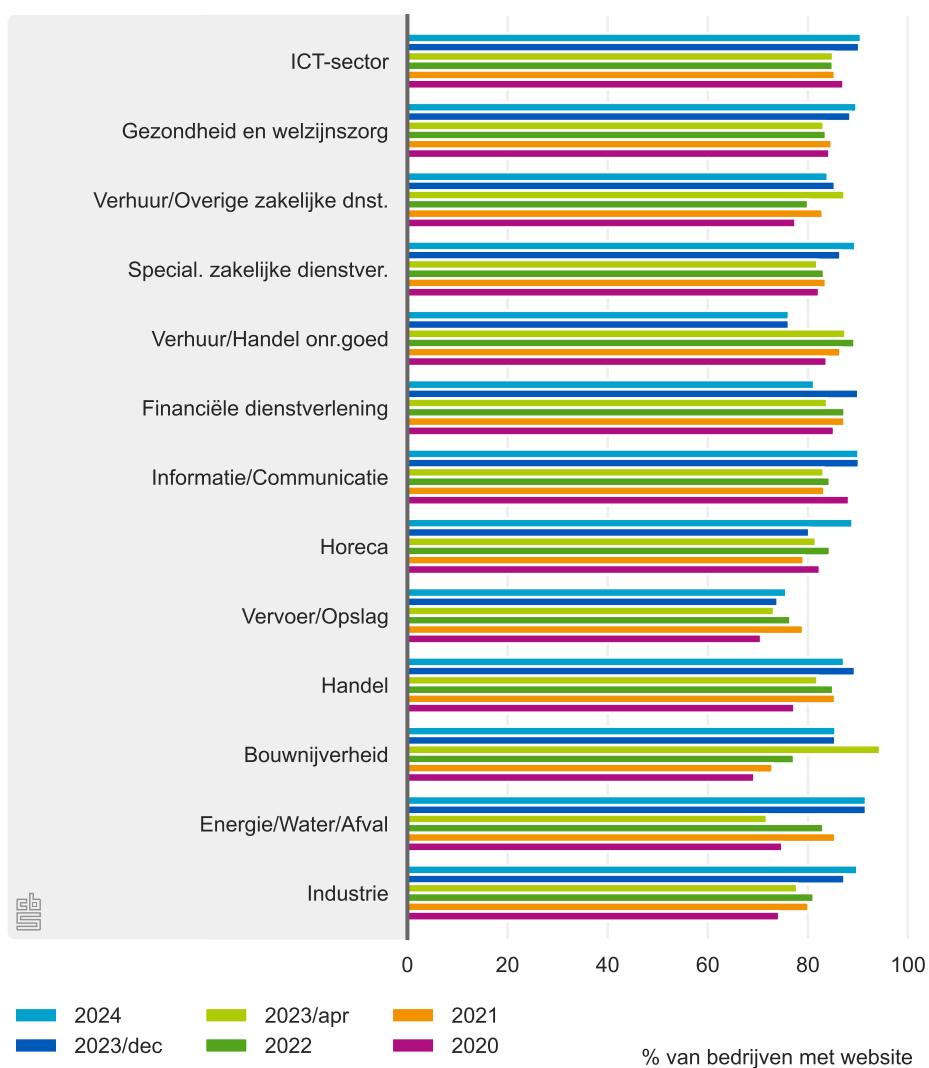


**B.3.18 Percentage van bedrijven met website met geslaagde website-test
`Domeinnaam op certificaat' per bedrijfsgrootteklasse (a) en bedrijfstak (b).**

(a) Bedrijfsgrootteklasse

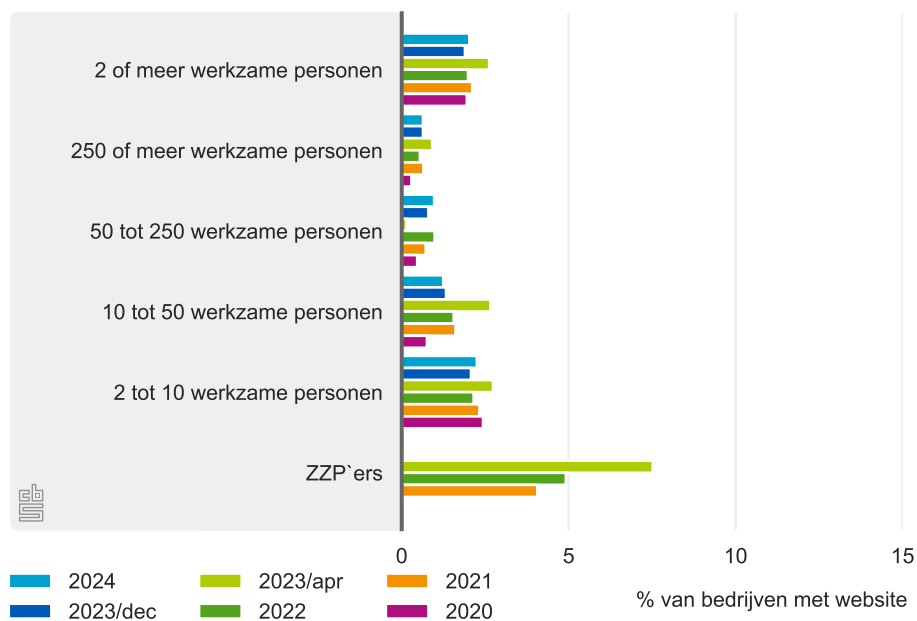


(b) Bedrijfstak

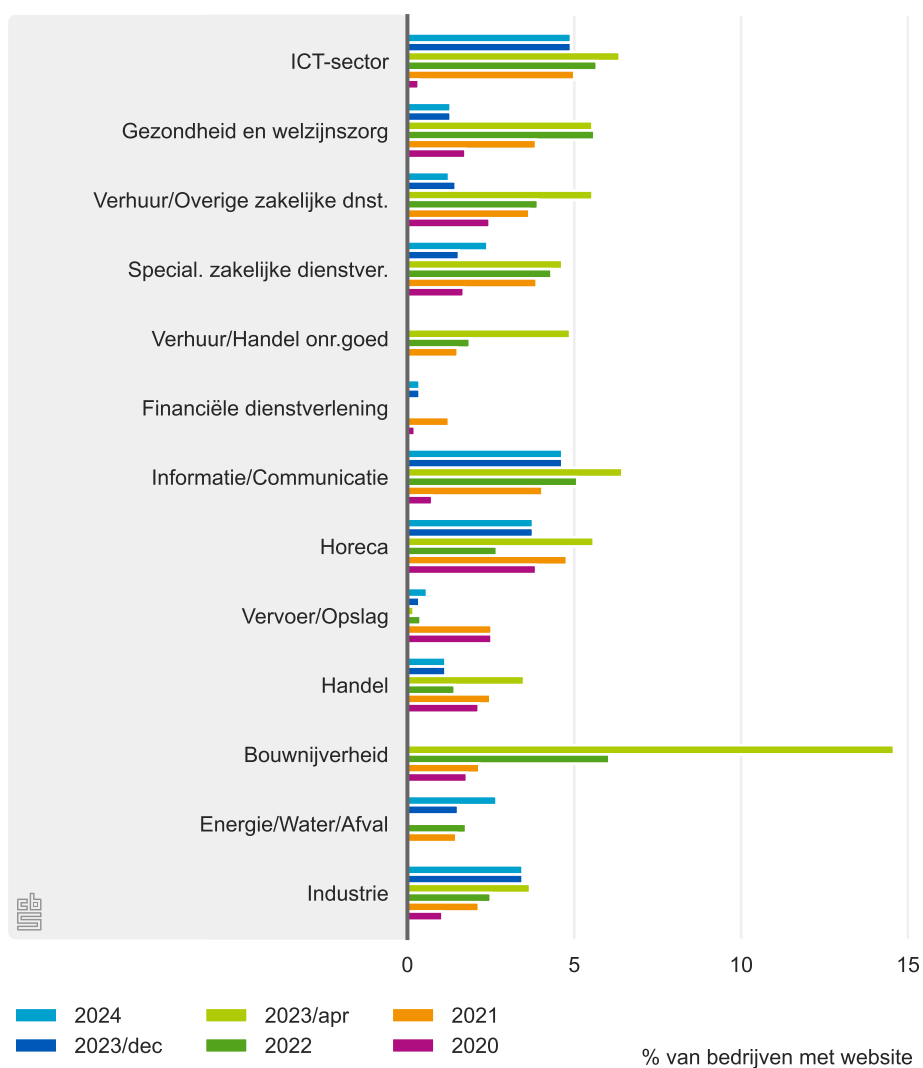


B.3.19 Percentage van bedrijven met website met geslaagde website-test `DANE aanwezig' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse

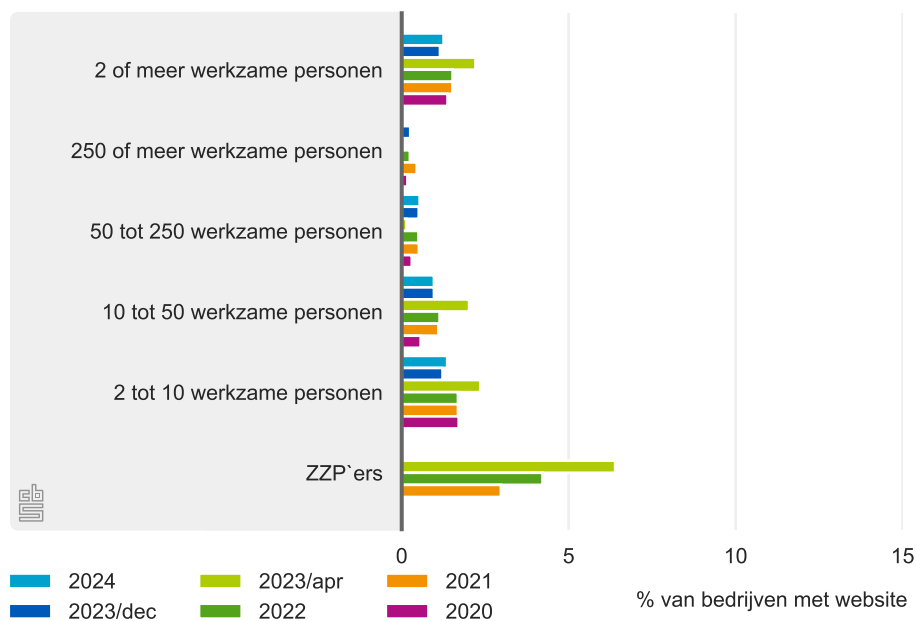


(b) Bedrijfstak

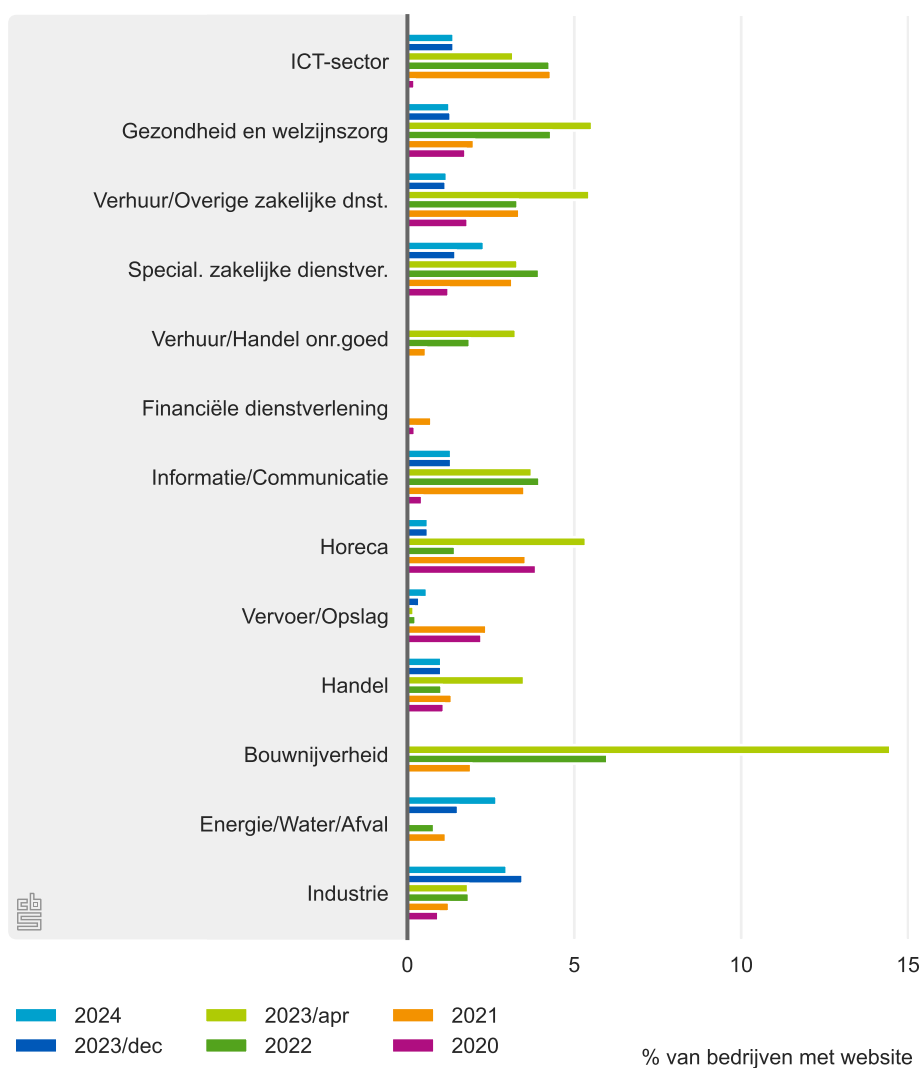


B.3.20 Percentage van bedrijven met website met geslaagde website-test 'DANE geldigheid' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse



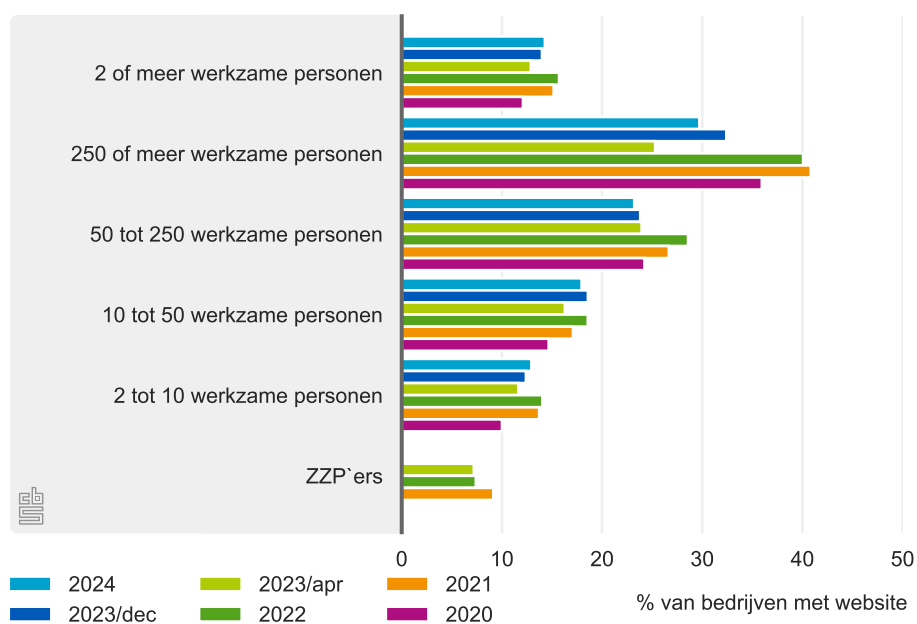
(b) Bedrijfstak



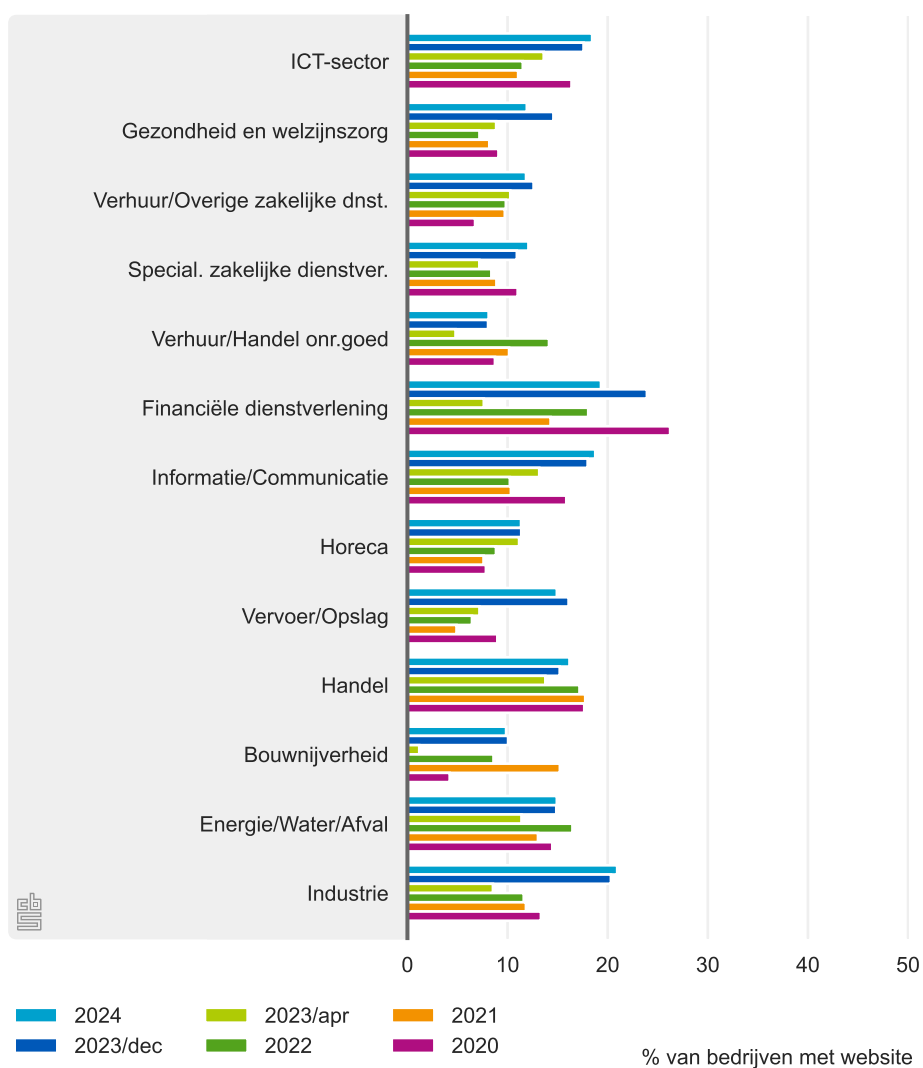
B.4 Website-testuitslagen voor categorie 'Beveiligingsopties'

B.4.1 Percentage van bedrijven met website met geslaagde website-test `X-Frame options` per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse

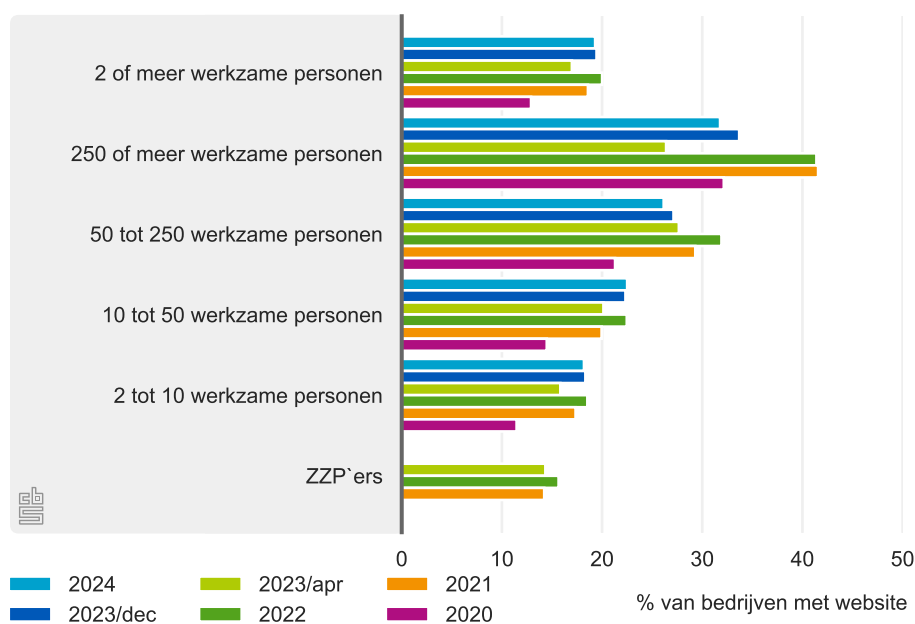


(b) Bedrijfstak

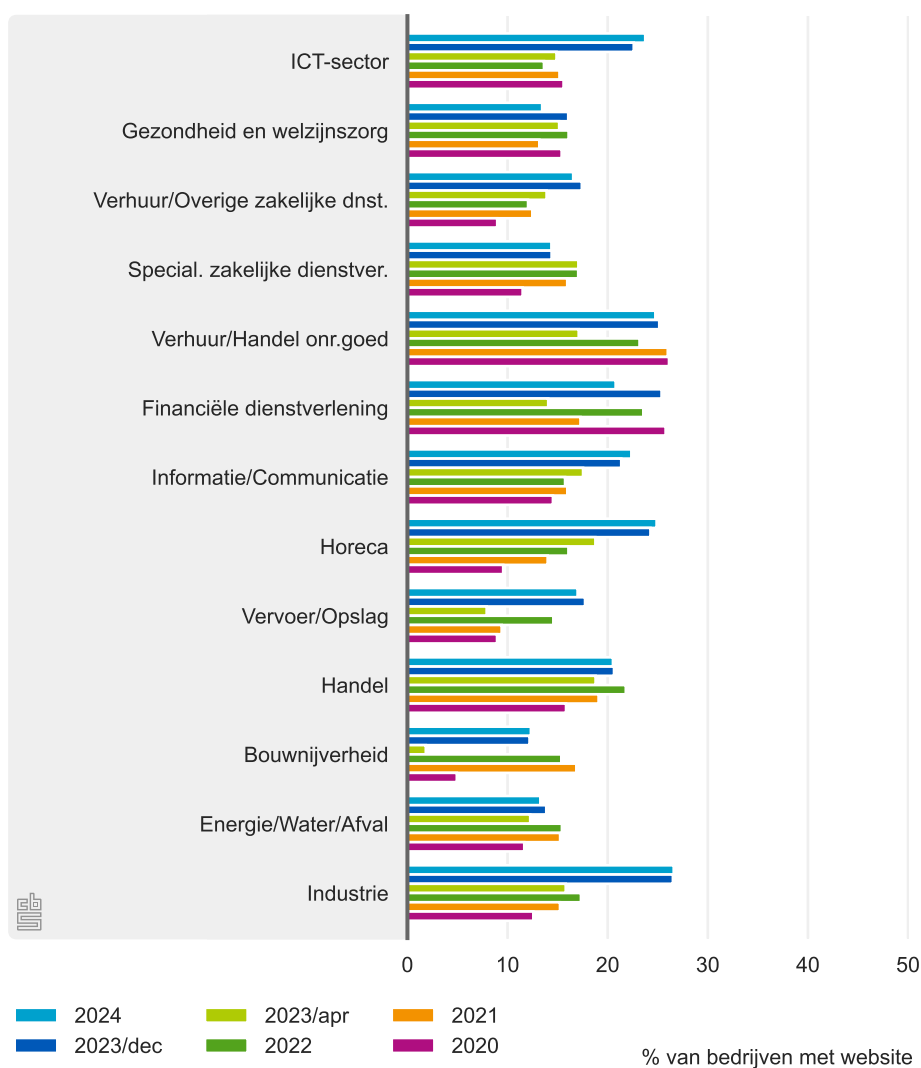


B.4.2 Percentage van bedrijven met website met geslaagde website-test 'X-Content-Type options' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse



(b) Bedrijfstak

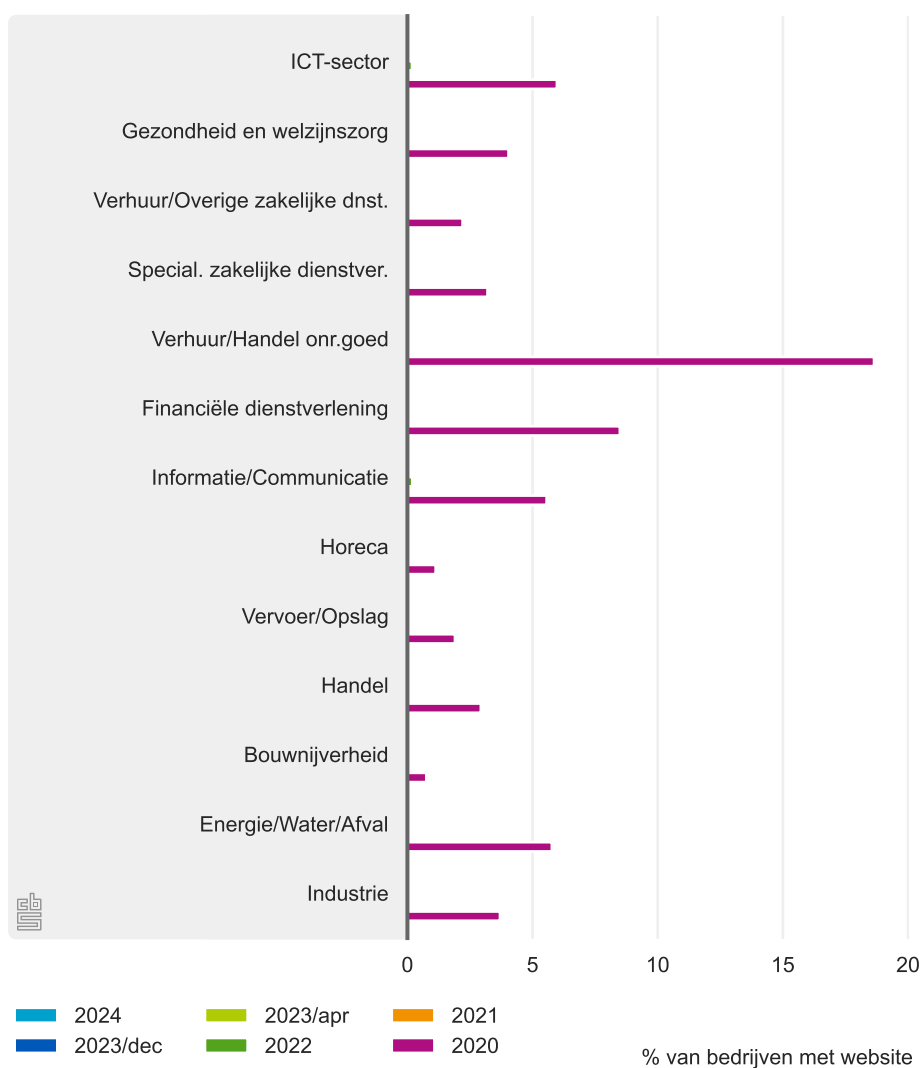


B.4.3 Percentage van bedrijven met website met geslaagde website-test 'Content-security policy' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse

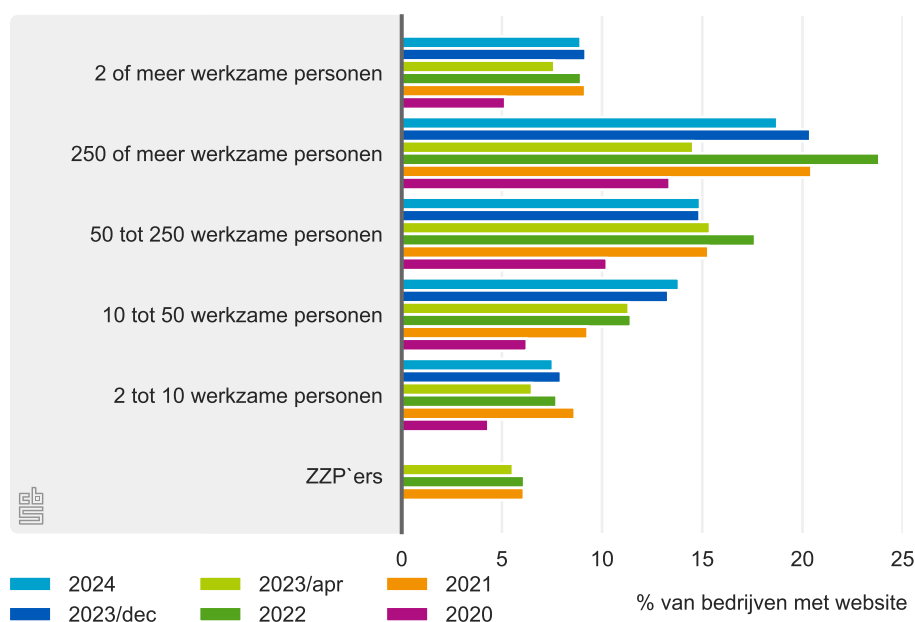


(b) Bedrijfstak

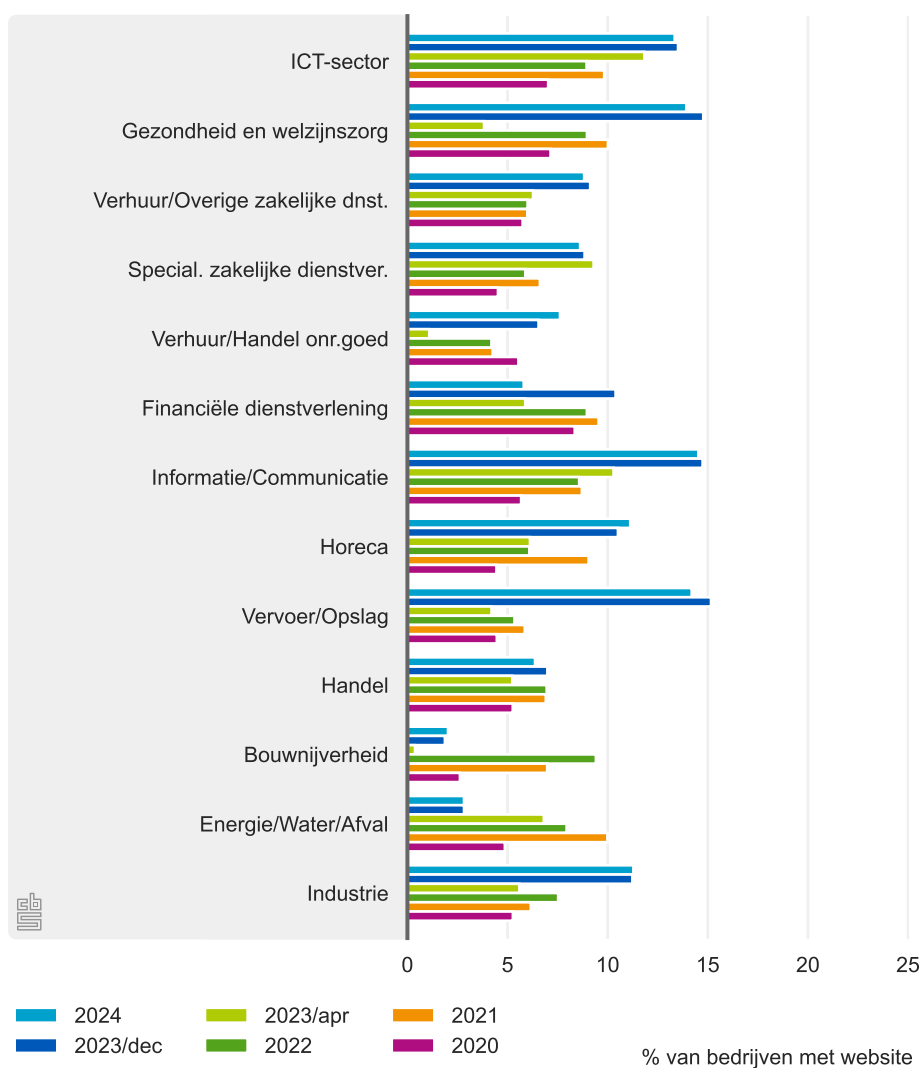


B.4.4 Percentage van bedrijven met website met geslaagde website-test 'Referred Policy aanwezig' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse



(b) Bedrijfstak



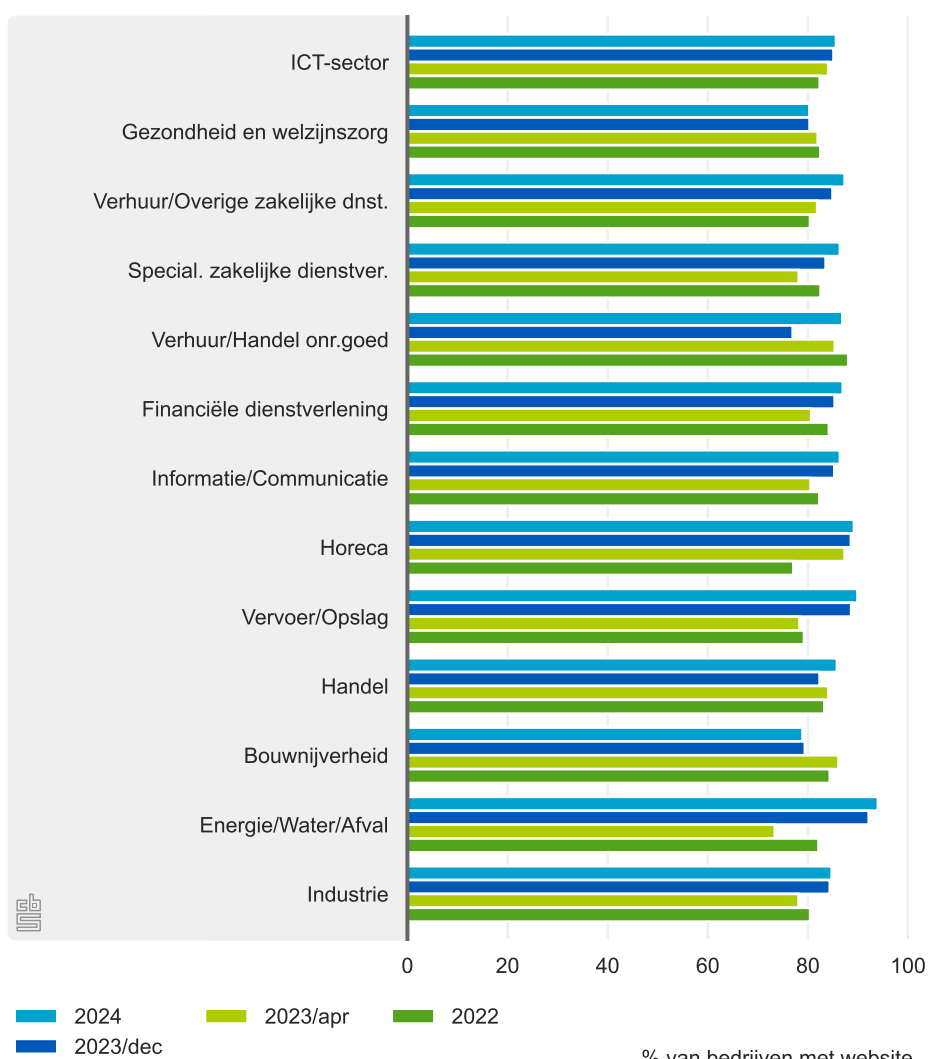
B.5 Website-testuitslagen voor categorie `RPKI`

B.5.1 Percentage van bedrijven met website met geslaagde website-test `RPKI Route Oorsprong Autorisatie bestaat' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse



(b) Bedrijfstak

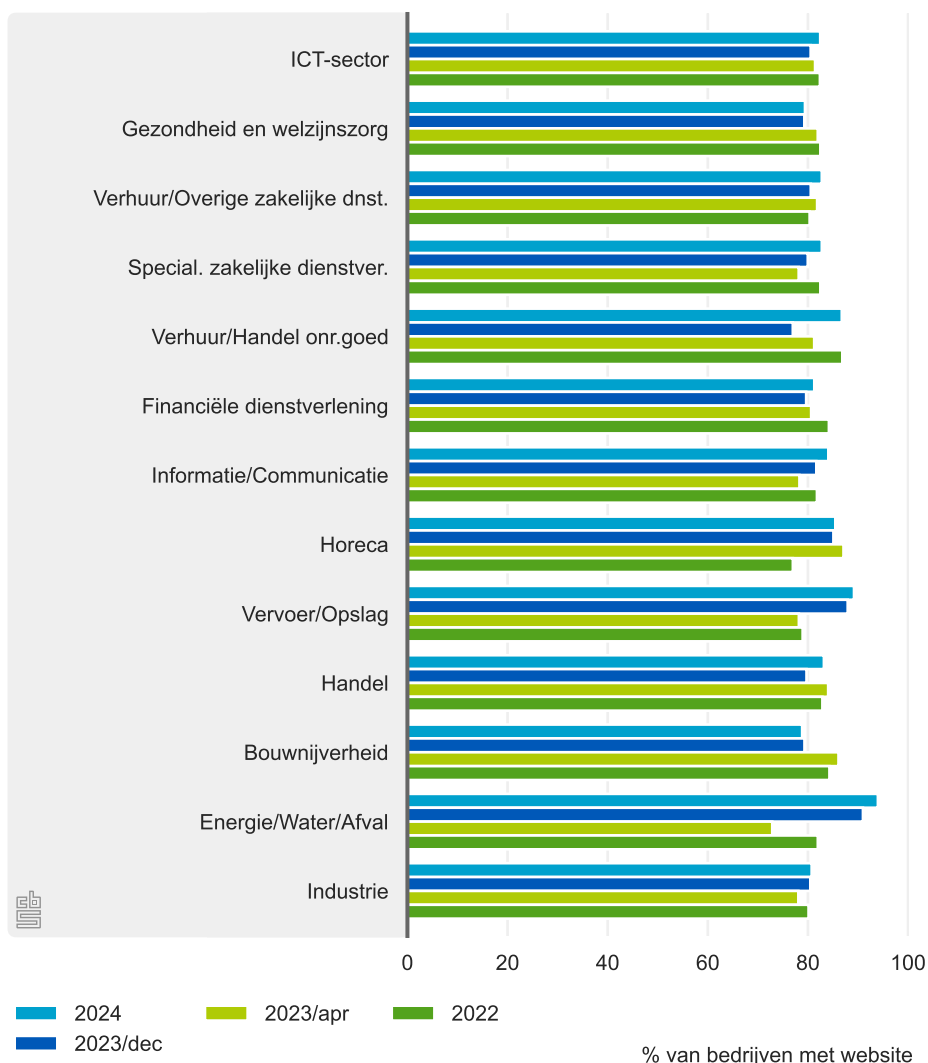


B.5.2 Percentage van bedrijven met website met geslaagde website-test `RPKI Route Oorsprong Autorisatie is geldig' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse

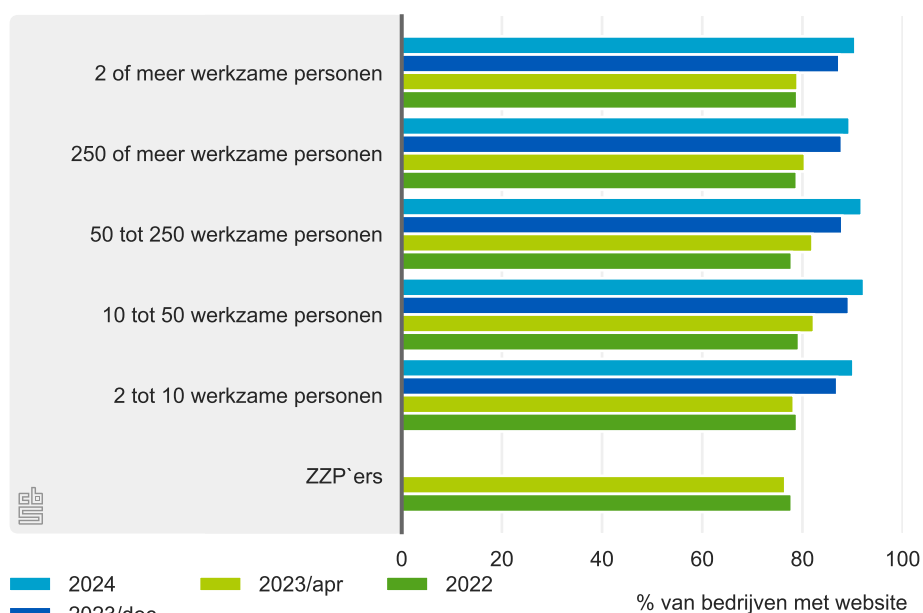


(b) Bedrijfstak

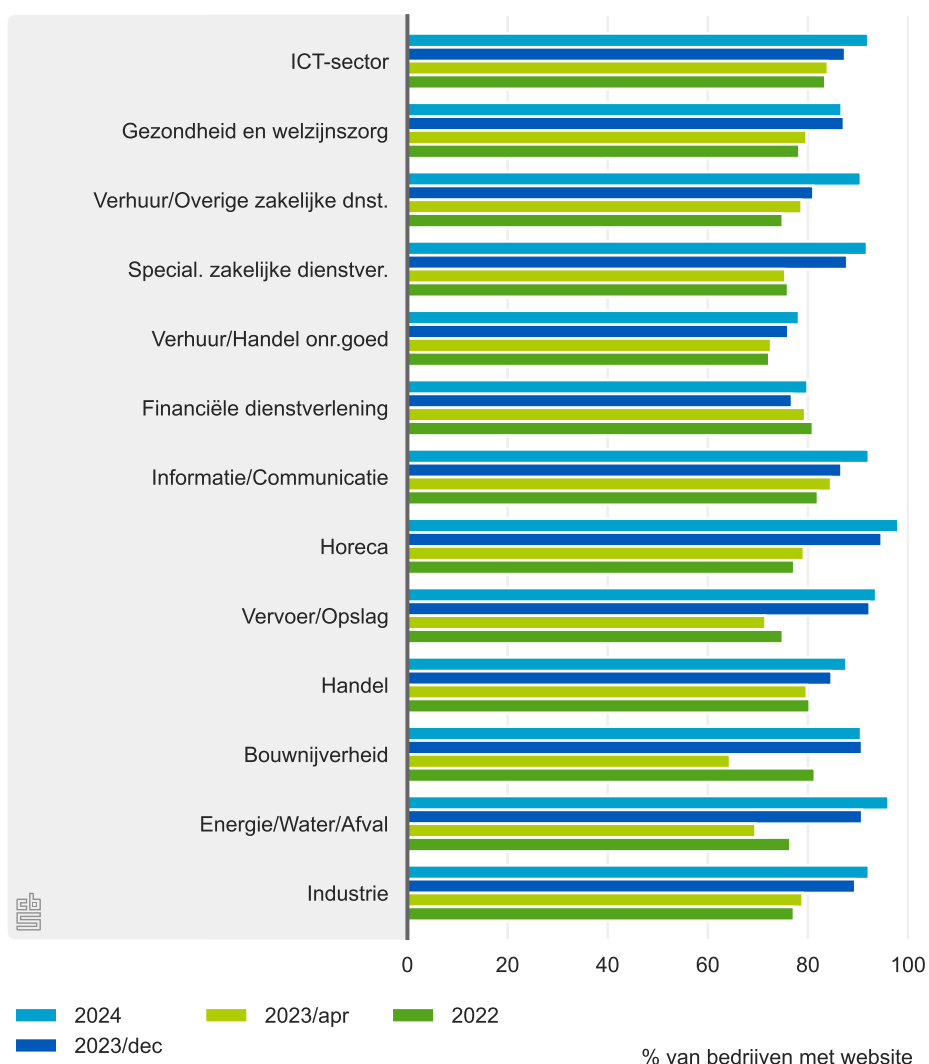


B.5.3 Percentage van bedrijven met website met geslaagde website-test `RPKI voor nameserver bestaat` per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse

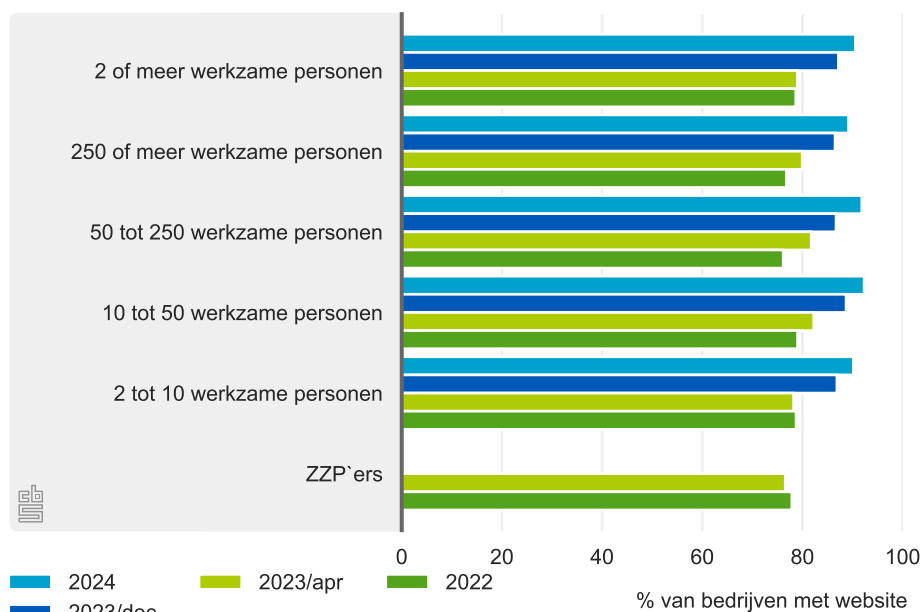


(b) Bedrijfstak

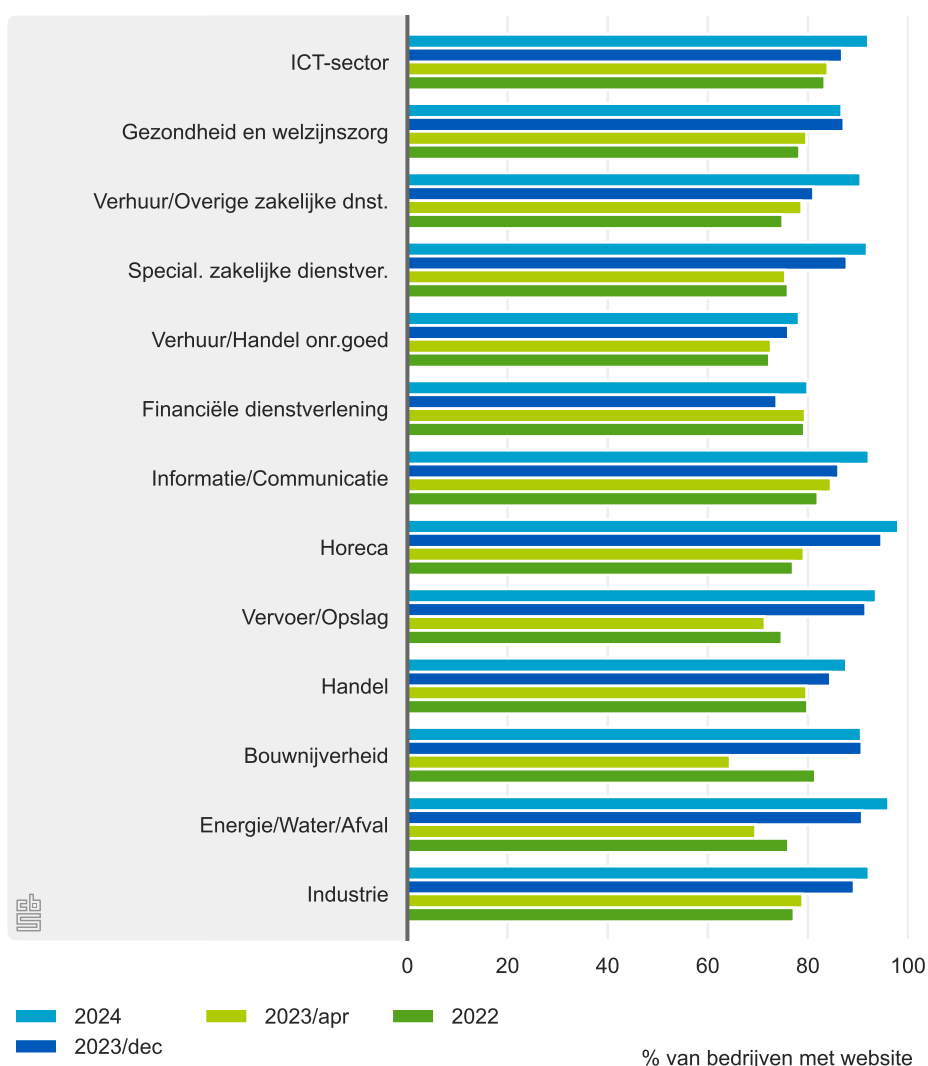


B.5.4 Percentage van bedrijven met website met geslaagde website-test 'Geldigheid van RPKI voor nameserver' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse



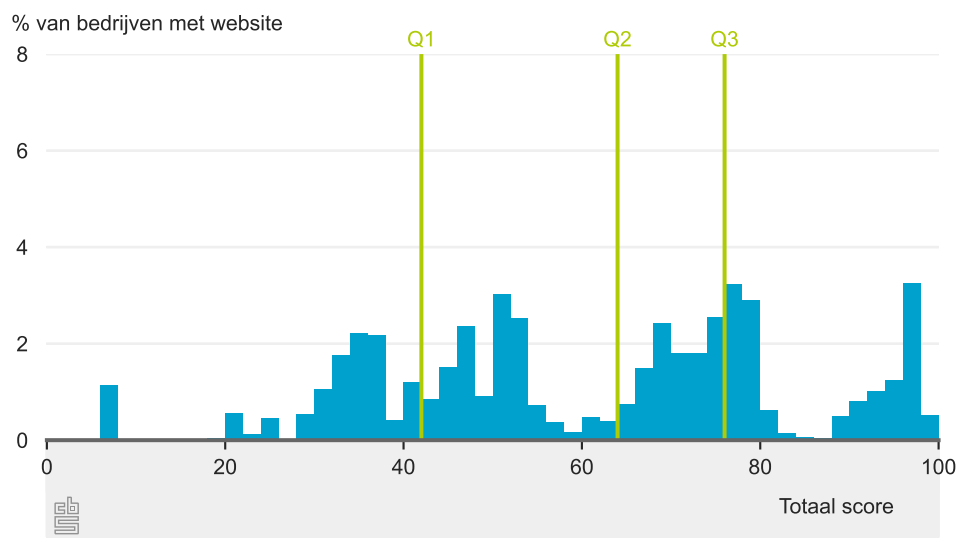
(b) Bedrijfstak



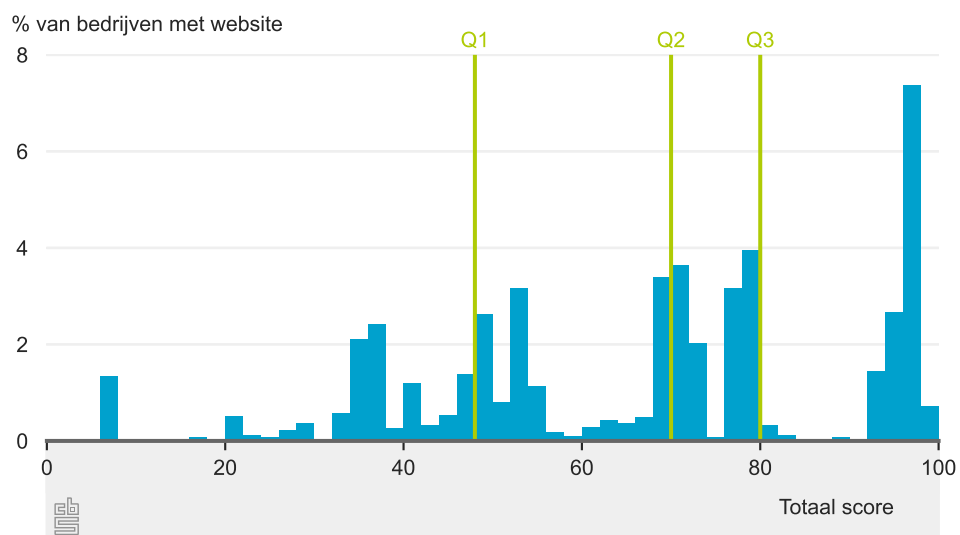
B.6 Website-scan eindscoreverderlingen

B.6.1 1) Verdeling van de website-scan Internet.nl-score voor alle bedrijven van Nederland...

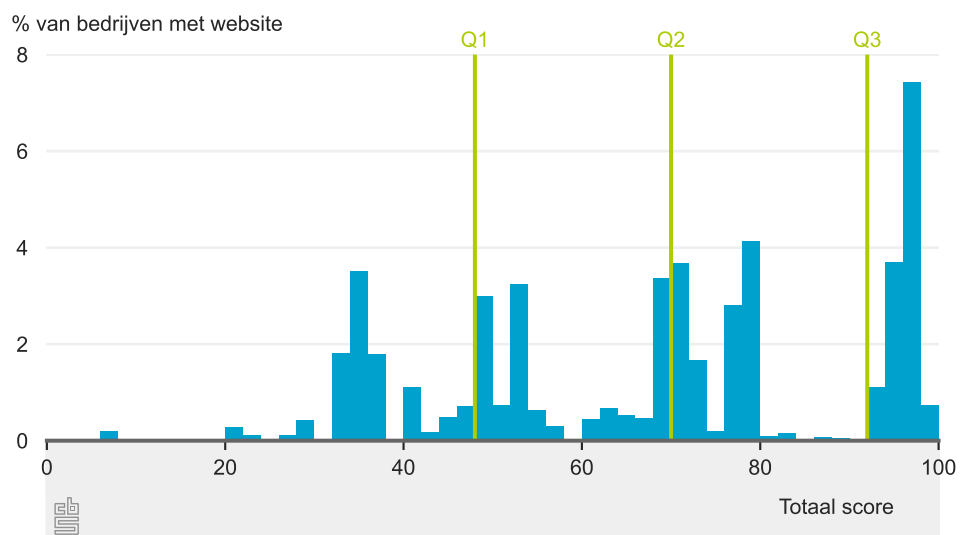
(a) Scoreverdeling voor oktober, 2020



(b) Scoreverdeling voor maart, 2021

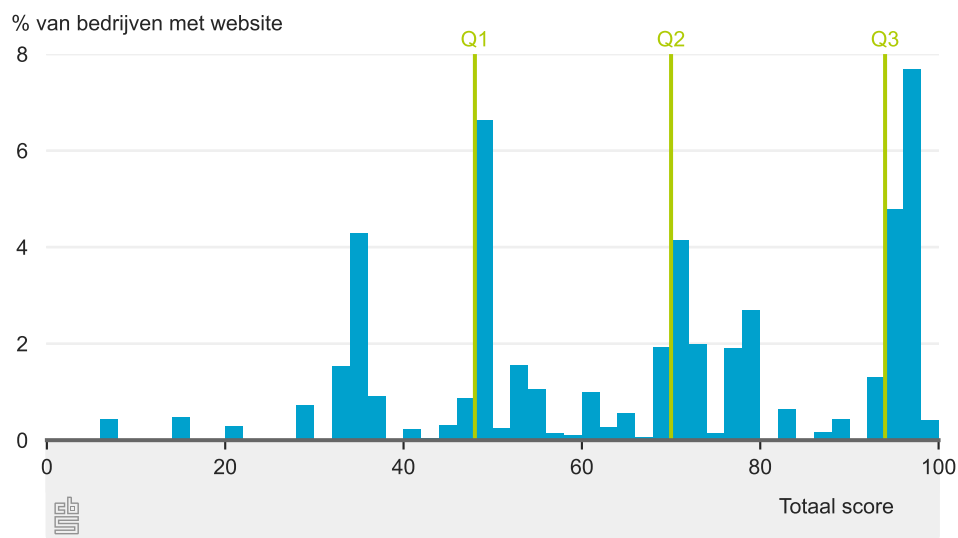


(c) Scoreverdeling voor december, 2022

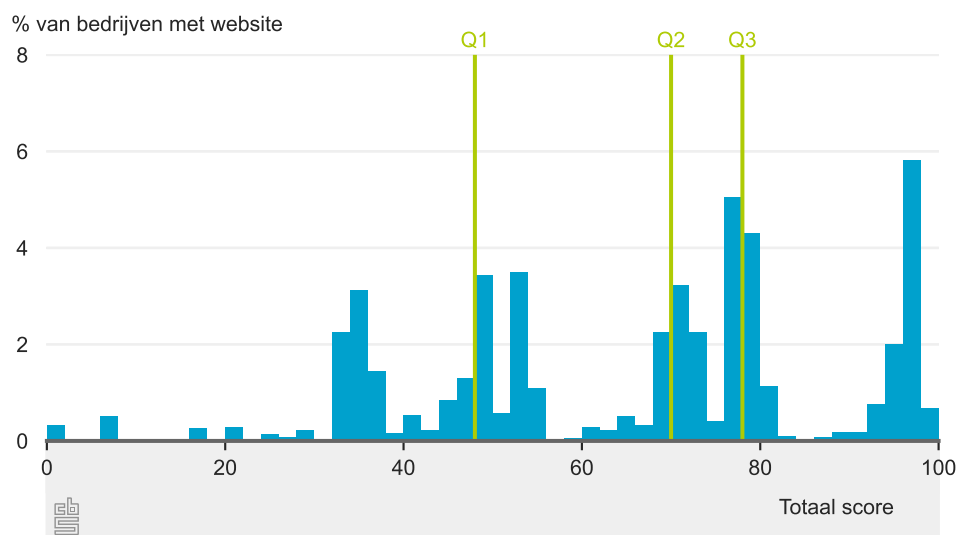


B.6.1 2) Verdeling van de website-scan Internet.nl-score voor alle bedrijven van Nederland

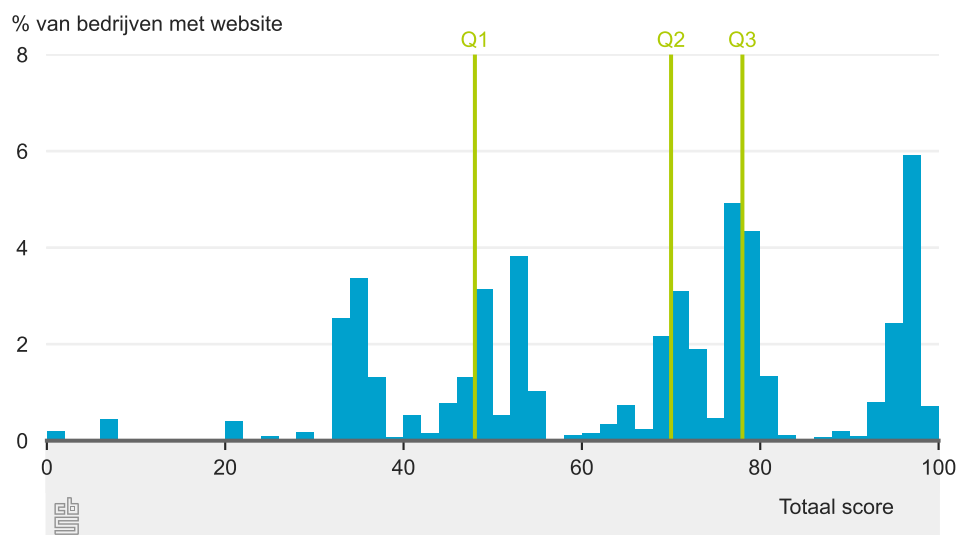
(d) Scoreverdeling voor april, 2023



(e) Scoreverdeling voor december, 2023



(f) Scoreverdeling voor april, 2024



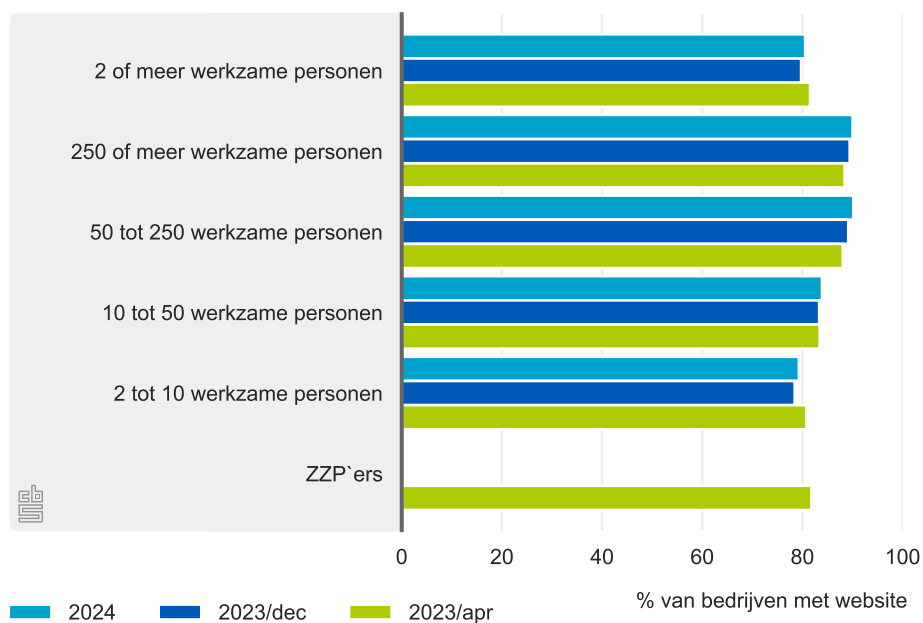
Bijlage C

Alle e-mailtestuitslagen

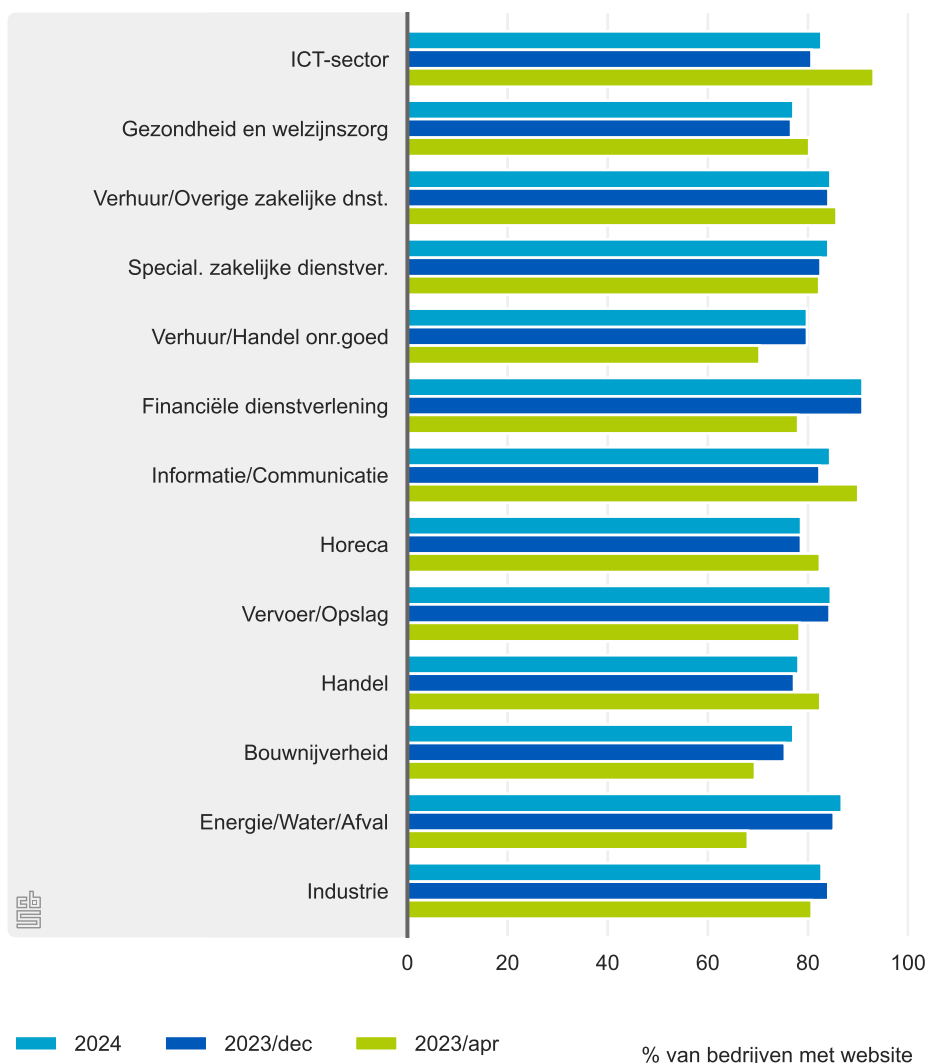
C.1 E-mailtestuitslagen voor categorie `IPv6'

**C.1.1 Percentage van bedrijven met website met geslaagde e-mailtest
'IPv6-adressen voor nameservers' per bedrijfsgrootteklasse (a) en bedrijfstak
(b).**

(a) Bedrijfsgrootteklasse

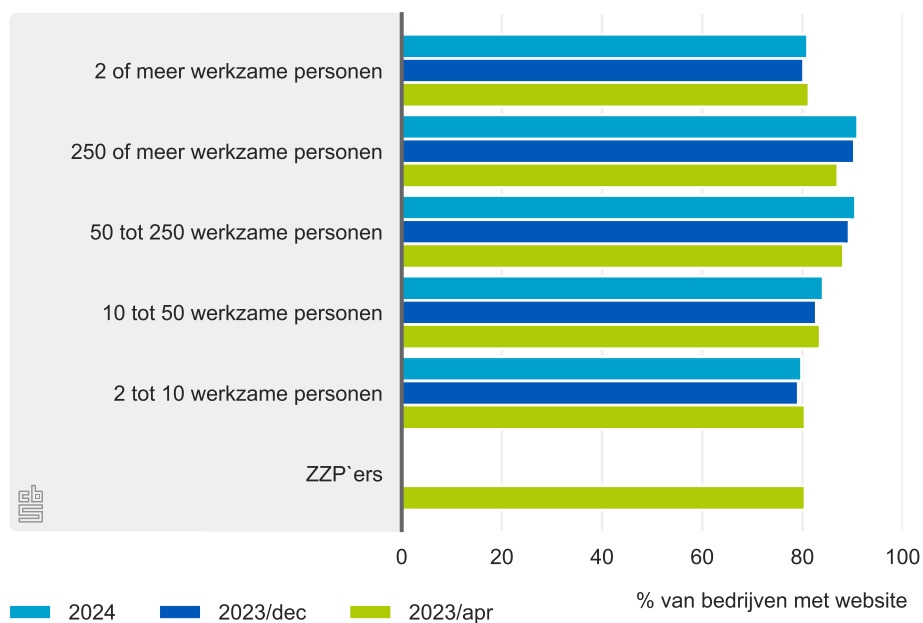


(b) Bedrijfstak

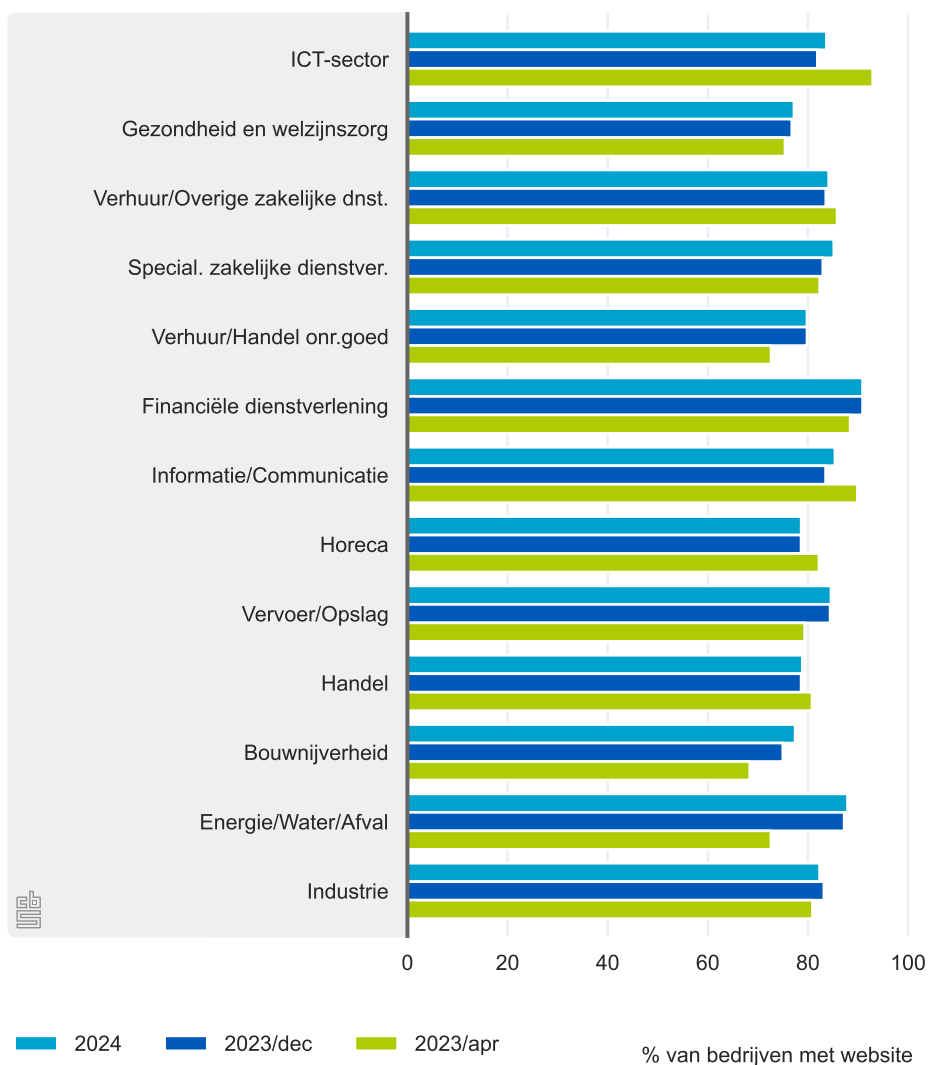


**C.1.2 Percentage van bedrijven met website met geslaagde e-mailtest
`IPv6-bereikbaarheid van nameservers' per bedrijfsgrootteklasse (a) en
bedrijfstak (b).**

(a) Bedrijfsgrootteklasse

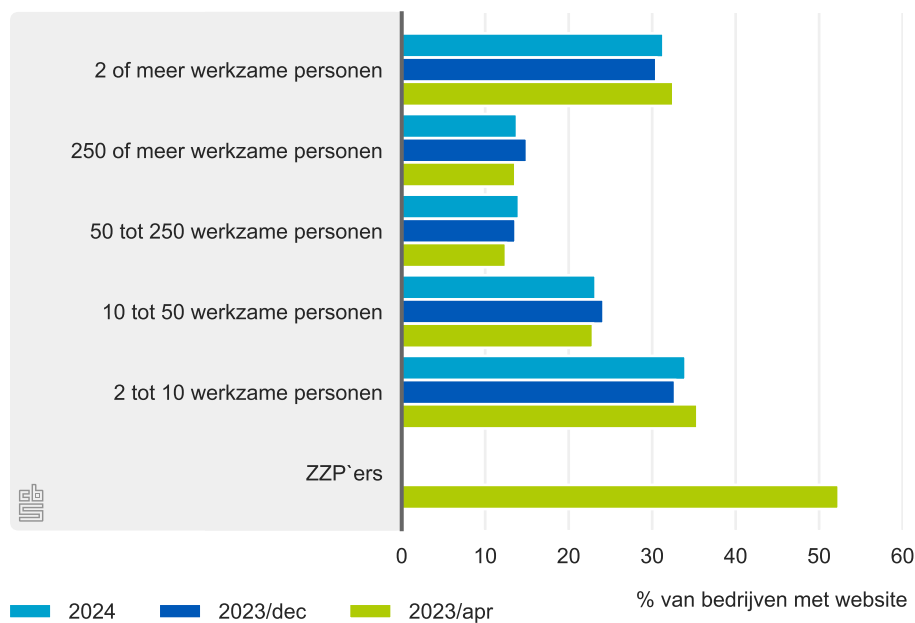


(b) Bedrijfstak

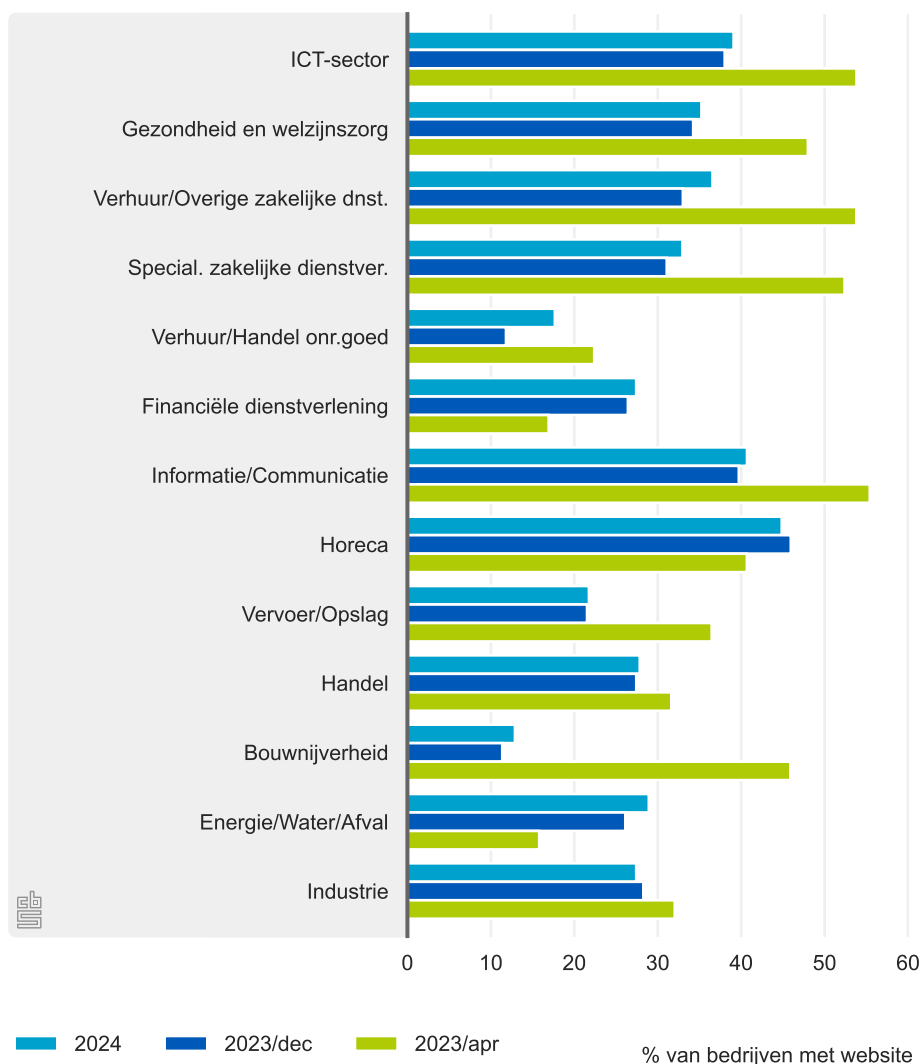


C.1.3 Percentage van bedrijven met website met geslaagde e-mailtest `IPv6-adres voor mailservers' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse

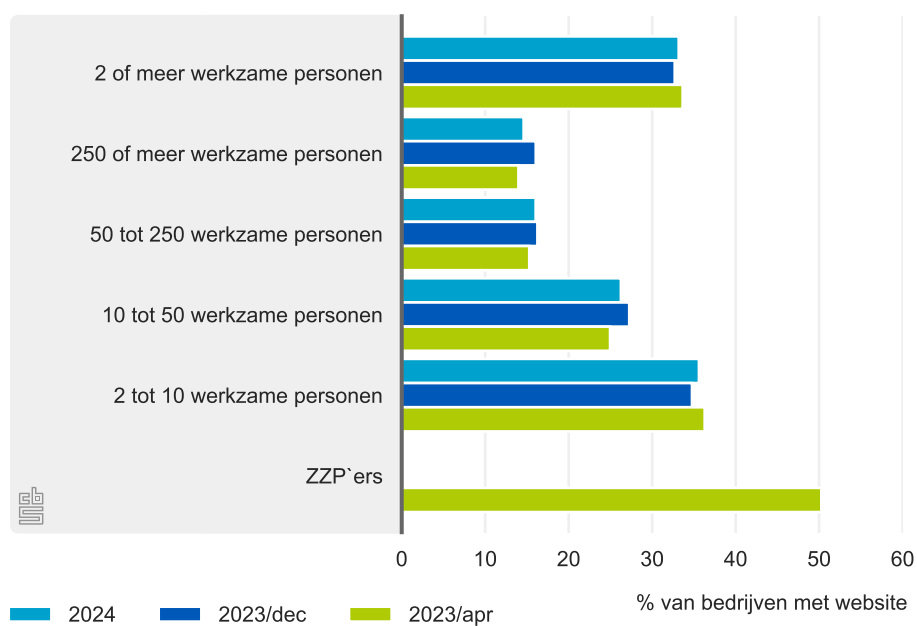


(b) Bedrijfstak

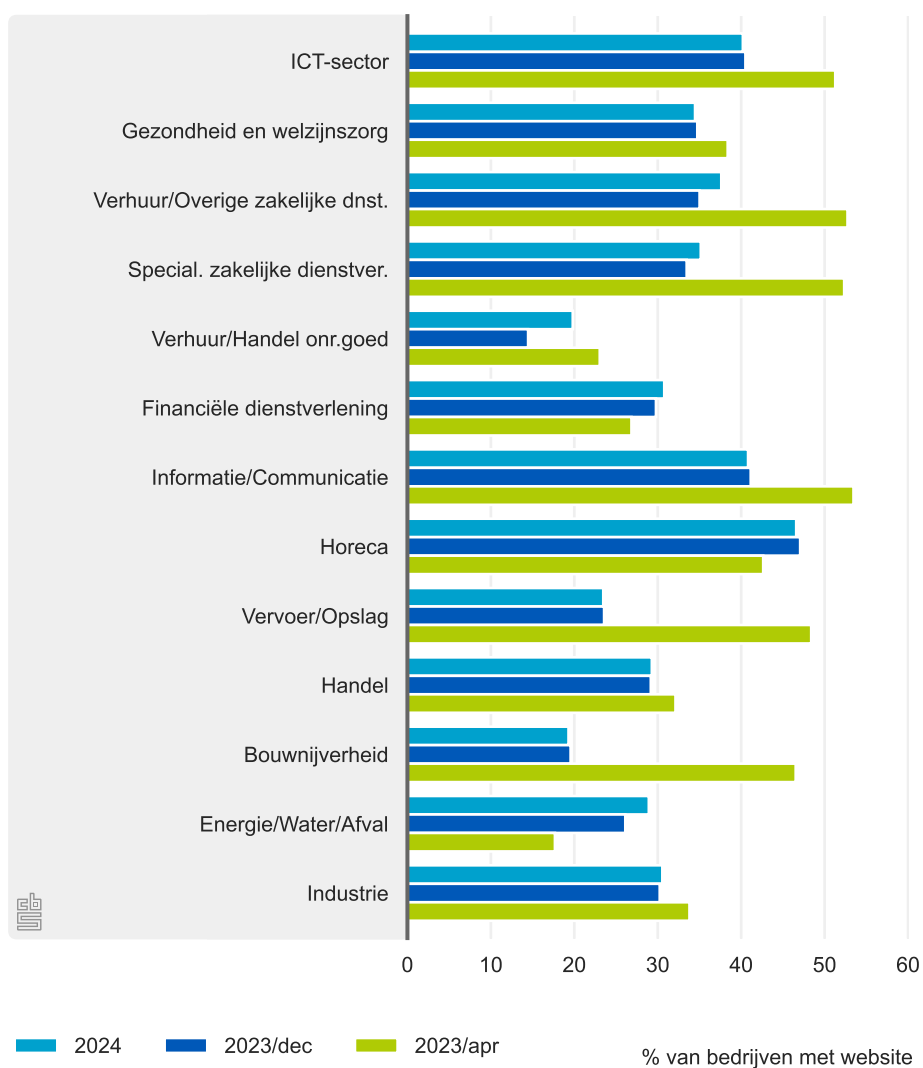


C.1.4 Percentage van bedrijven met website met geslaagde e-mailtest 'IPv6-adres mailservers bereikbaarheid' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse



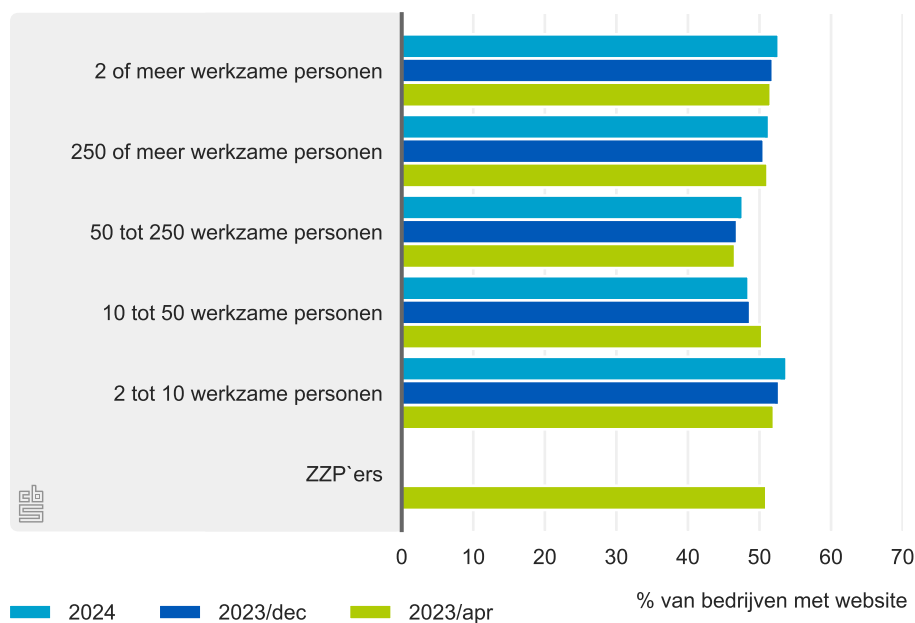
(b) Bedrijfstak



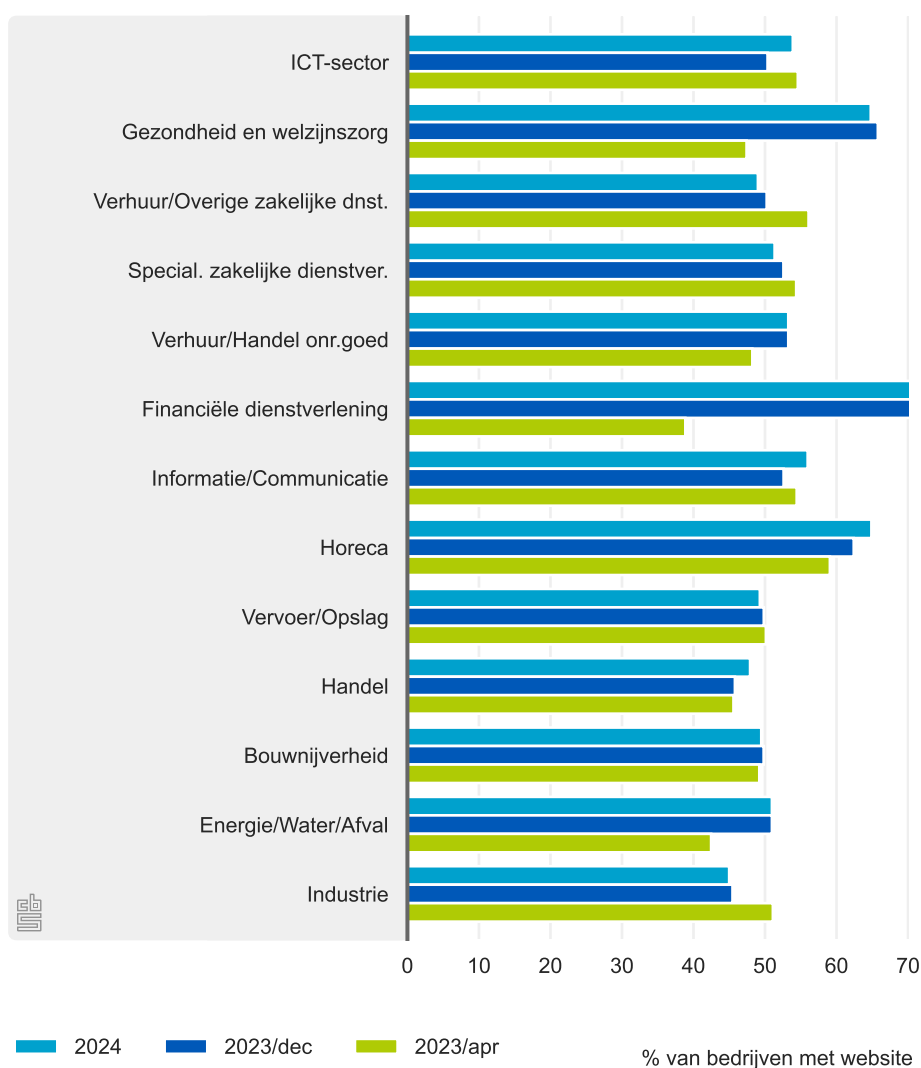
C.2 E-mailtestuitslagen voor categorie `Domeinnaamhandtekening' (DNSSEC)

**C.2.1 Percentage van bedrijven met website met geslaagde e-mailtest
'E-maildomein heeft DNSSEC handtekening' per bedrijfsgrootteklasse (a) en
bedrijfstak (b).**

(a) Bedrijfsgrootteklasse

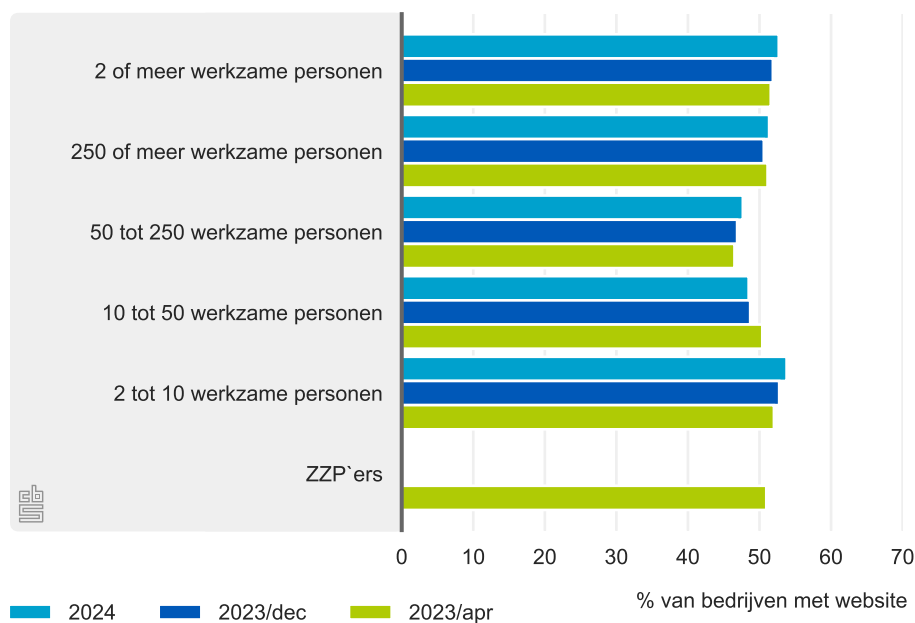


(b) Bedrijfstak

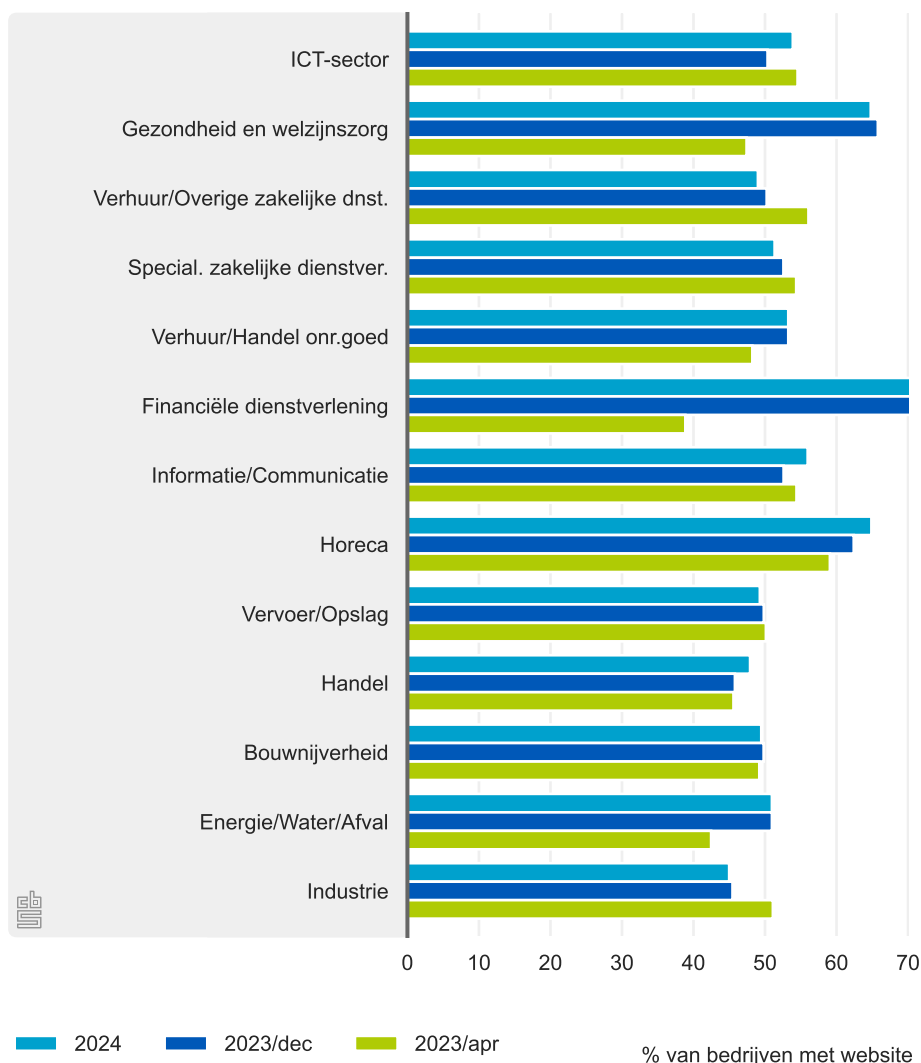


**C.2.2 Percentage van bedrijven met website met geslaagde e-mailtest
'E-maildomein met geldige DNSSEC handtekening' per bedrijfsgrootteklasse
(a) en bedrijfstak (b).**

(a) Bedrijfsgrootteklasse

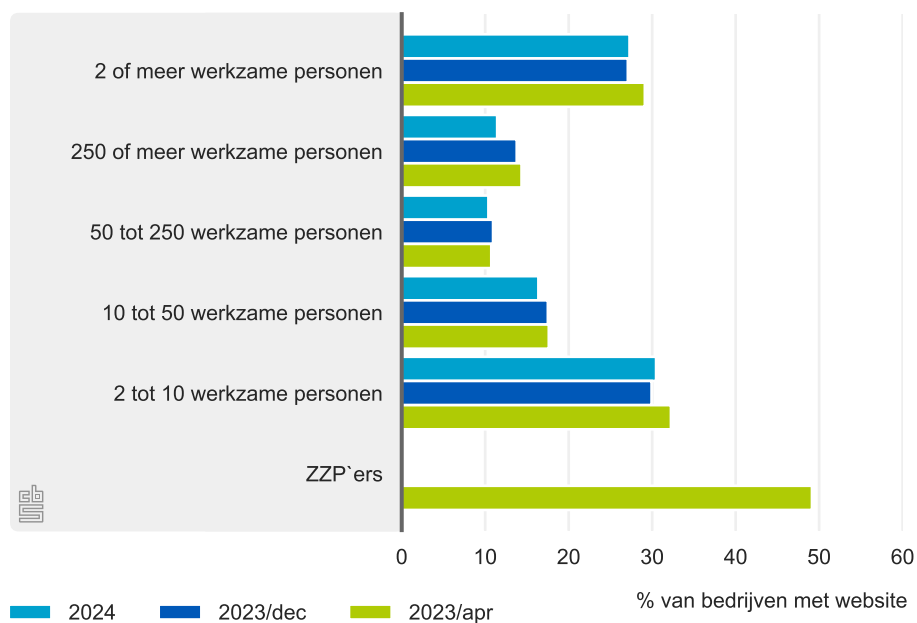


(b) Bedrijfstak

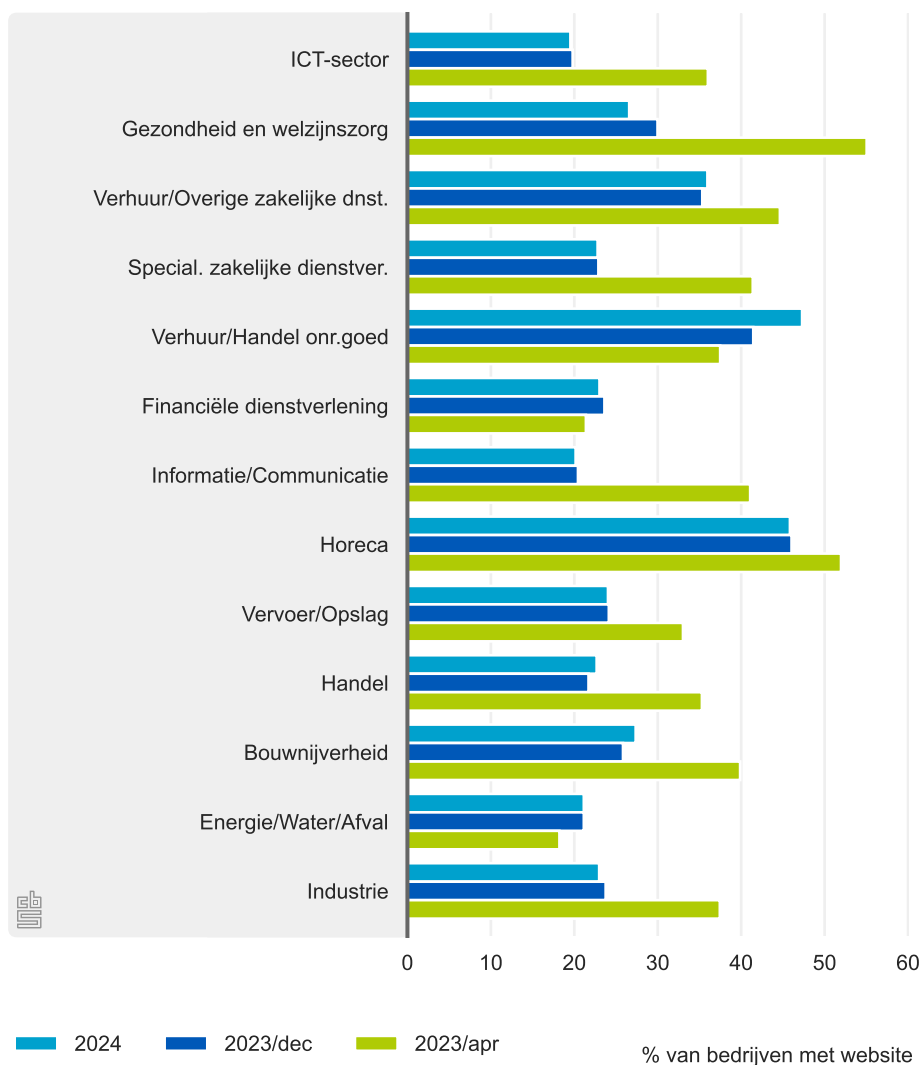


**C.2.3 Percentage van bedrijven met website met geslaagde e-mailtest
'Ontvangende mailserver heeft DNSSEC handtekening' per
bedrijfsgrootteklasse (a) en bedrijfstak (b).**

(a) Bedrijfsgrootteklasse

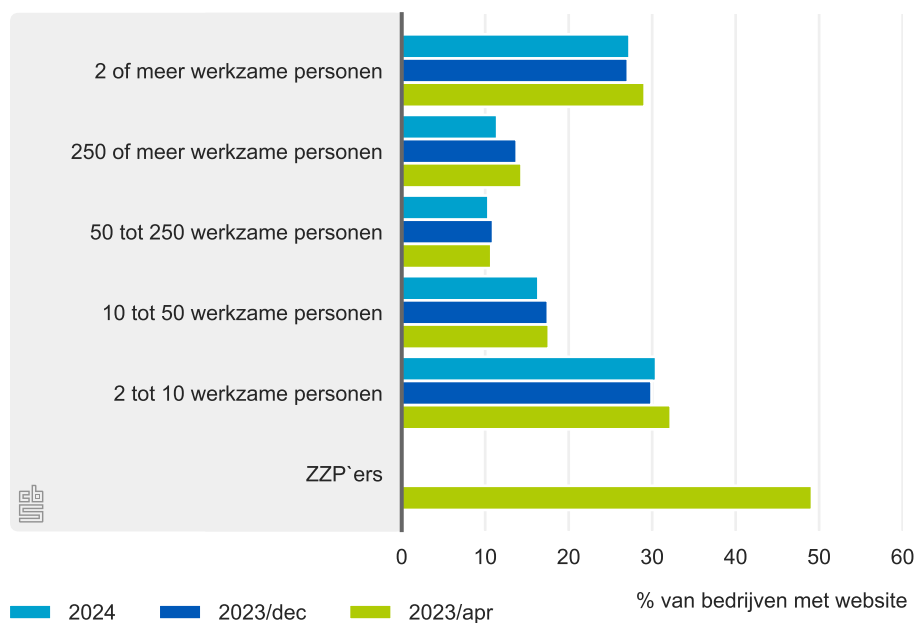


(b) Bedrijfstak

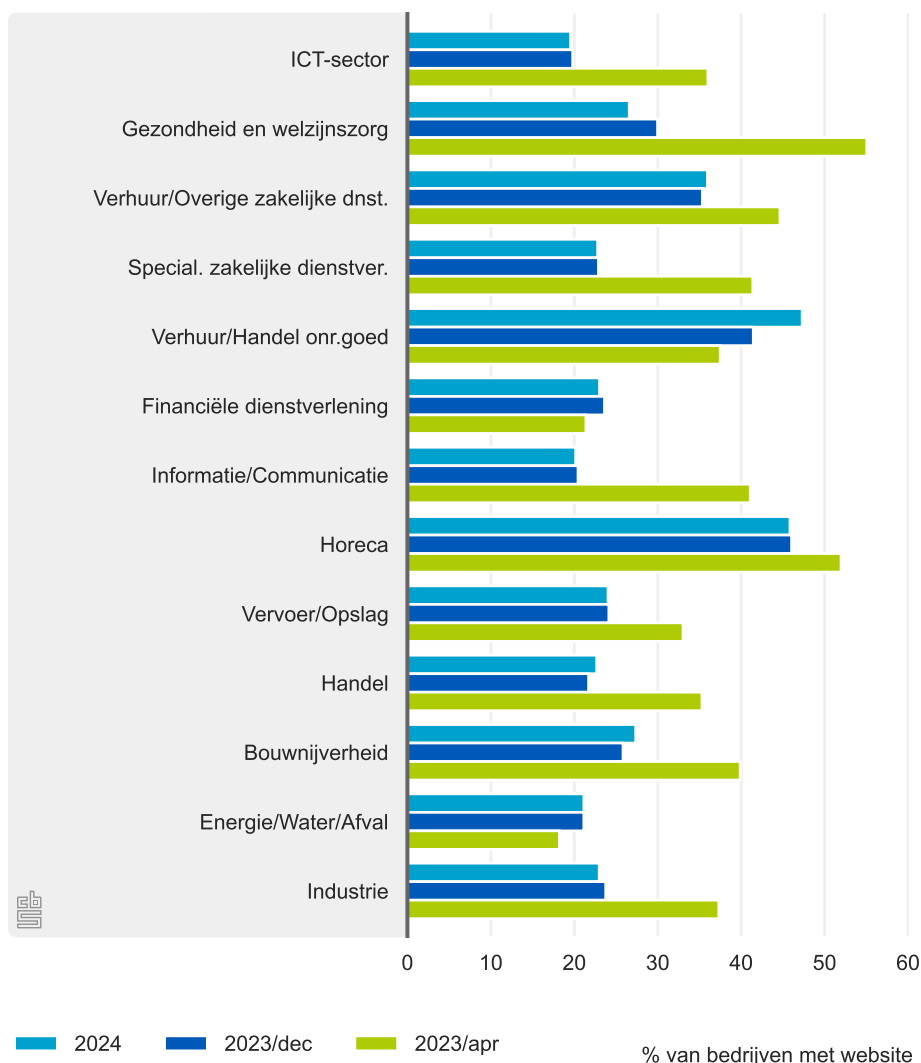


**C.2.4 Percentage van bedrijven met website met geslaagde e-mailtest
'Ontvangende mailserver met geldige DNSSEC handtekening' per
bedrijfsgrootteklasse (a) en bedrijfstak (b).**

(a) Bedrijfsgrootteklasse



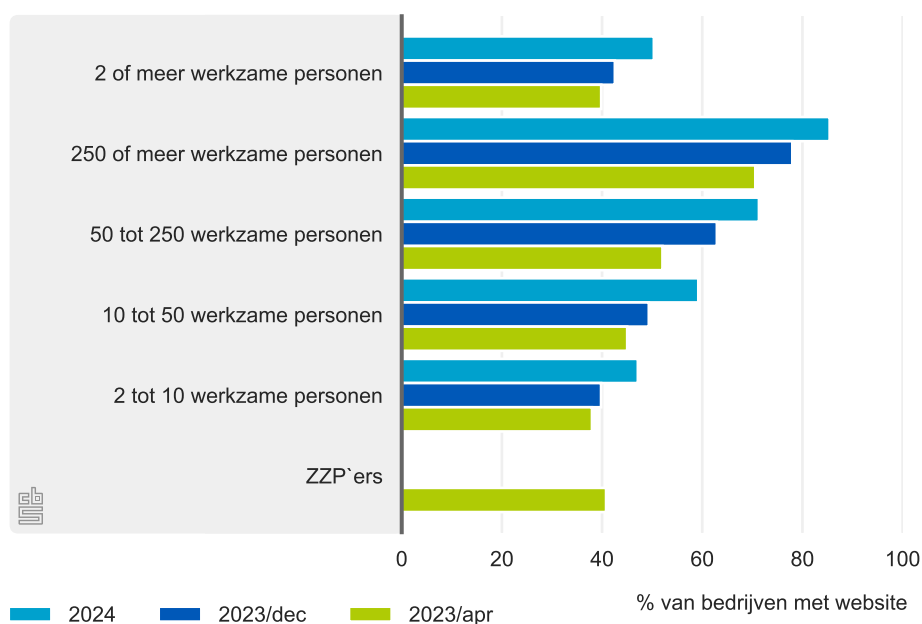
(b) Bedrijfstak



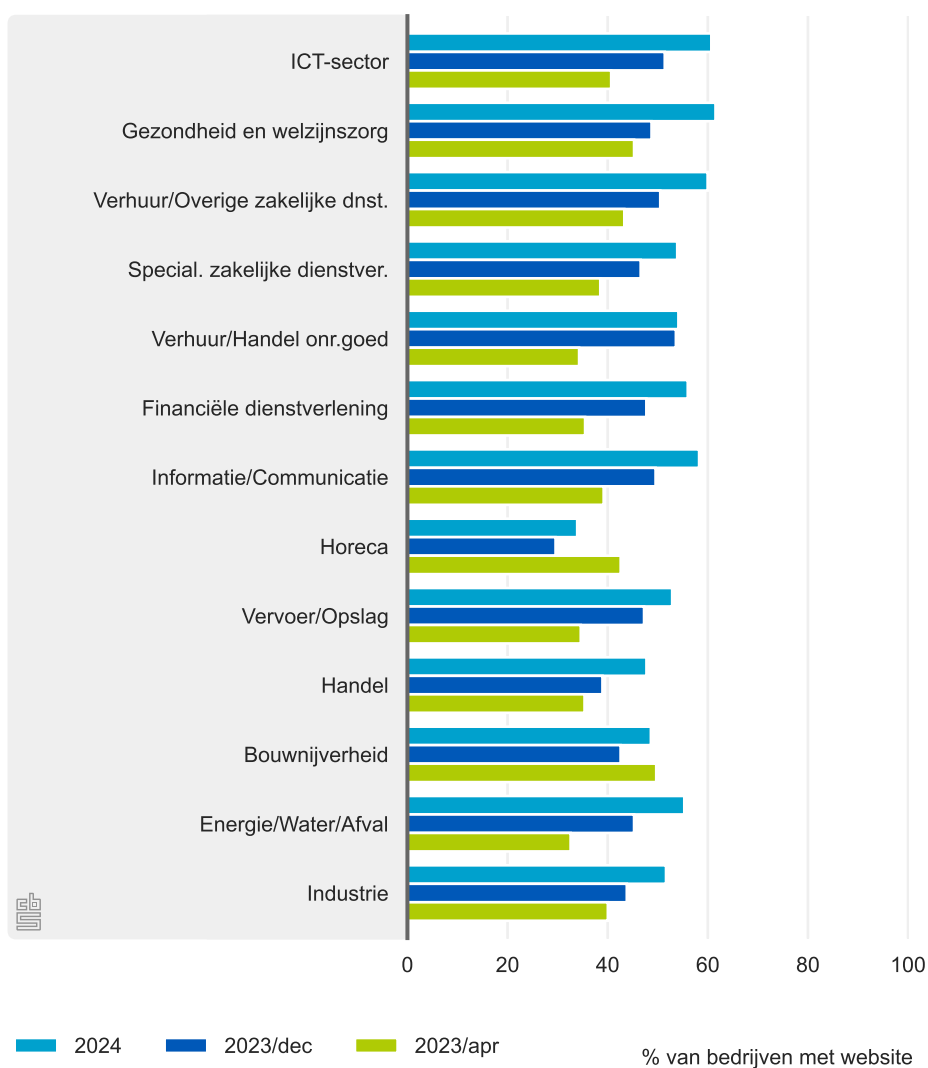
C.3 E-mailtestuitslagen voor categorie `Authenticatie`

C.3.1 Percentage van bedrijven met website met geslaagde e-mailtest `DMARC bestaat' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse

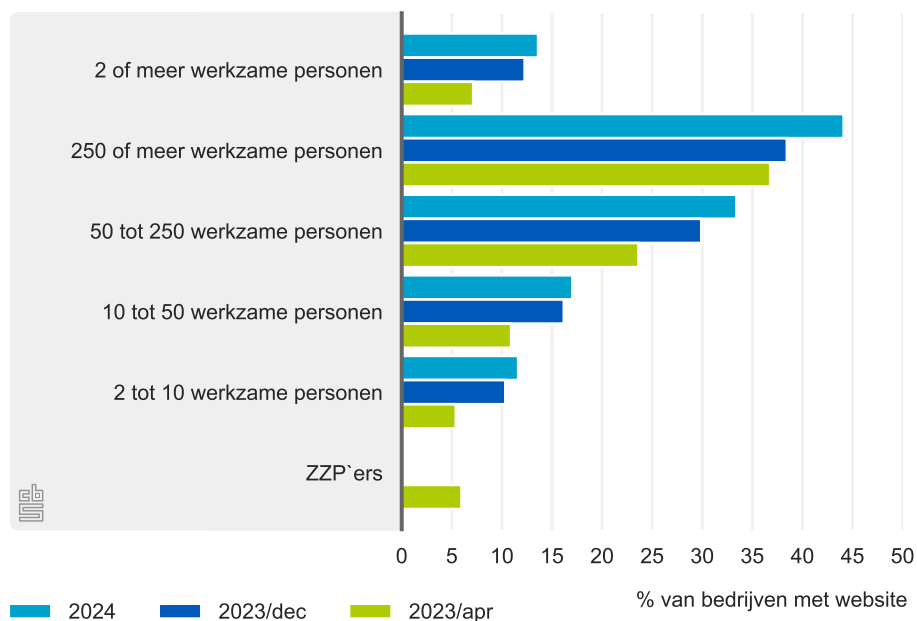


(b) Bedrijfstak

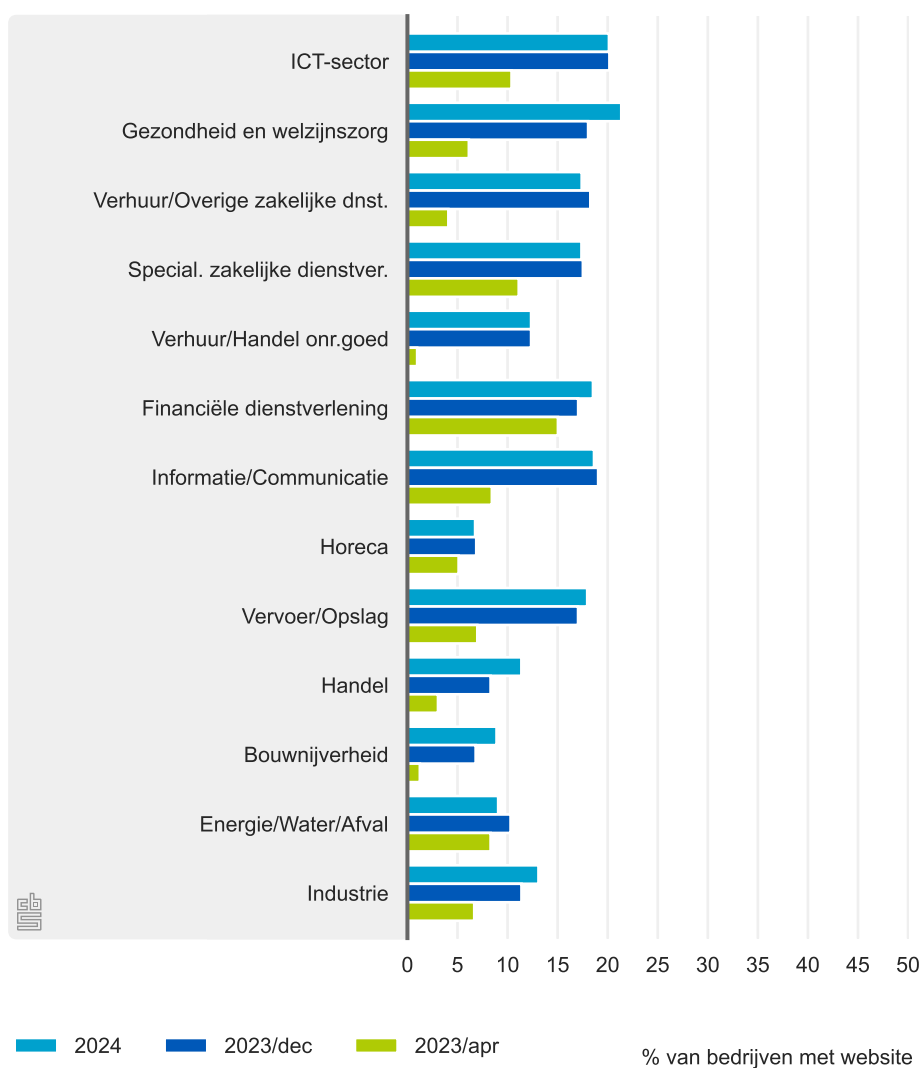


C.3.2 Percentage van bedrijven met website met geslaagde e-mailtest `DMARC heeft voldoende strict beleid' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse

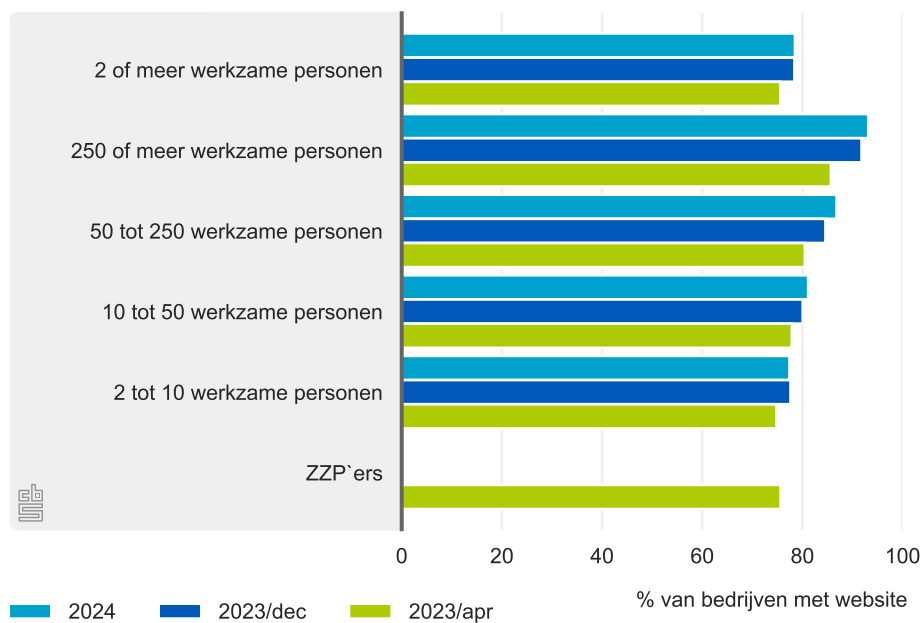


(b) Bedrijfstak

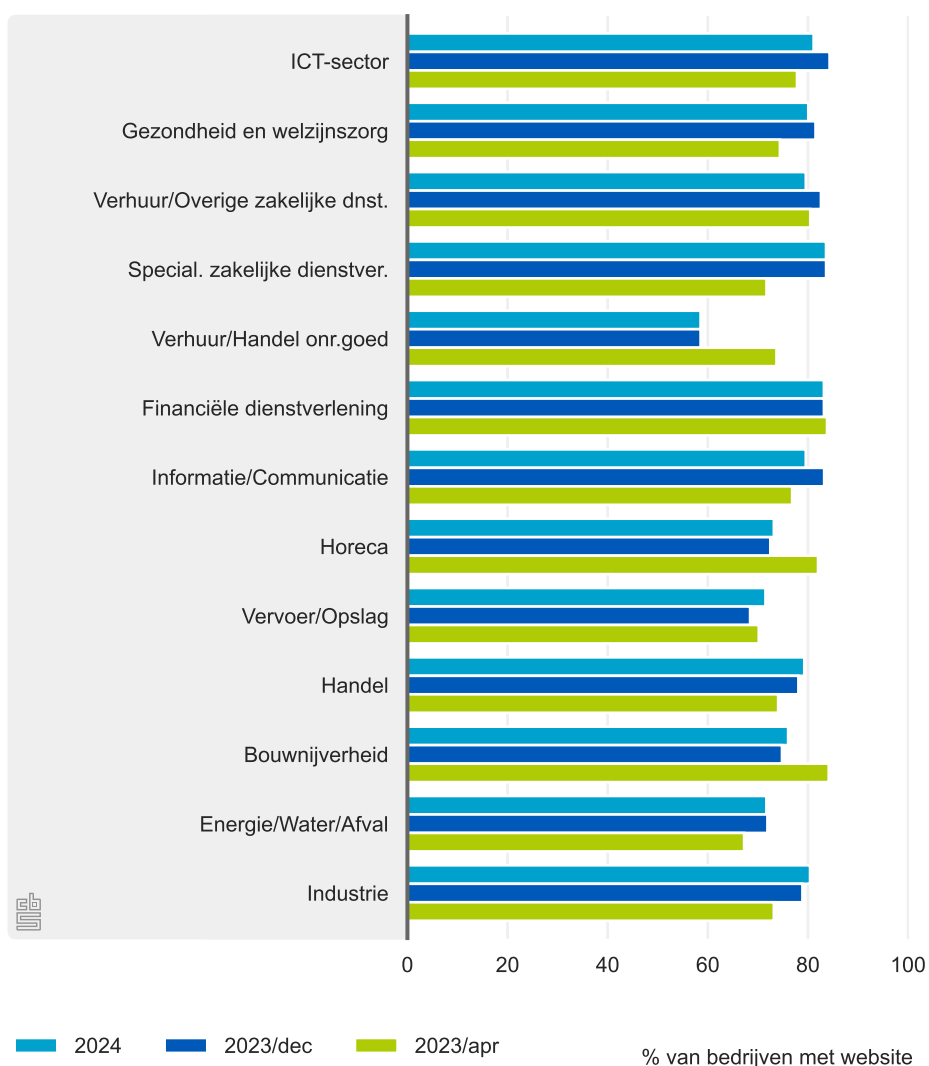


C.3.3 Percentage van bedrijven met website met geslaagde e-mailtest `DKIM bestaat' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse

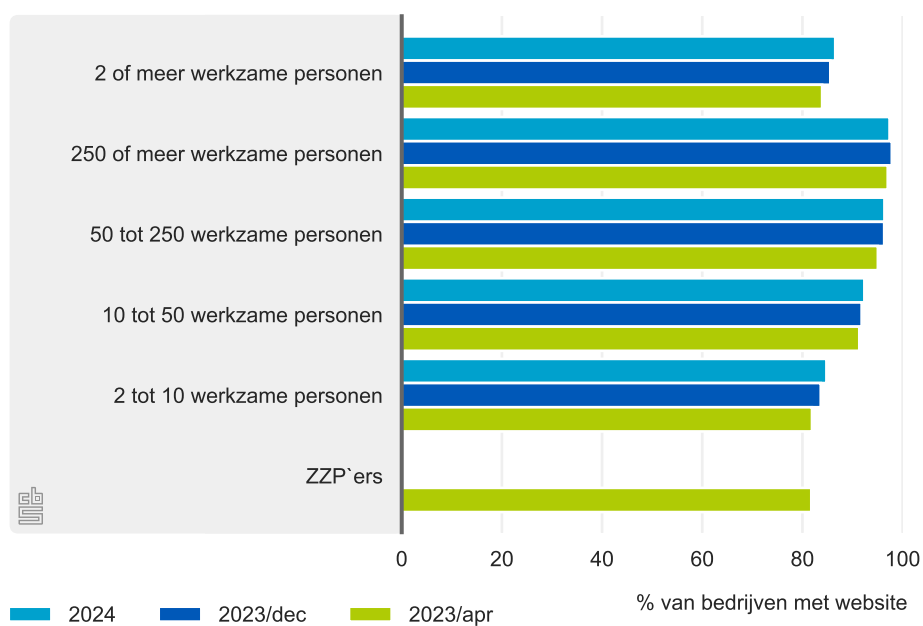


(b) Bedrijfstak

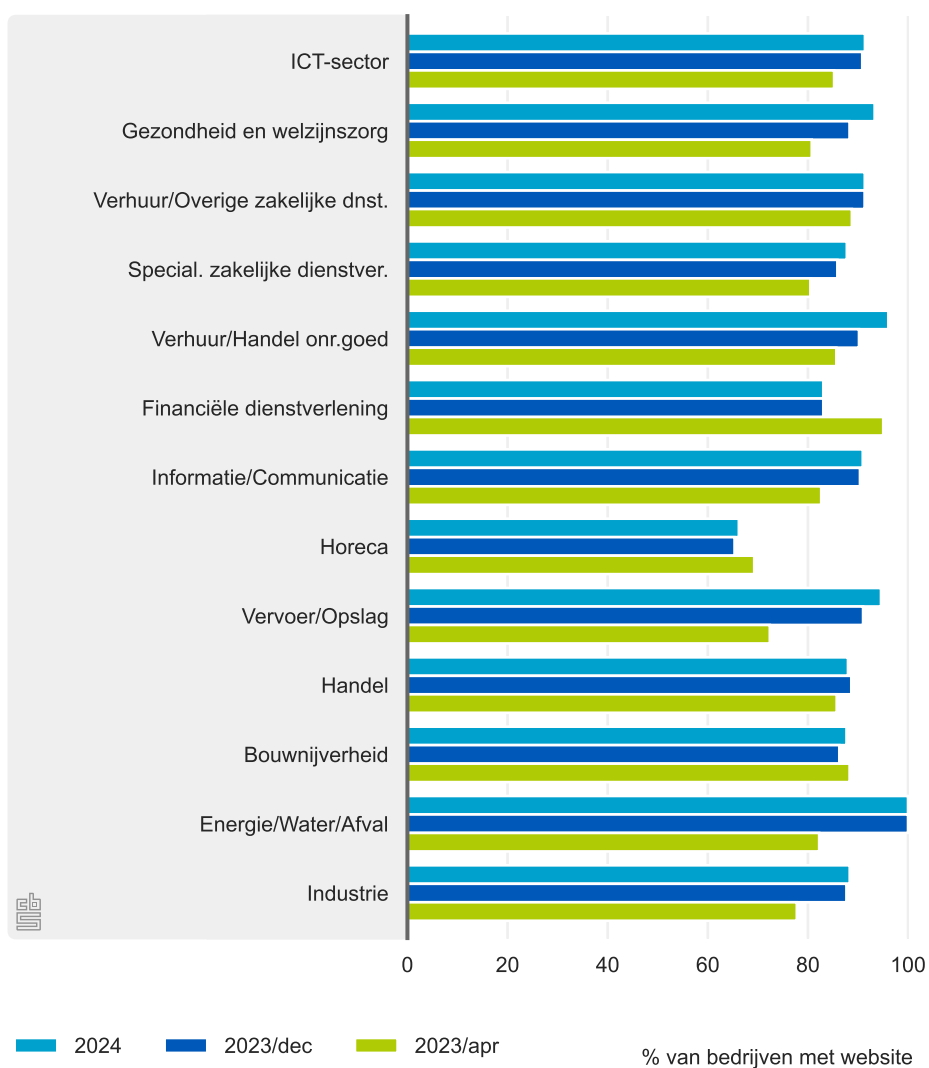


C.3.4 Percentage van bedrijven met website met geslaagde e-mailtest 'SPF bestaat' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse

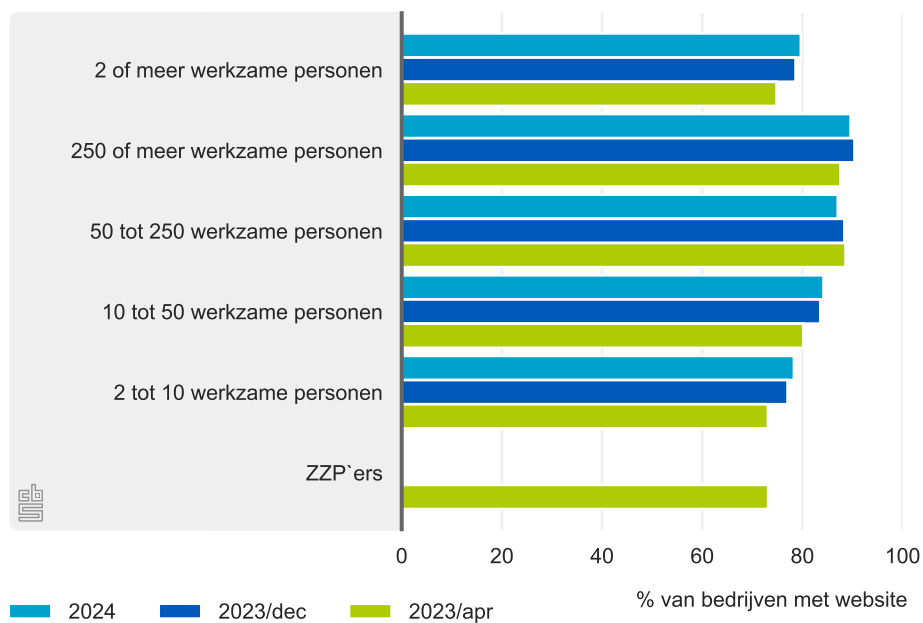


(b) Bedrijfstak

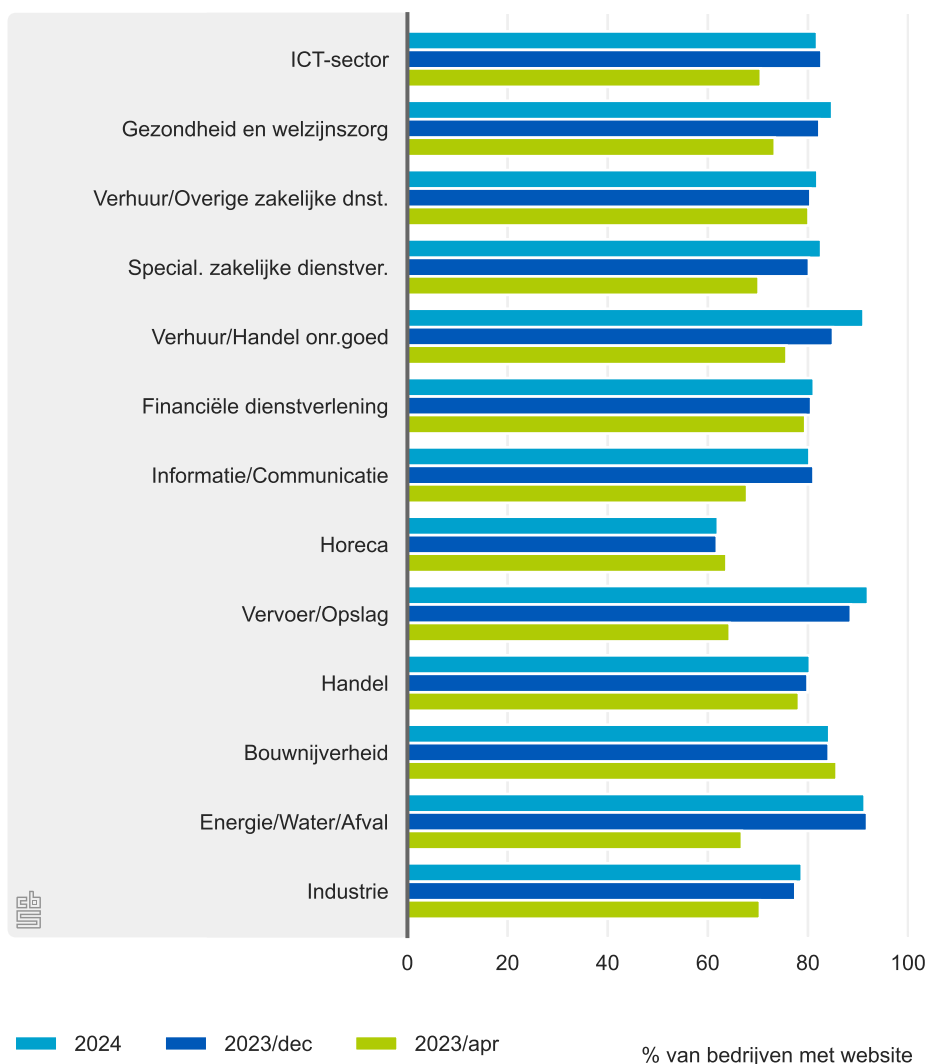


C.3.5 Percentage van bedrijven met website met geslaagde e-mailtest 'SPF beleid' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse



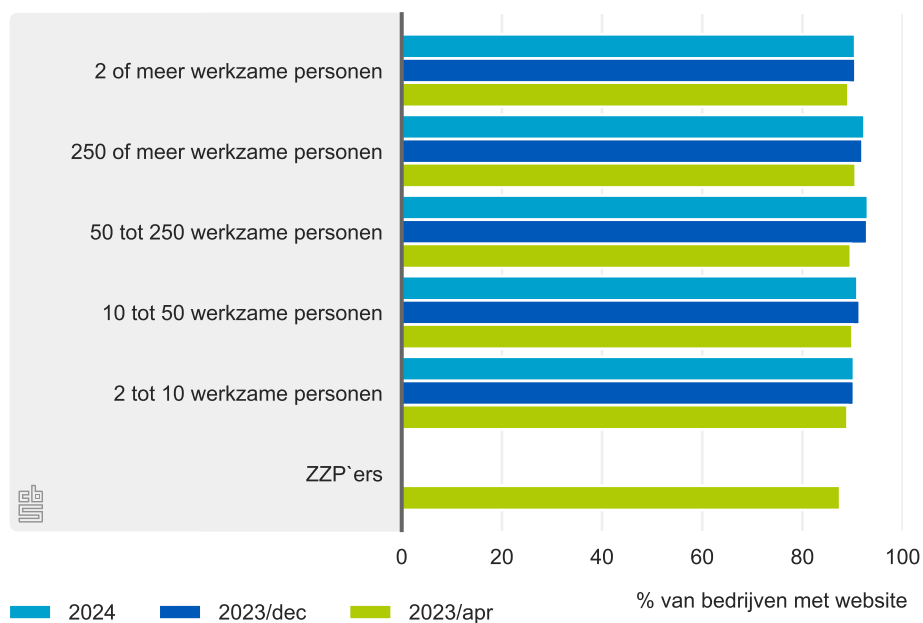
(b) Bedrijfstak



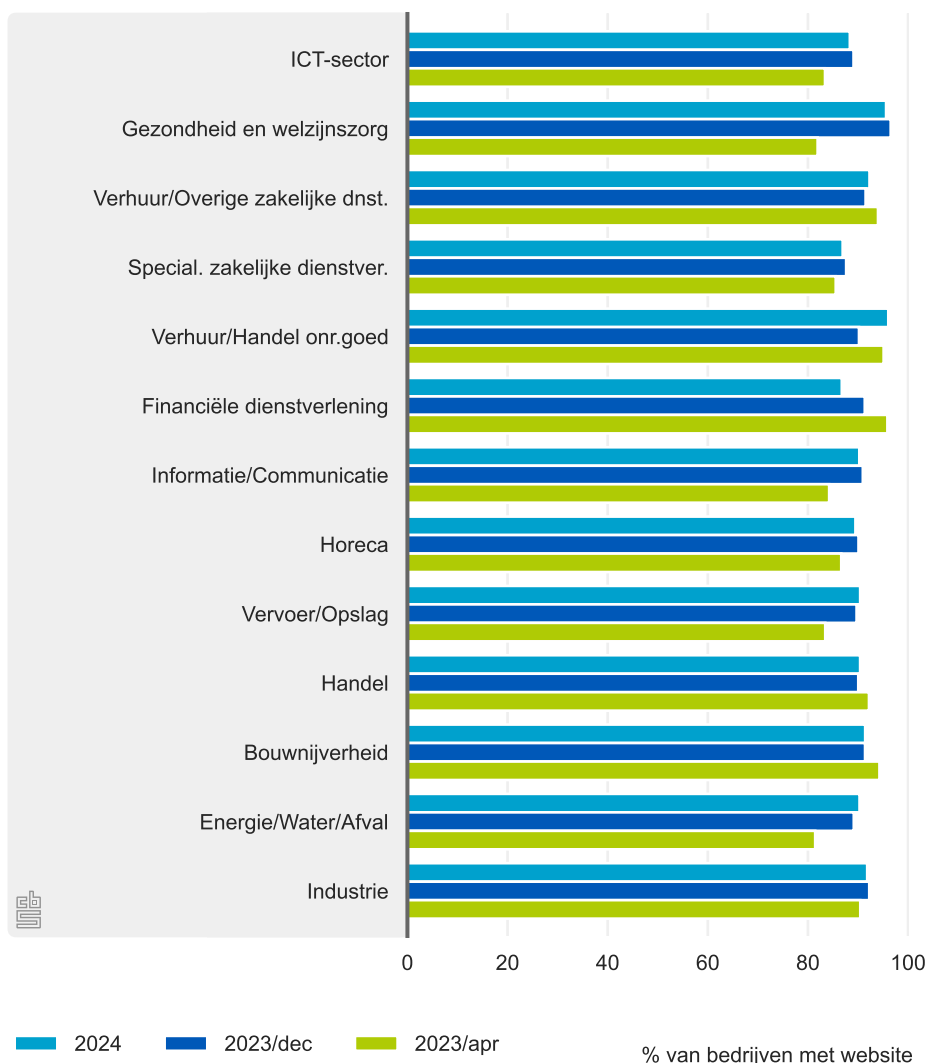
C.4 E-mailtestuitslagen voor categorie 'StartTLS'

C.4.1 Percentage van bedrijven met website met geslaagde e-mailtest 'STARTTLS beschikbaar voor ontvangende mailserver' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse

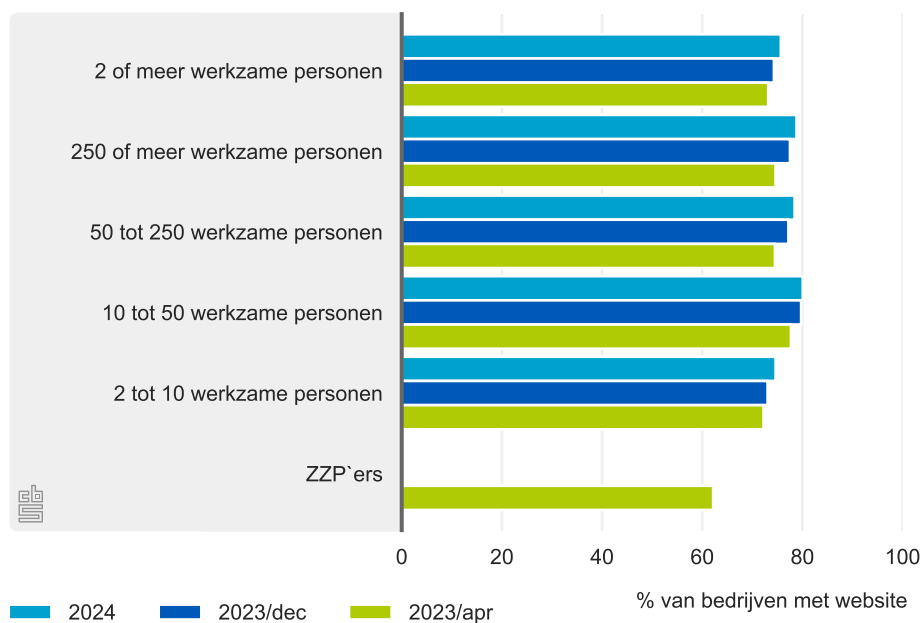


(b) Bedrijfstak

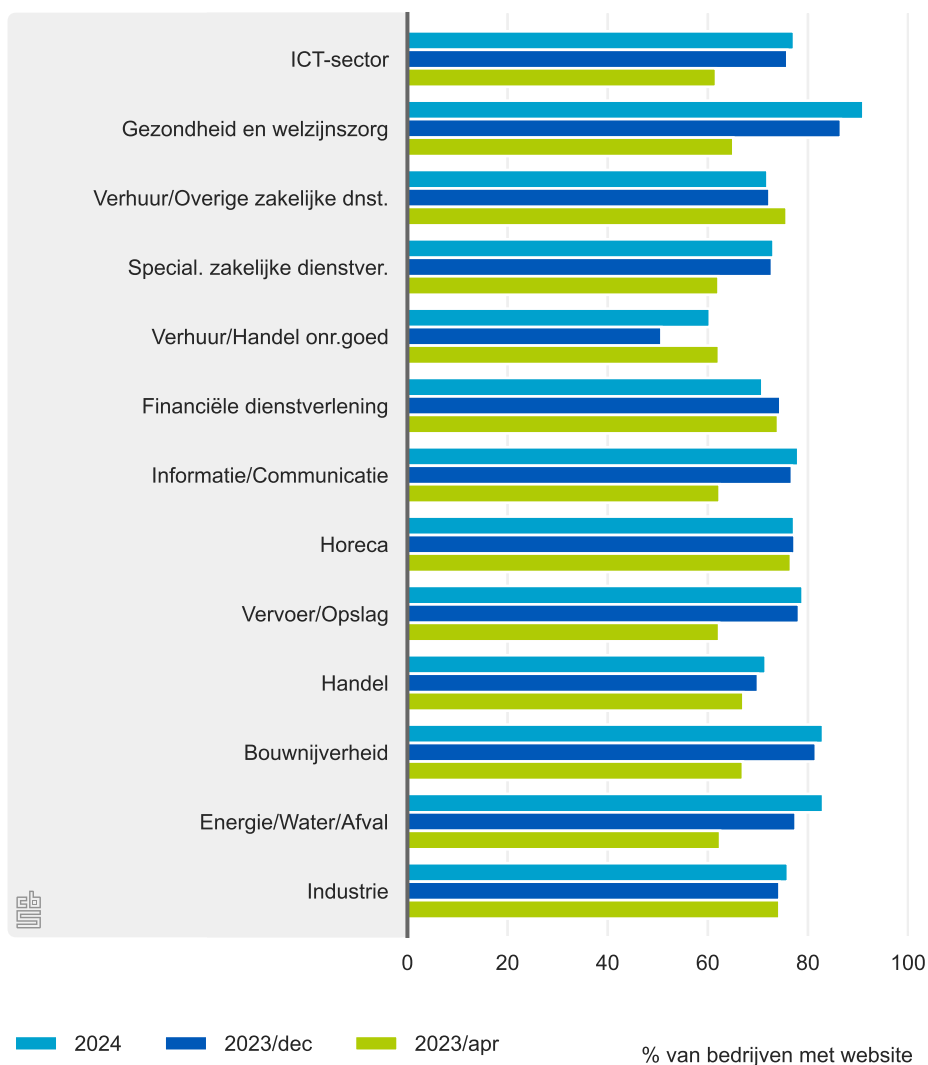


C.4.2 Percentage van bedrijven met website met geslaagde e-mailtest 'STARTTLS sleuteluitwisselingsparameters' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse

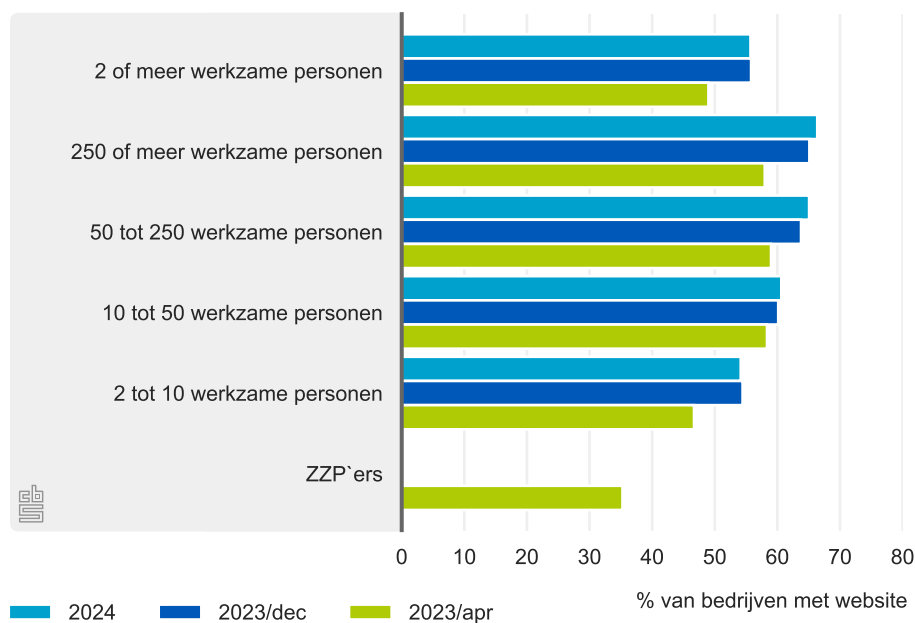


(b) Bedrijfstak

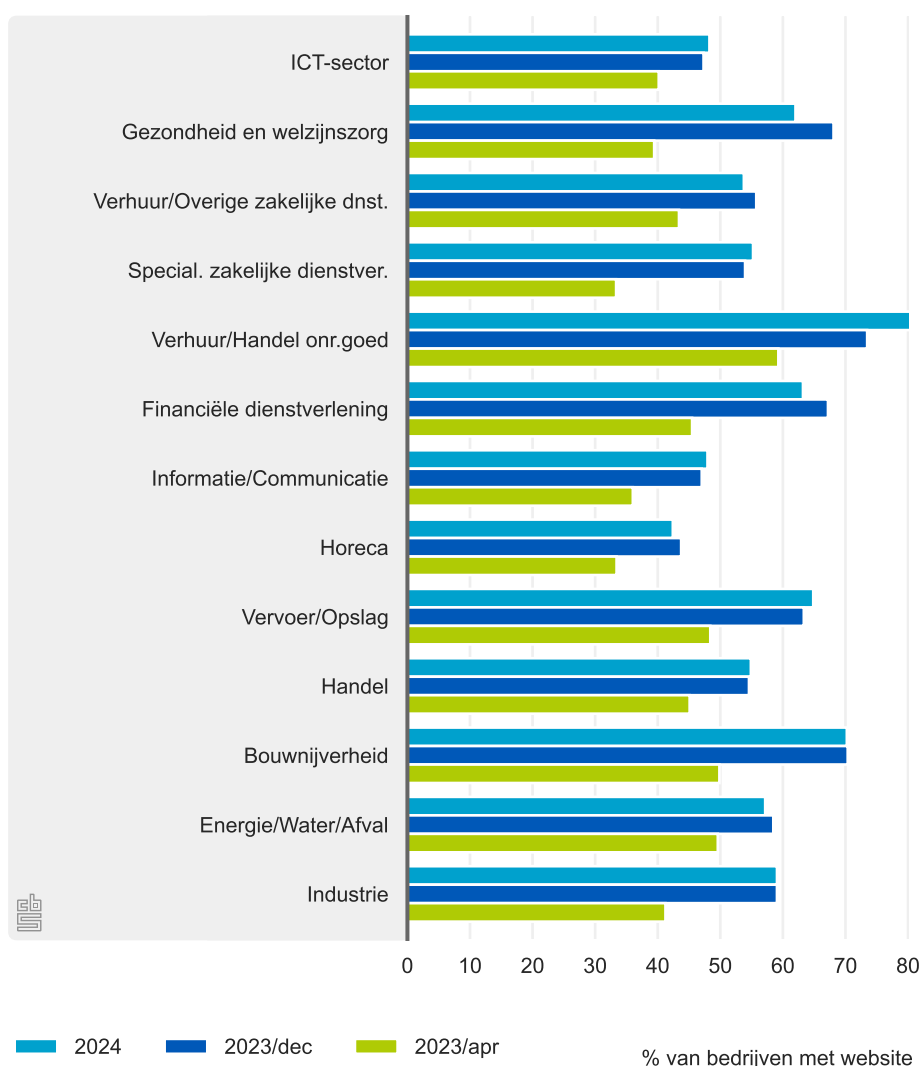


C.4.3 Percentage van bedrijven met website met geslaagde e-mailtest
 `Ontvangende mailserver ondersteunt alleen veilige algoritmeselecties' per
 bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse

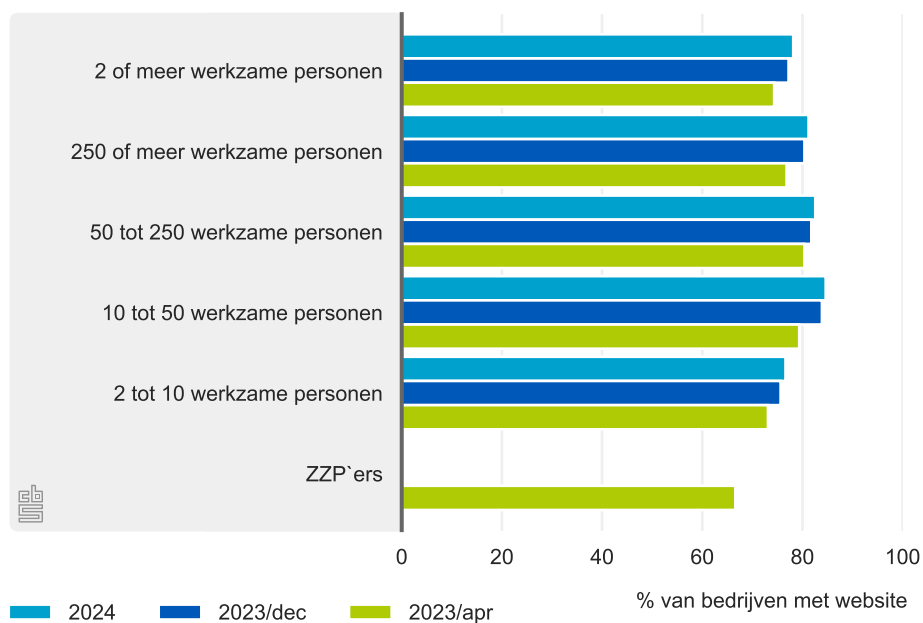


(b) Bedrijfstak

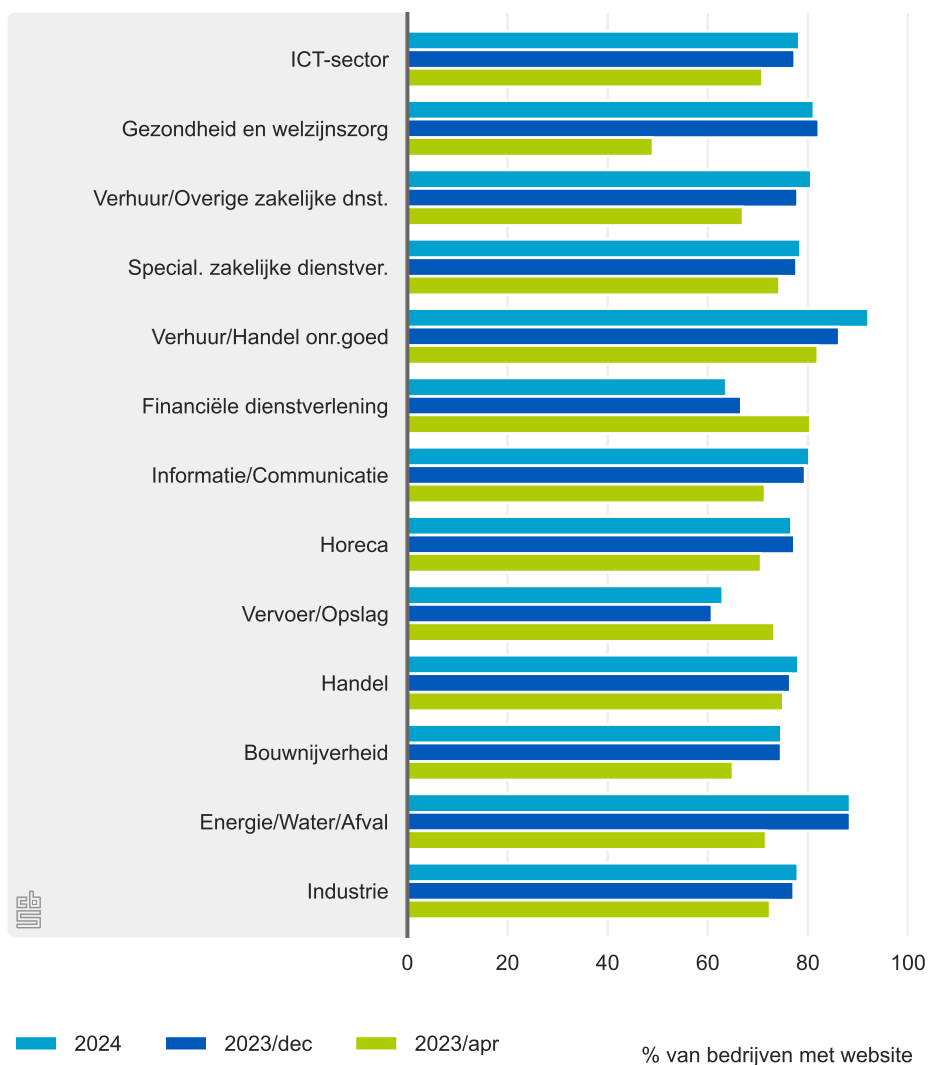


C.4.4 Percentage van bedrijven met website met geslaagde e-mailtest 'Volgorde Algoritmeselectie afgedwongen' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse

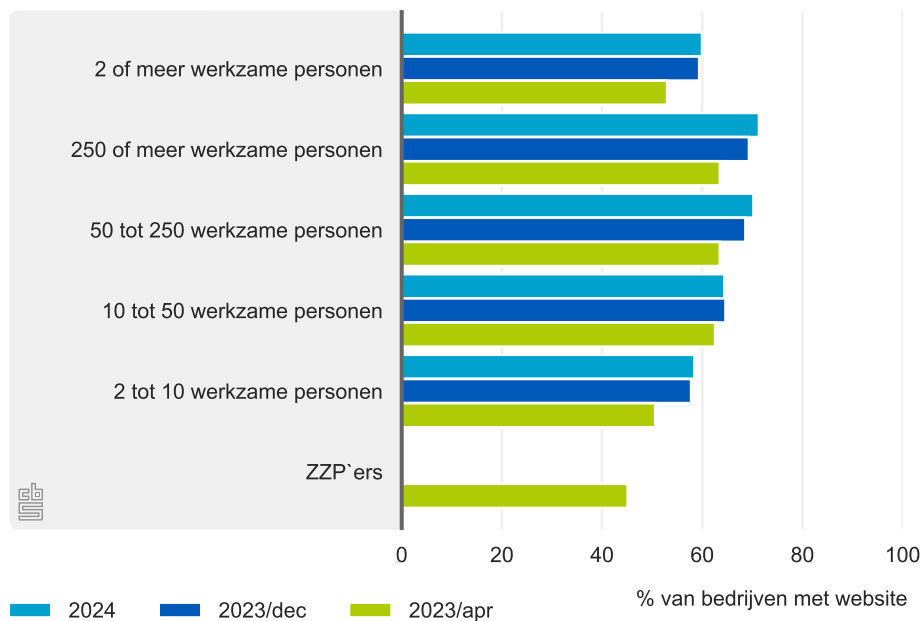


(b) Bedrijfstak

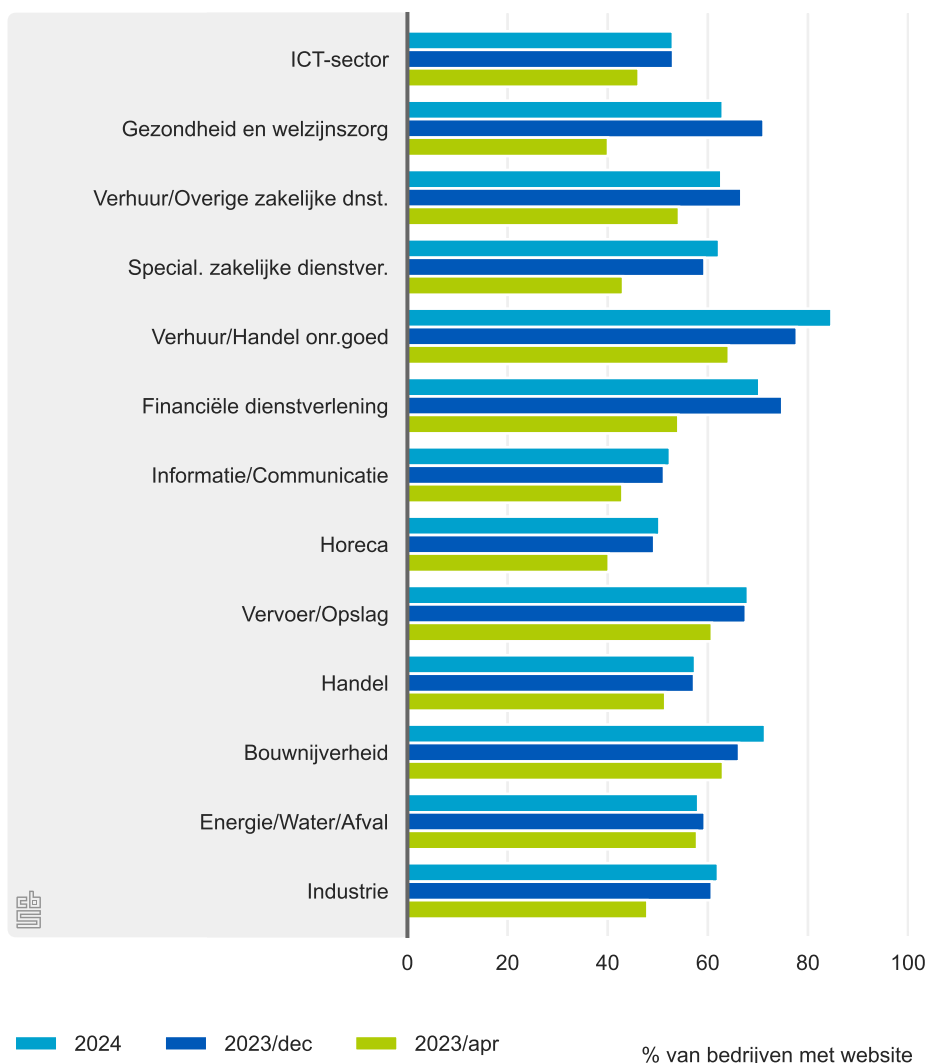


C.4.5 Percentage van bedrijven met website met geslaagde e-mailtest
 'Ontvangende mailserver ondersteunt alleen veilige TLS versies' per
 bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse

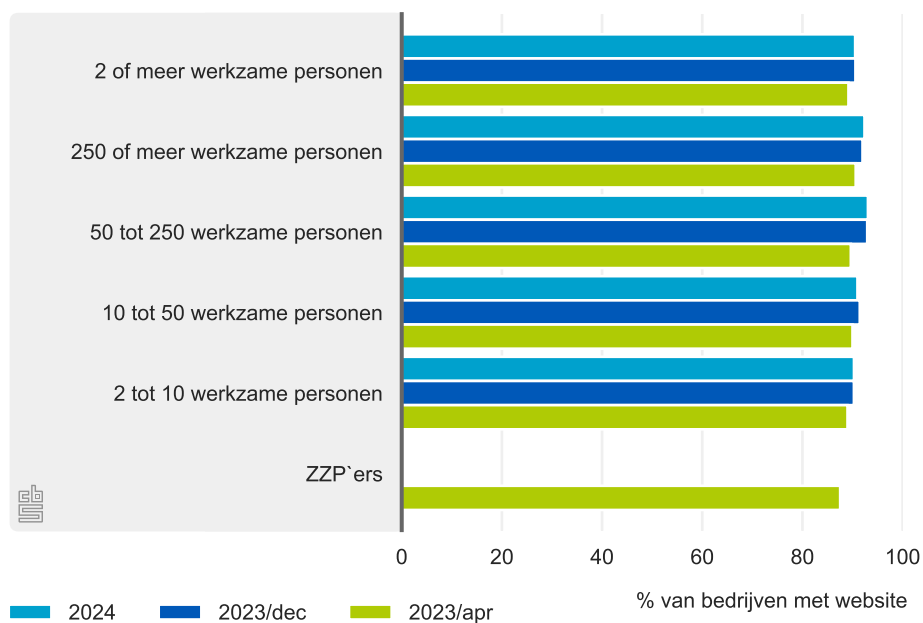


(b) Bedrijfstak

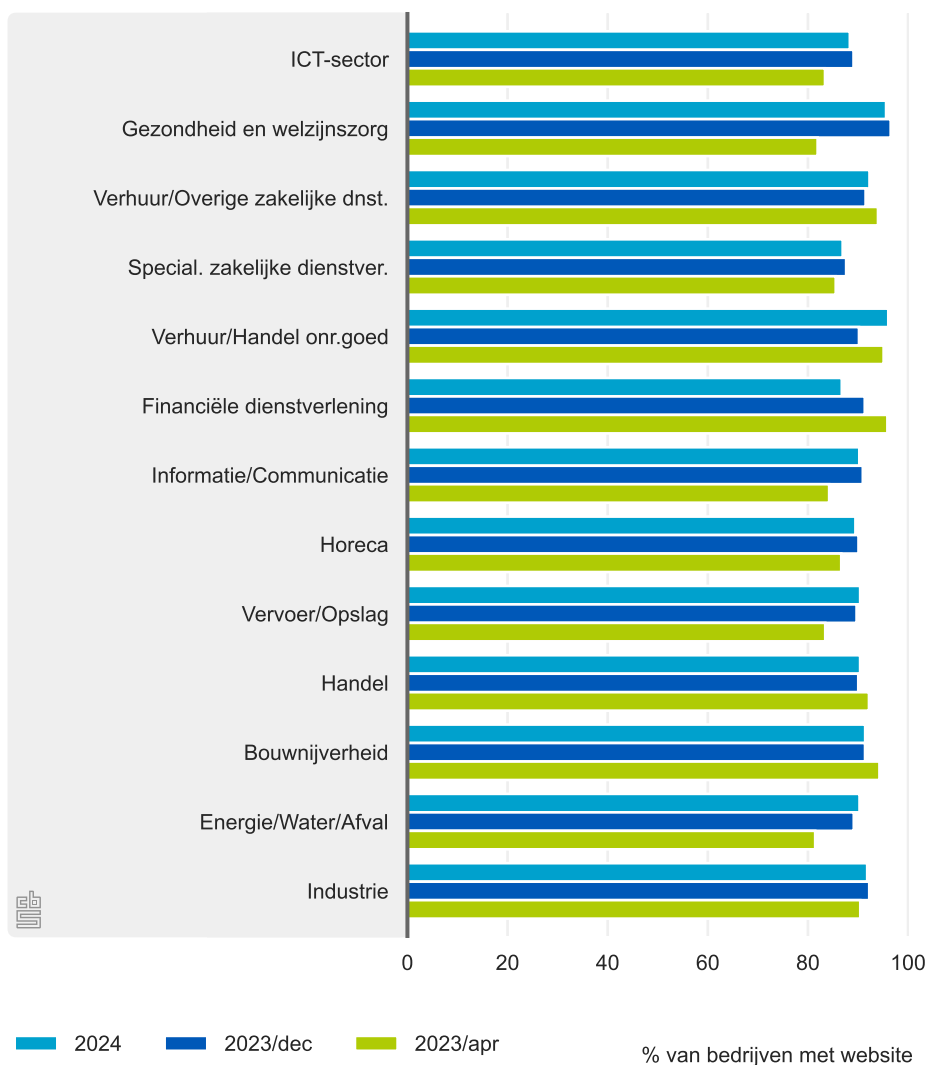


**C.4.6 Percentage van bedrijven met website met geslaagde e-mailtest
'Ontvangende mailserver ondersteunt geen TLS-compressie' per
bedrijfsgrootteklasse (a) en bedrijfstak (b).**

(a) Bedrijfsgrootteklasse

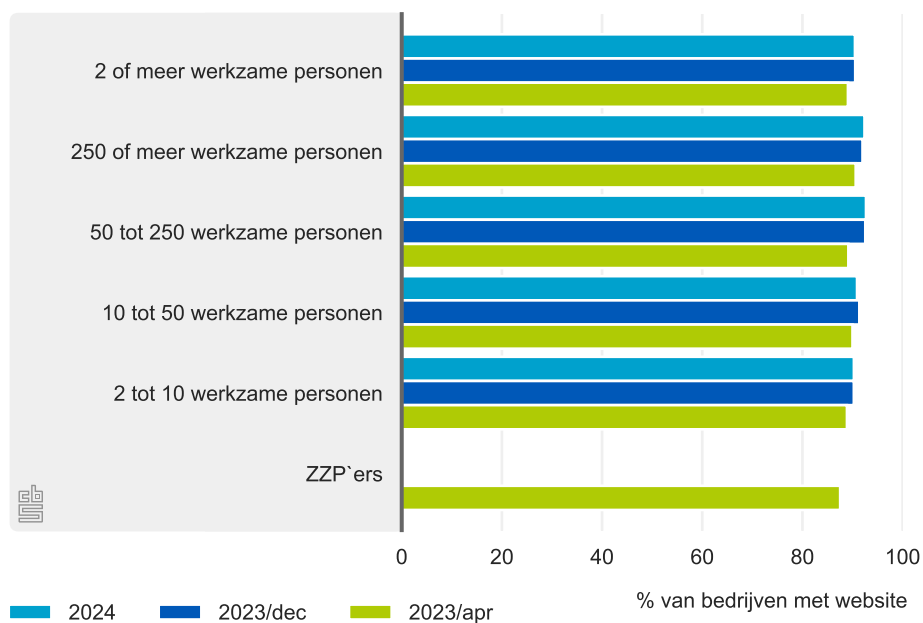


(b) Bedrijfstak

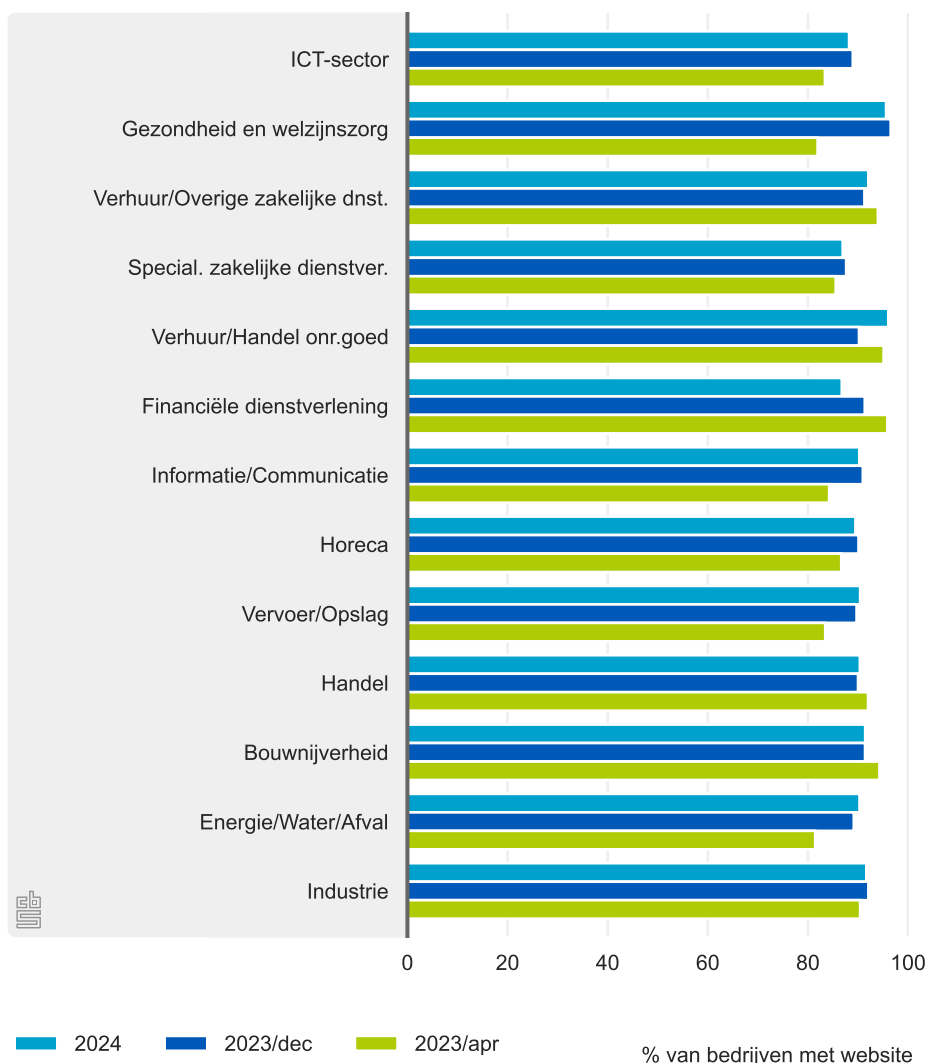


**C.4.7 Percentage van bedrijven met website met geslaagde e-mailtest
'Ontvangende mailserver ondersteunt secure renegotiation' per
bedrijfsgrootteklasse (a) en bedrijfstak (b).**

(a) Bedrijfsgrootteklasse

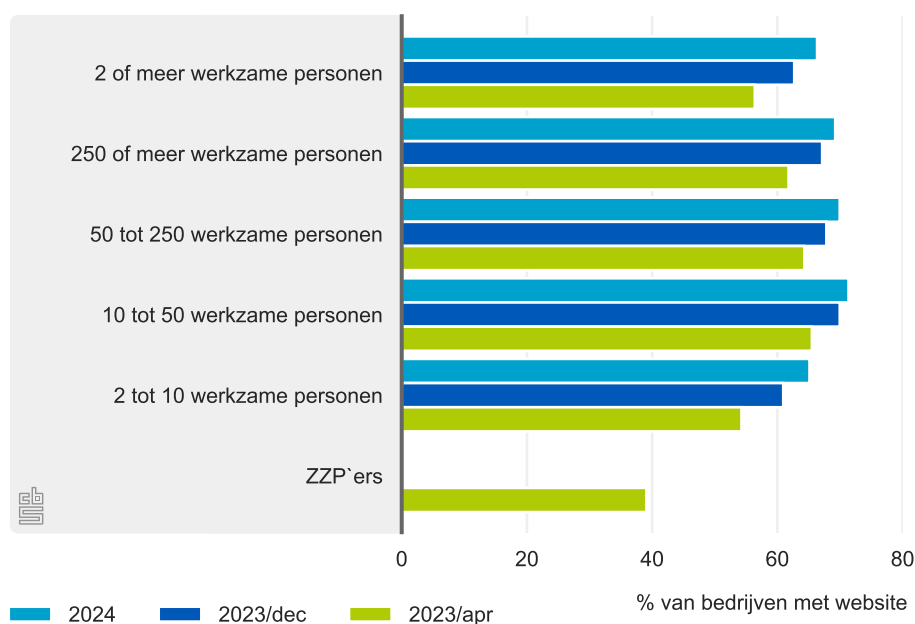


(b) Bedrijfstak

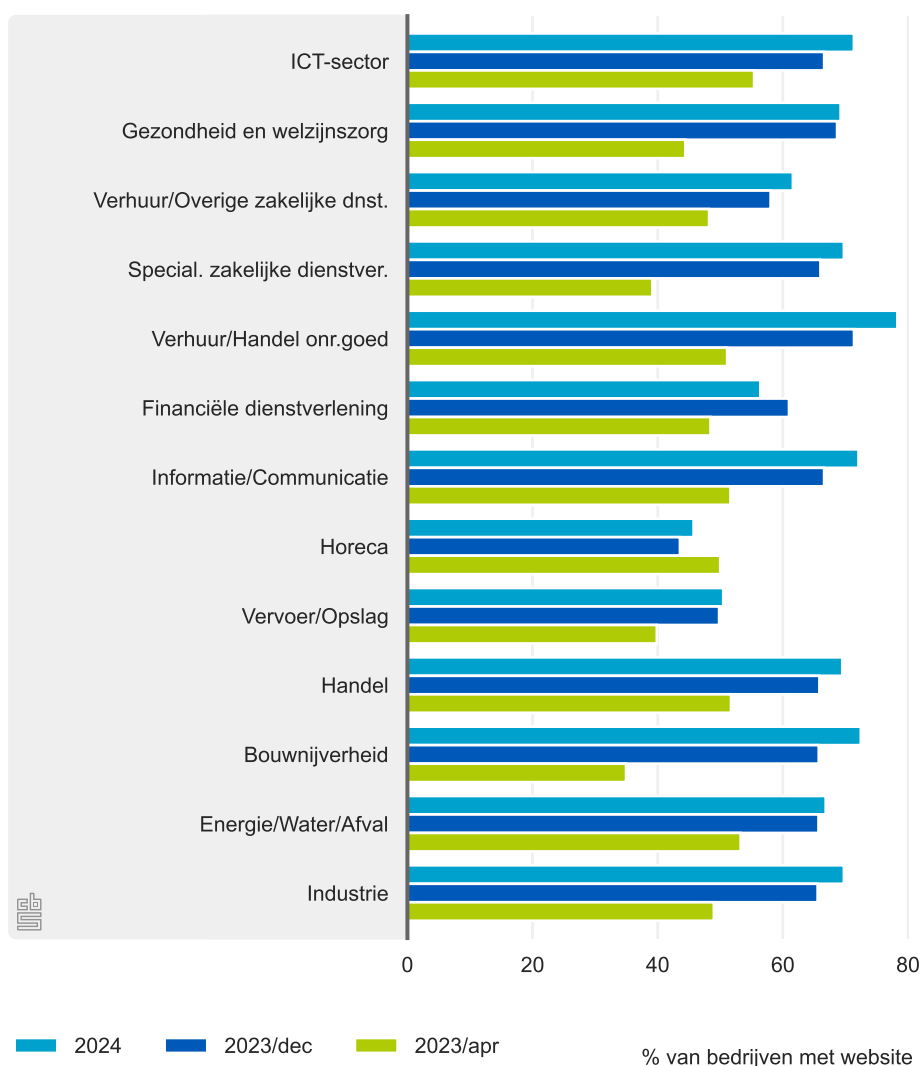


C.4.8 Percentage van bedrijven met website met geslaagde e-mailtest 'TLS client-initiated renegotiation' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse

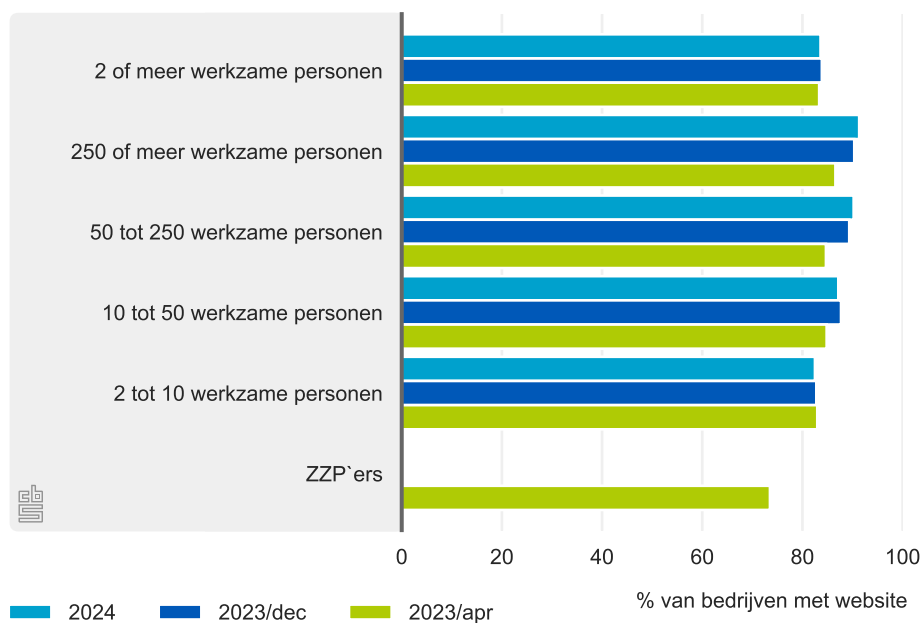


(b) Bedrijfstak

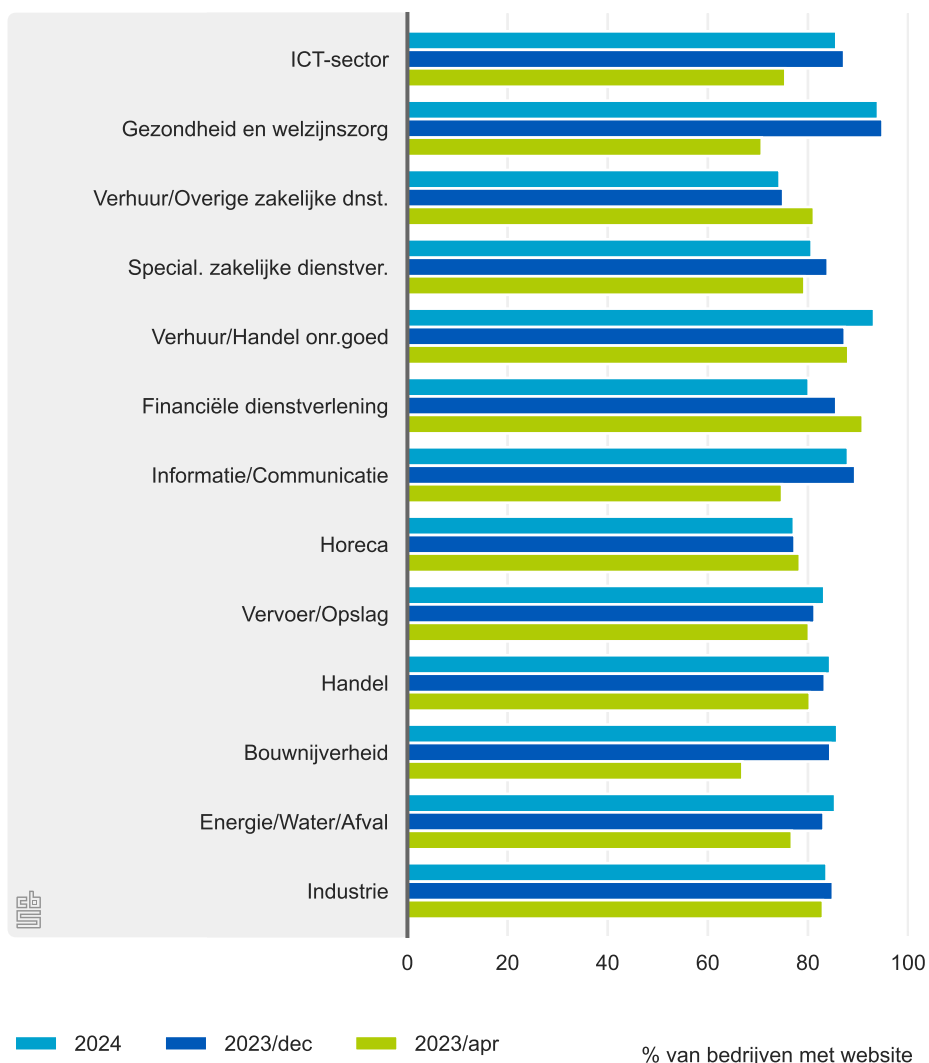


**C.4.9 Percentage van bedrijven met website met geslaagde e-mailtest
`Vertrouwensketen van certificaat' per bedrijfsgrootteklasse (a) en
bedrijfstak (b).**

(a) Bedrijfsgrootteklasse

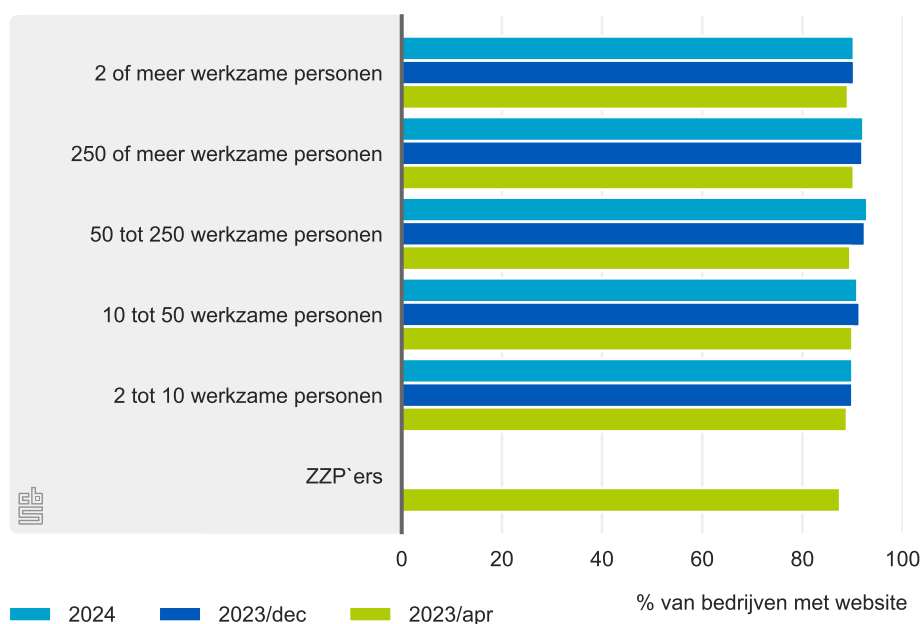


(b) Bedrijfstak

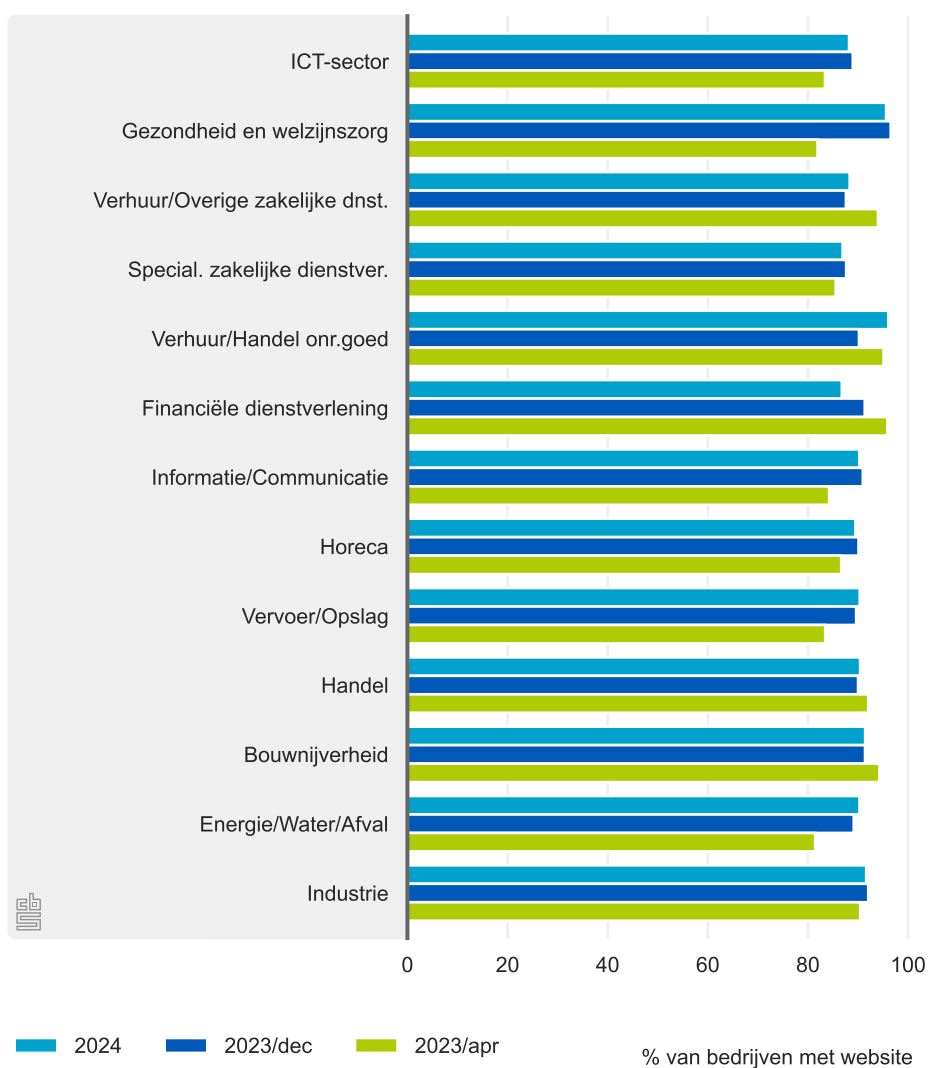


C.4.10 Percentage van bedrijven met website met geslaagde e-mailtest 'Publieke sleutel van certificaat' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse

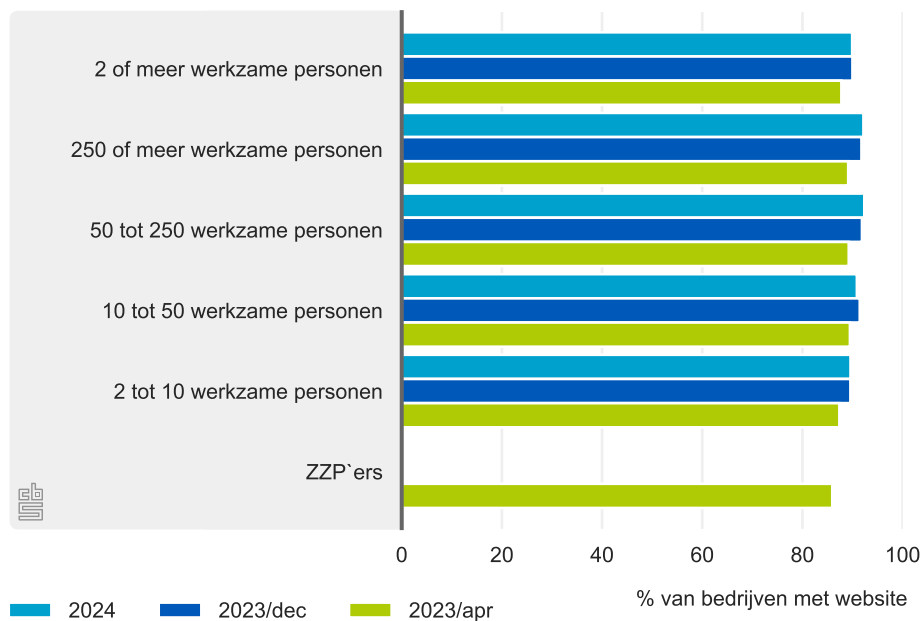


(b) Bedrijfstak

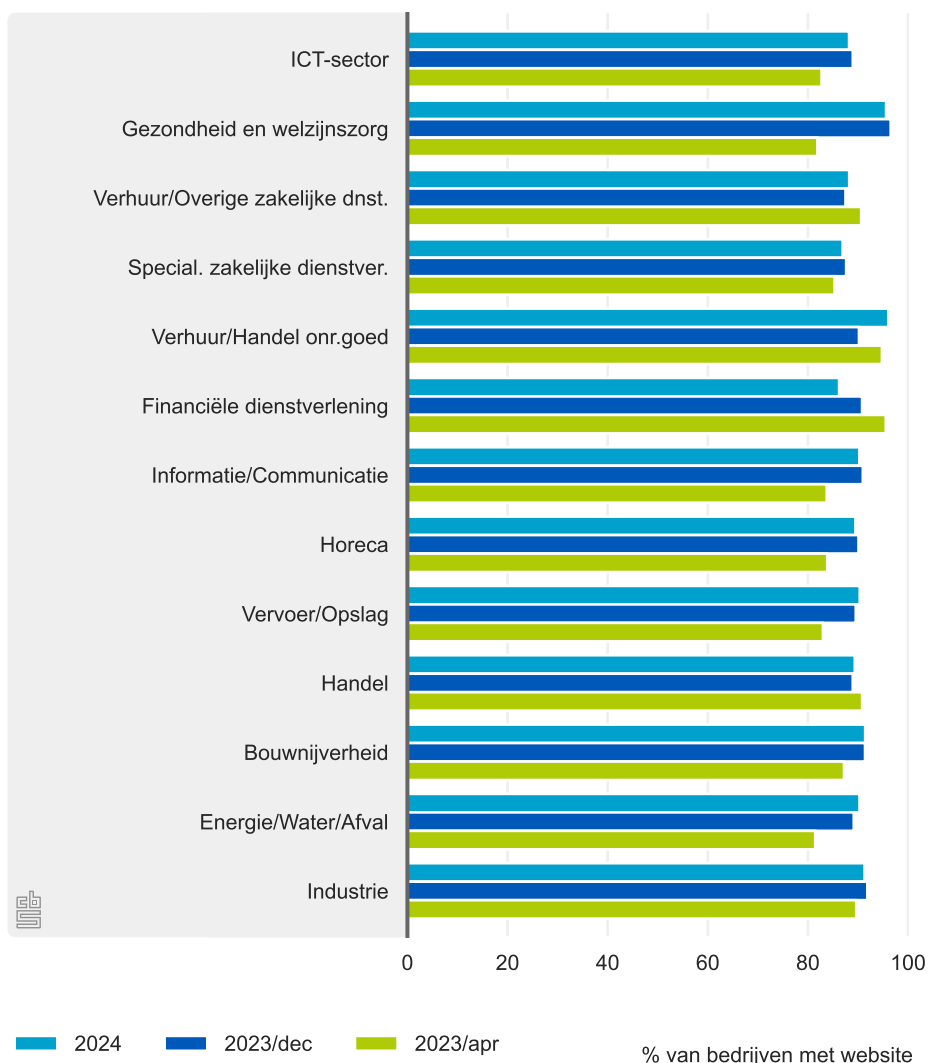


**C.4.11 Percentage van bedrijven met website met geslaagde e-mailtest
'Handtekening van certificaat' per bedrijfsgrootteklasse (a) en bedrijfstak
(b).**

(a) Bedrijfsgrootteklasse

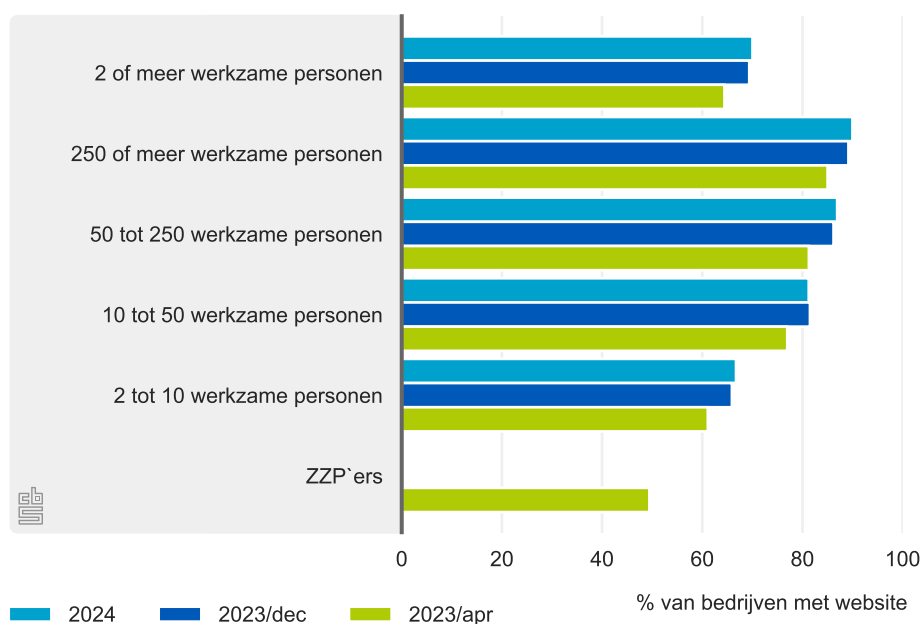


(b) Bedrijfstak

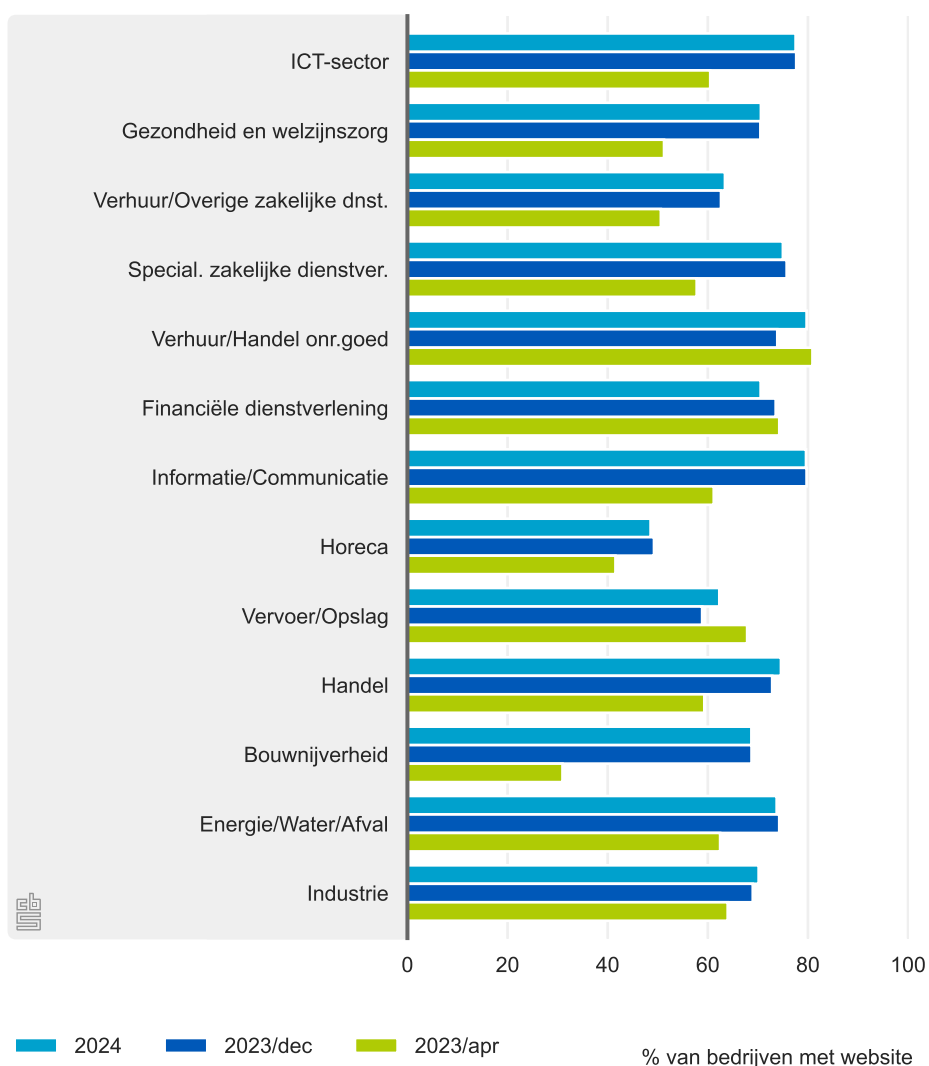


C.4.12 Percentage van bedrijven met website met geslaagde e-mailtest 'Domein op certificaat' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse

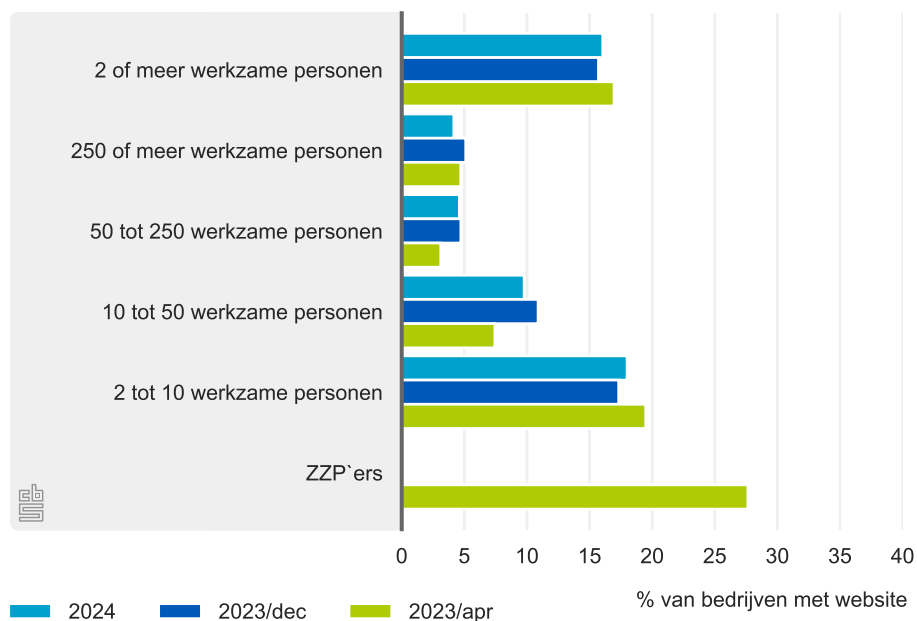


(b) Bedrijfstak

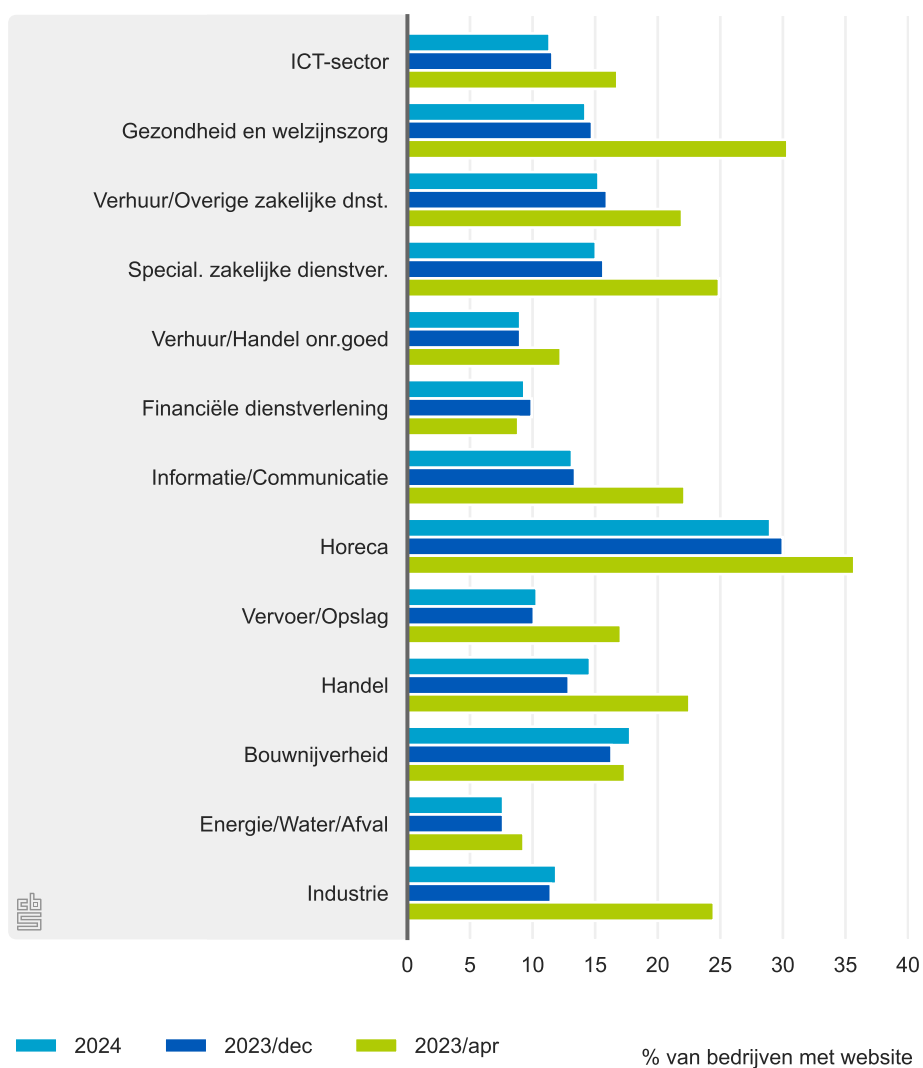


**C.4.13 Categorie StartTLS: percentage van bedrijven met geslaagde e-mailtest
`DANE bestaat' per bedrijfsgrootteklasse (a) en bedrijfstak (b).**

(a) Bedrijfsgrootteklasse

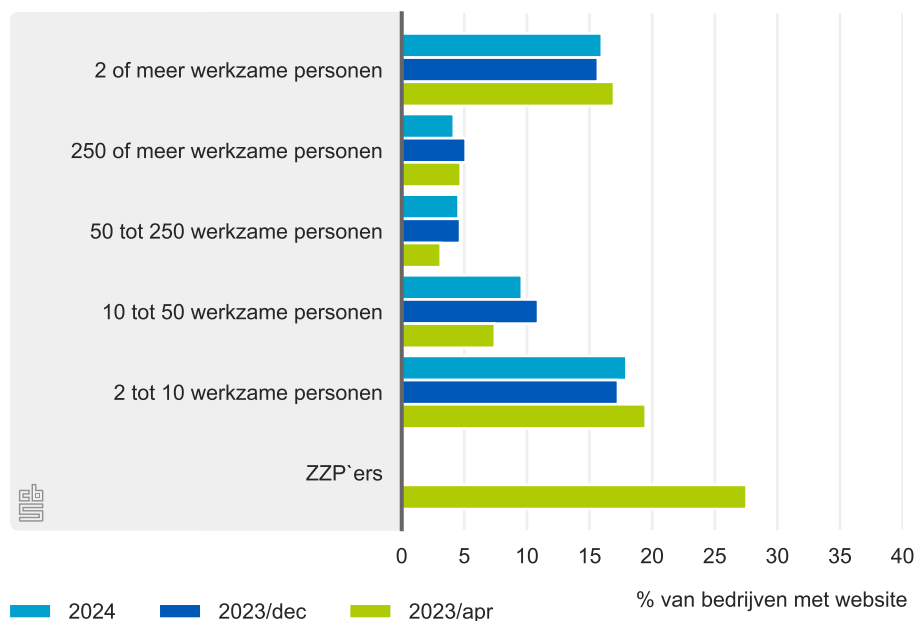


(b) Bedrijfstak

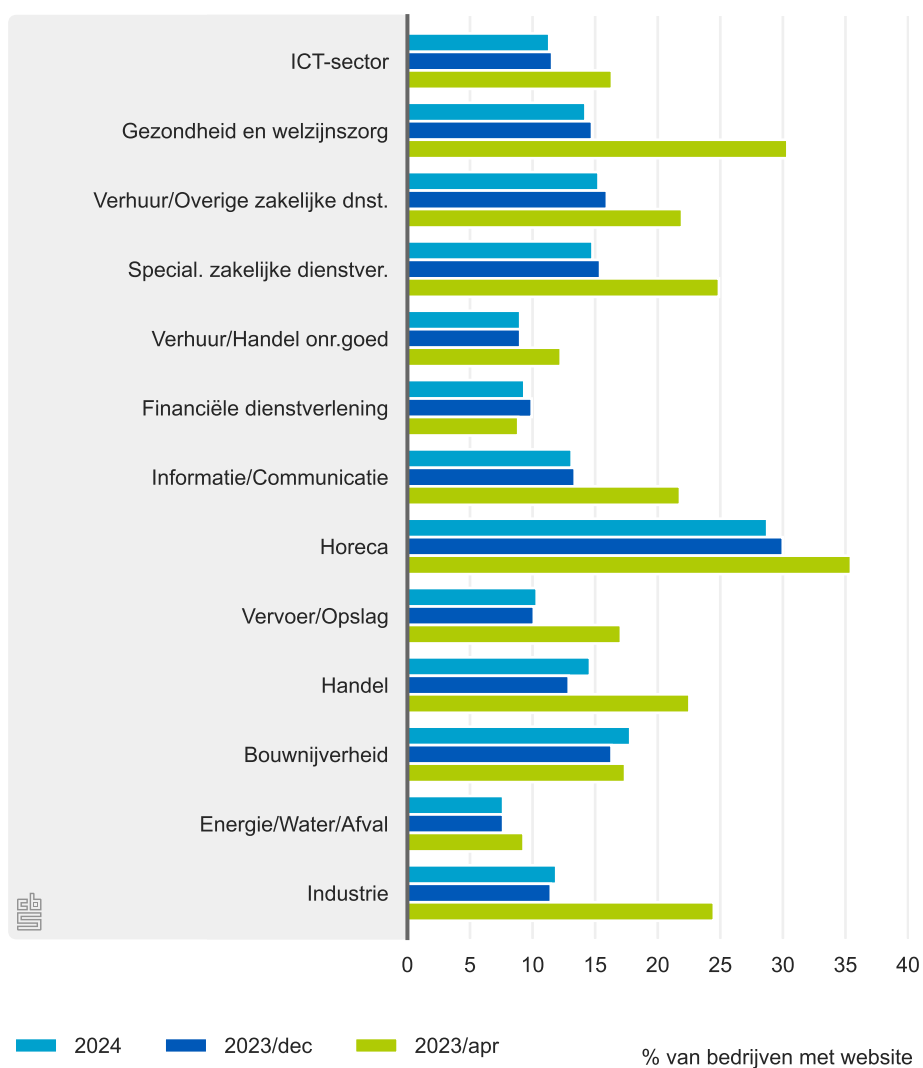


C.4.14 Percentage van bedrijven met website met geslaagde e-mailtest 'DANE geldigheid' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse

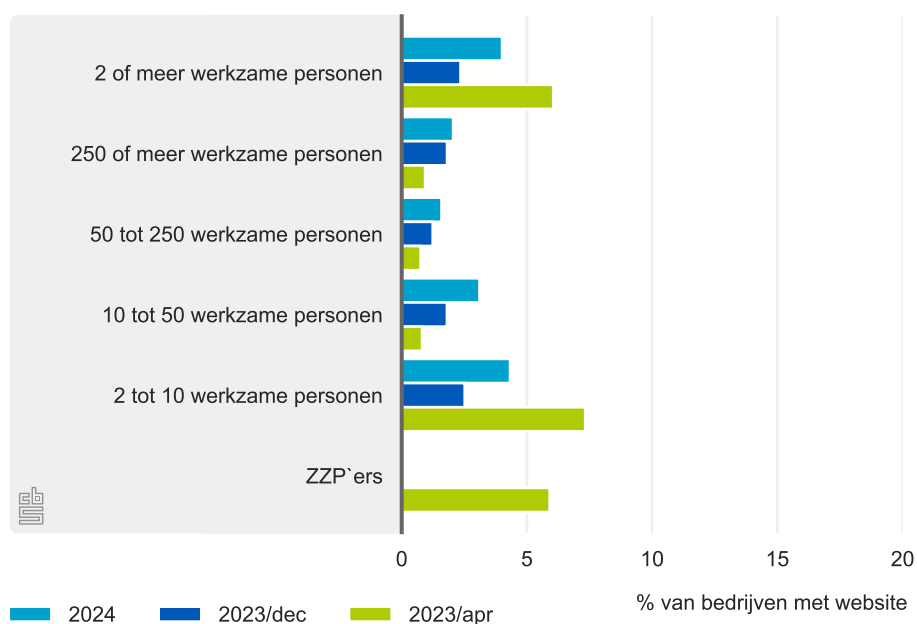


(b) Bedrijfstak

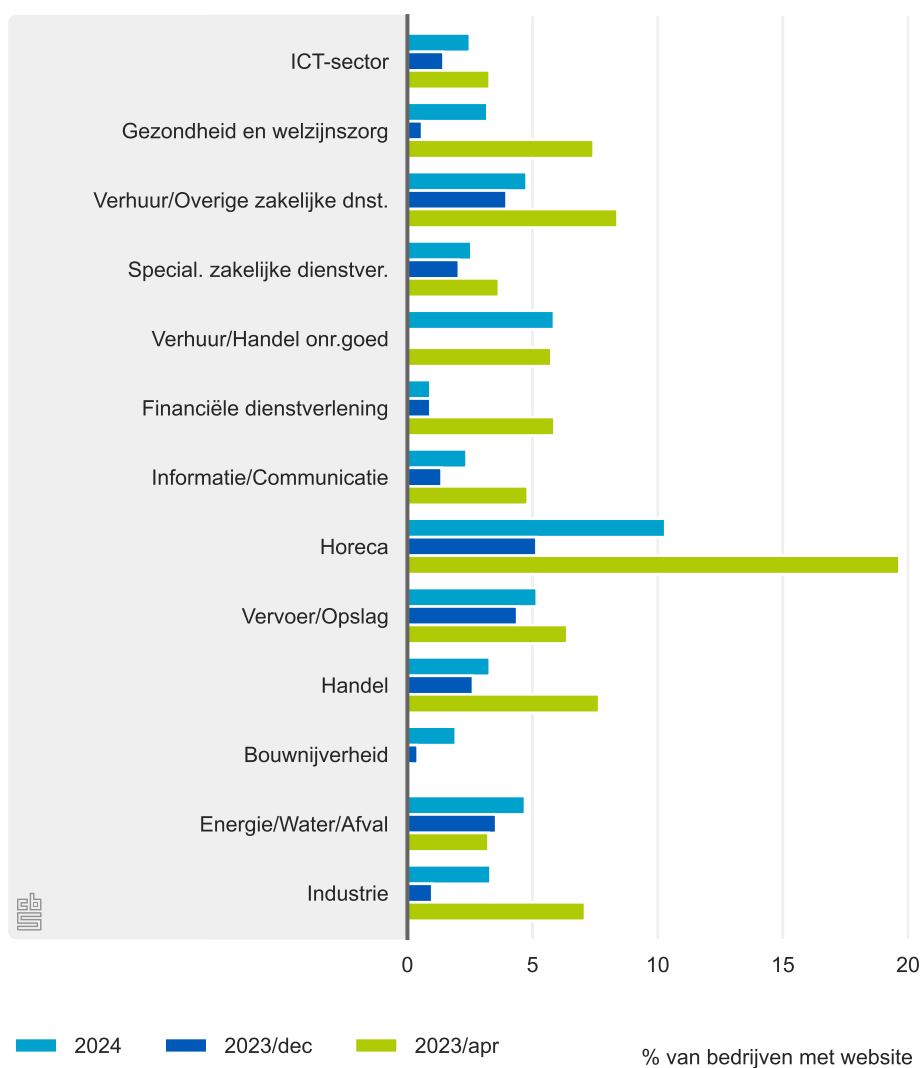


C.4.15 Percentage van bedrijven met website met geslaagde e-mailtest `DANE Rollover-schema' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse

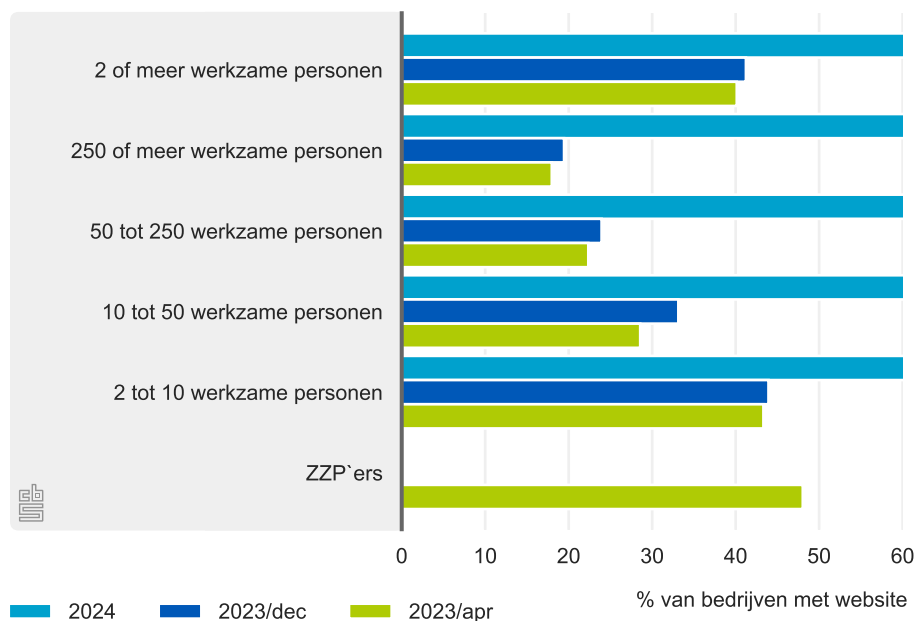


(b) Bedrijfstak

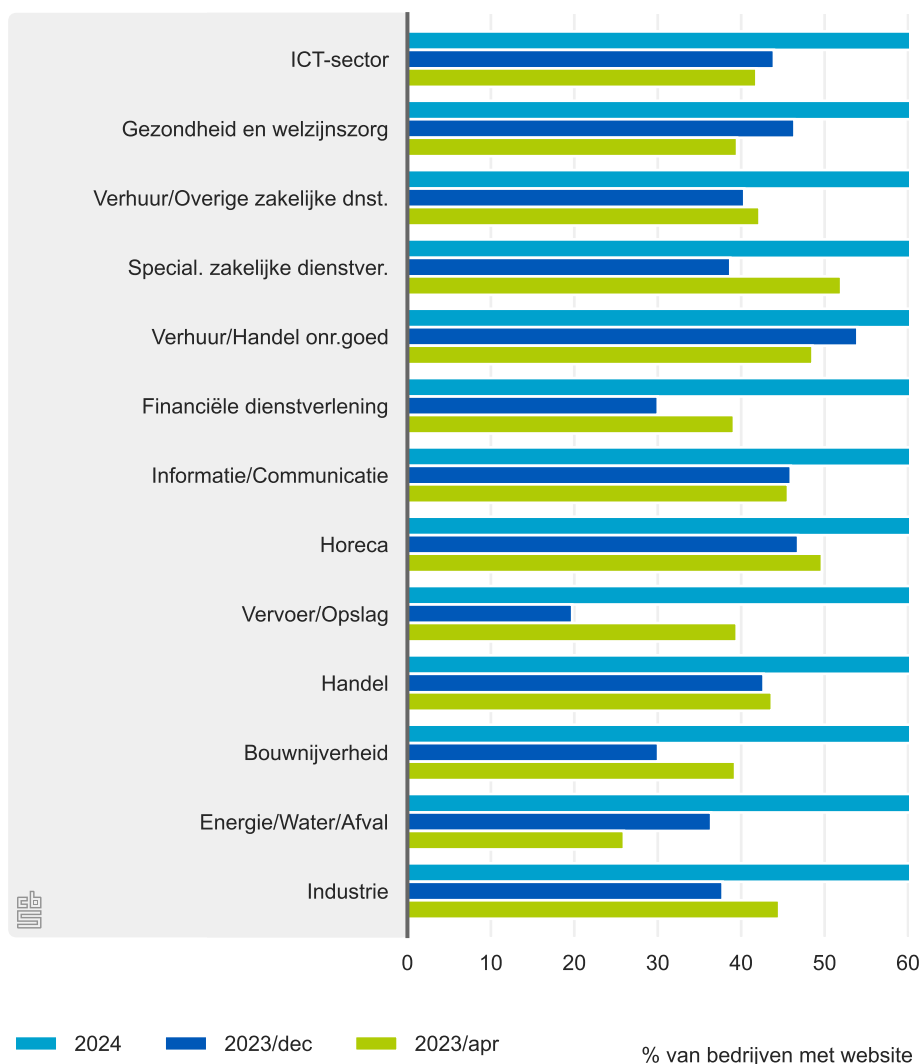


C.4.16 Percentage van bedrijven met website met geslaagde e-mailtest 'TLS 0-RTT' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse

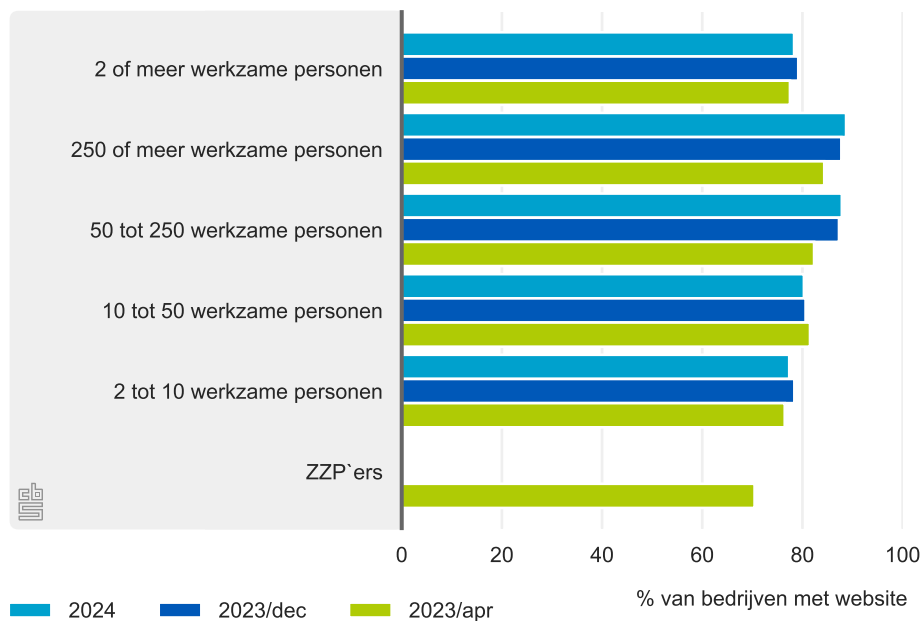


(b) Bedrijfstak

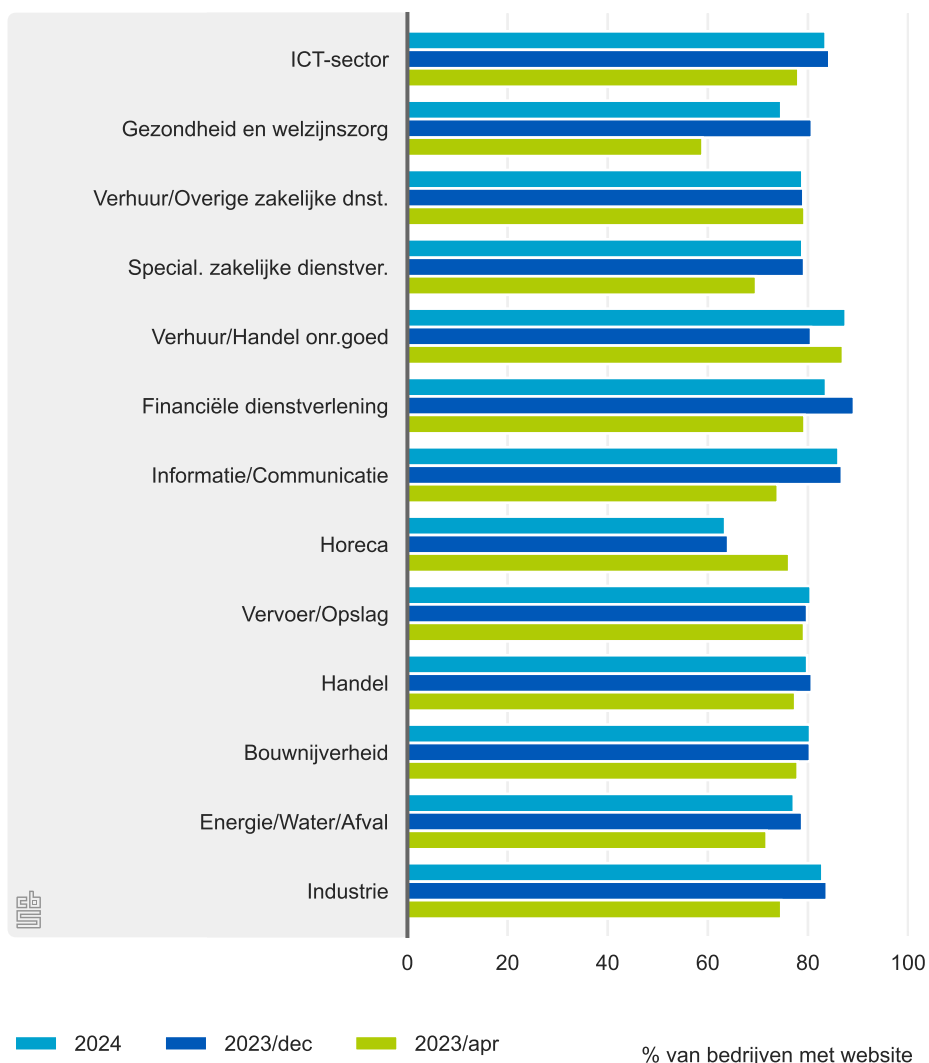


C.4.17 Percentage van bedrijven met website met geslaagde e-mailtest 'TLS Hashfunctie voor sleuteluitwisseling' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse



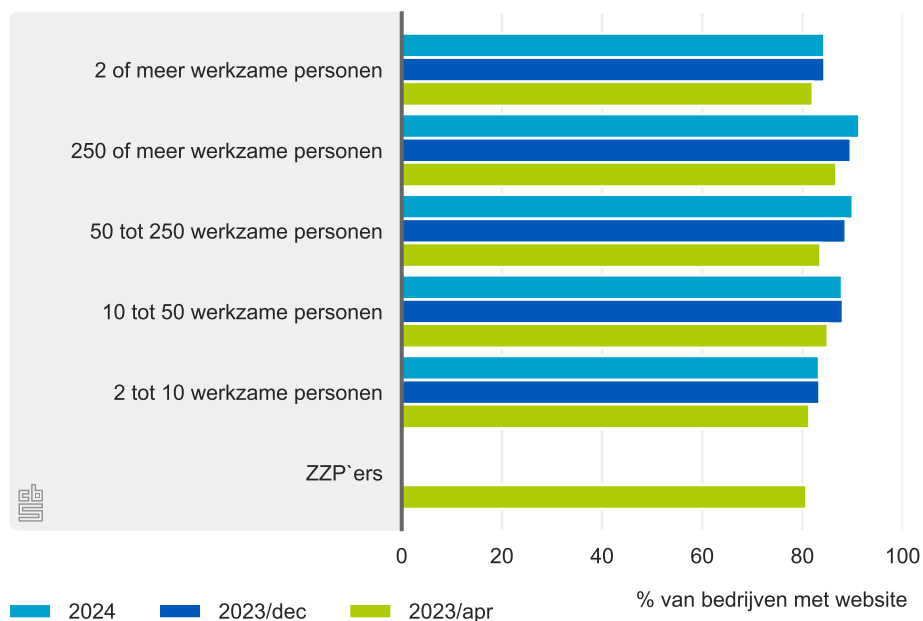
(b) Bedrijfstak



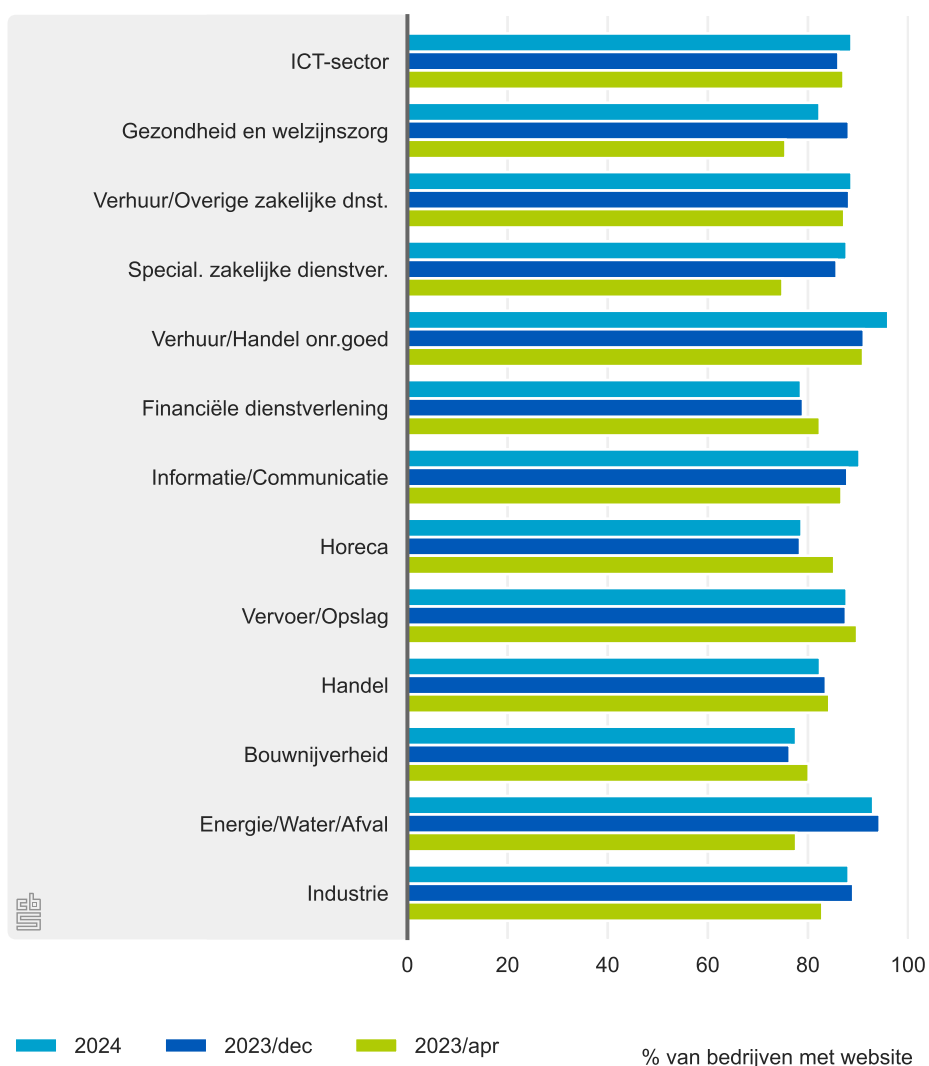
C.5 E-mailtestuitslagen voor categorie `RPKI`

C.5.1 Percentage van bedrijven met website met geslaagde e-mailtest 'RPKI Route Oorsprong Autorisatie bestaat' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse

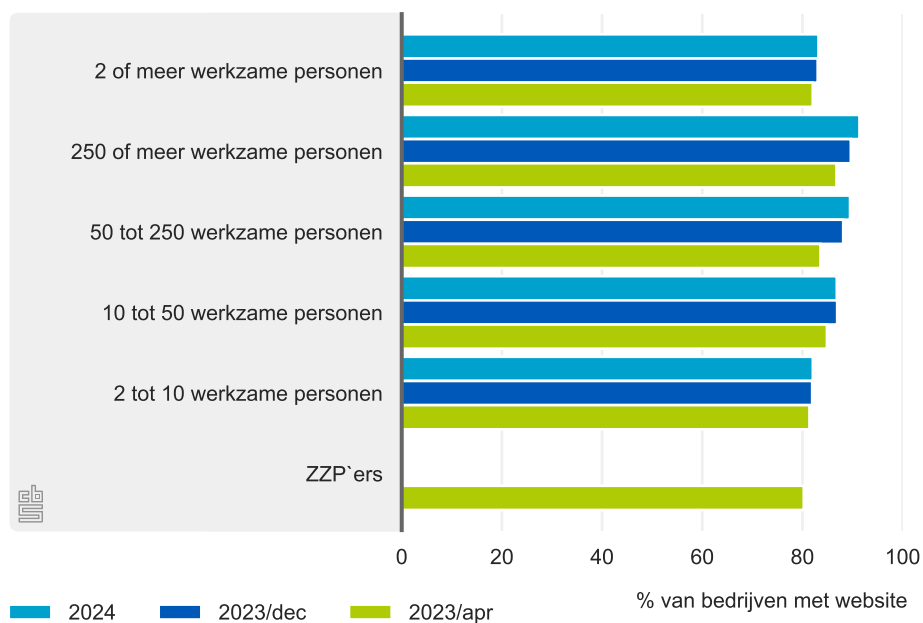


(b) Bedrijfstak

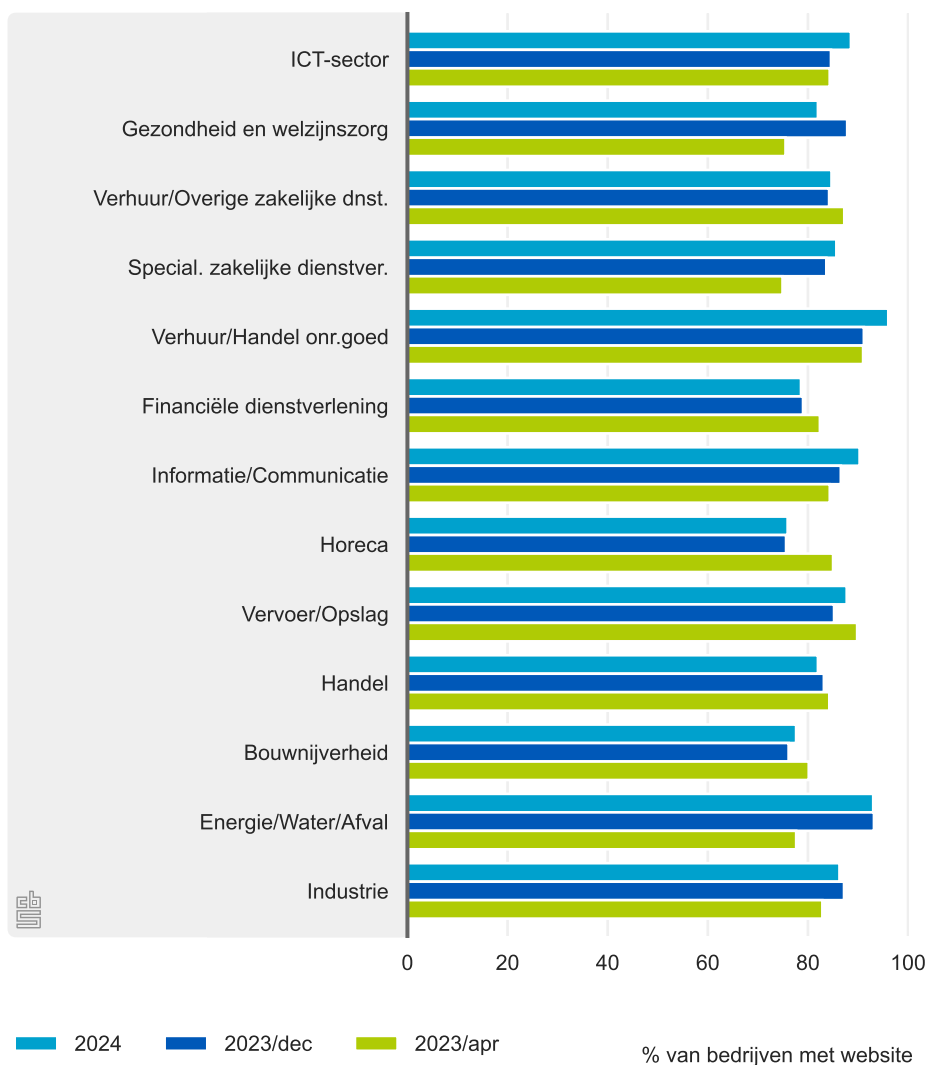


C.5.2 Percentage van bedrijven met website met geslaagde e-mailtest 'RPKI Route Oorsprong Autorisatie is geldig' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse

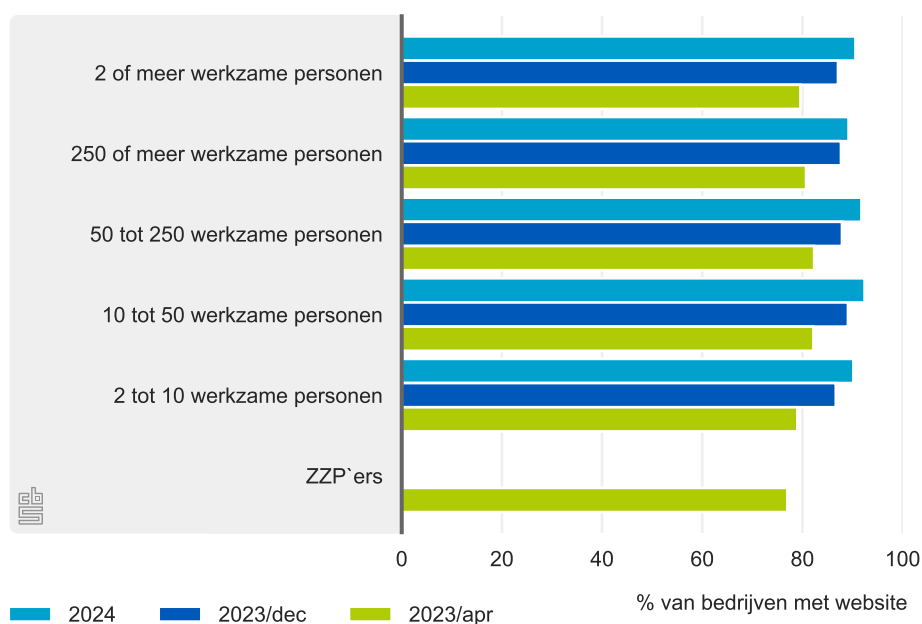


(b) Bedrijfstak

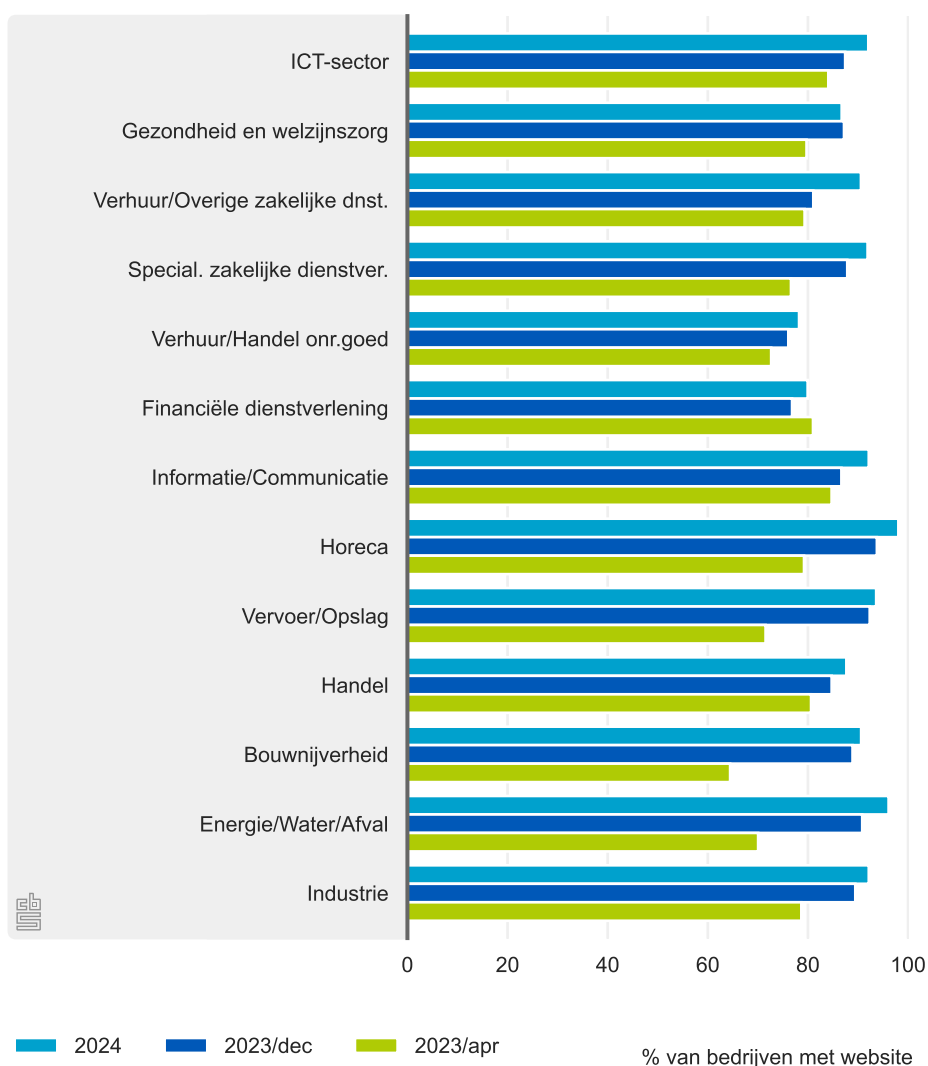


C.5.3 Percentage van bedrijven met website met geslaagde e-mailtest `RPKI voor nameserver bestaat' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse

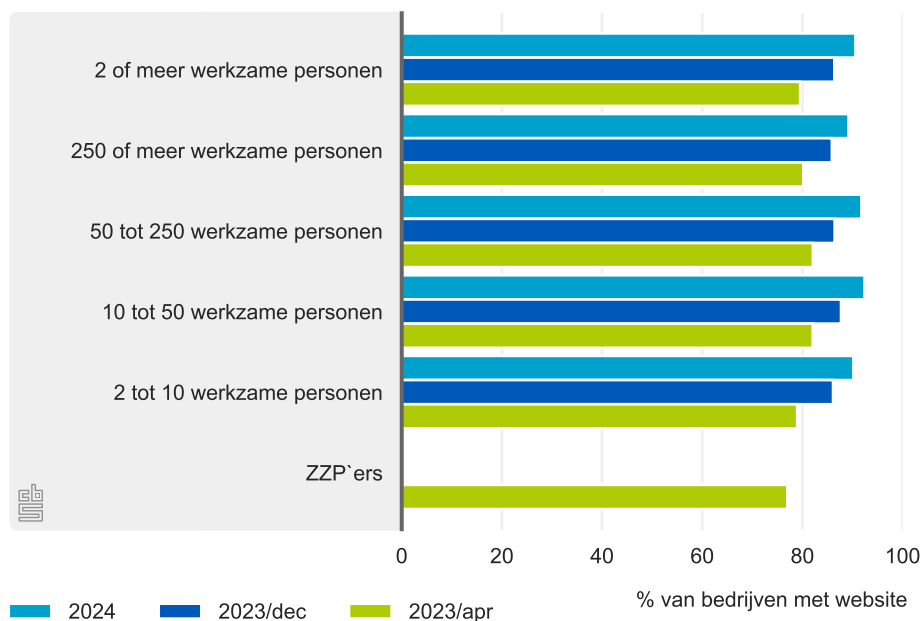


(b) Bedrijfstak

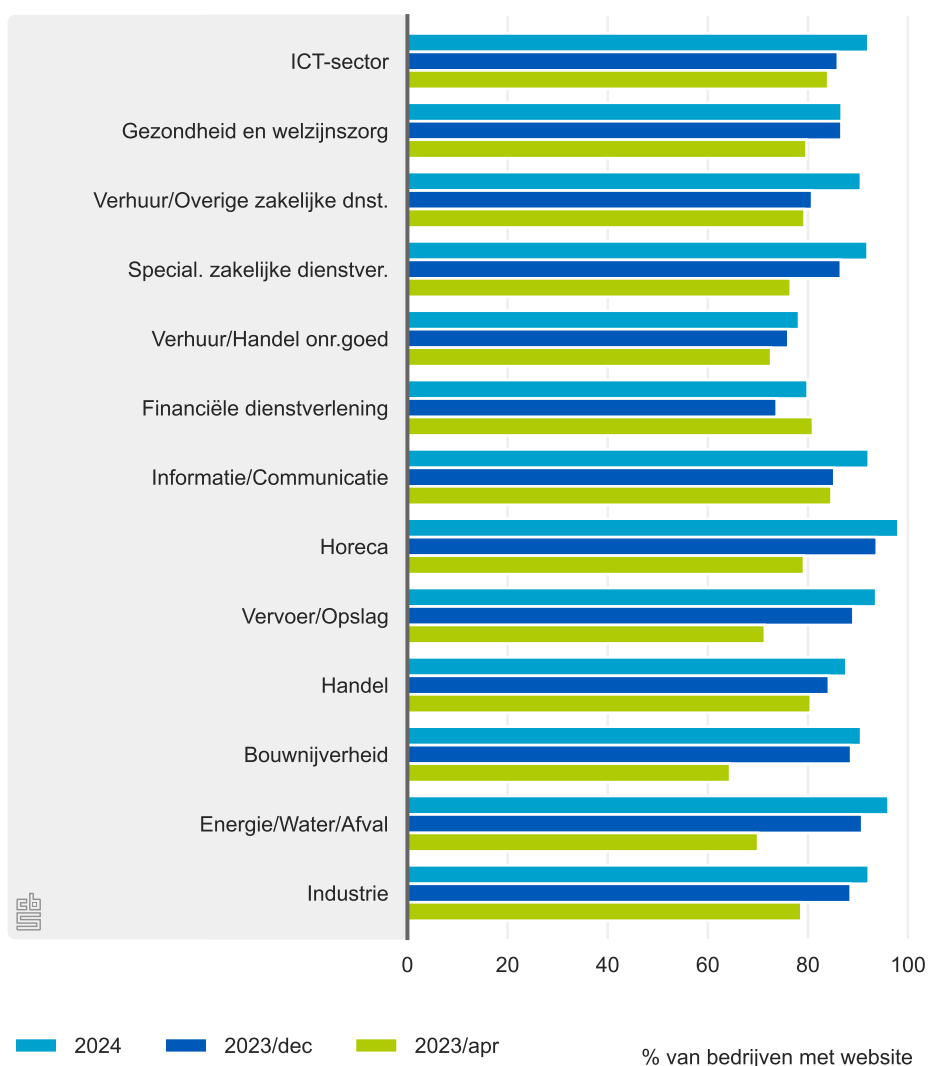


C.5.4 Percentage van bedrijven met website met geslaagde e-mailtest 'Geldigheid van RPKI voor nameserver' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse

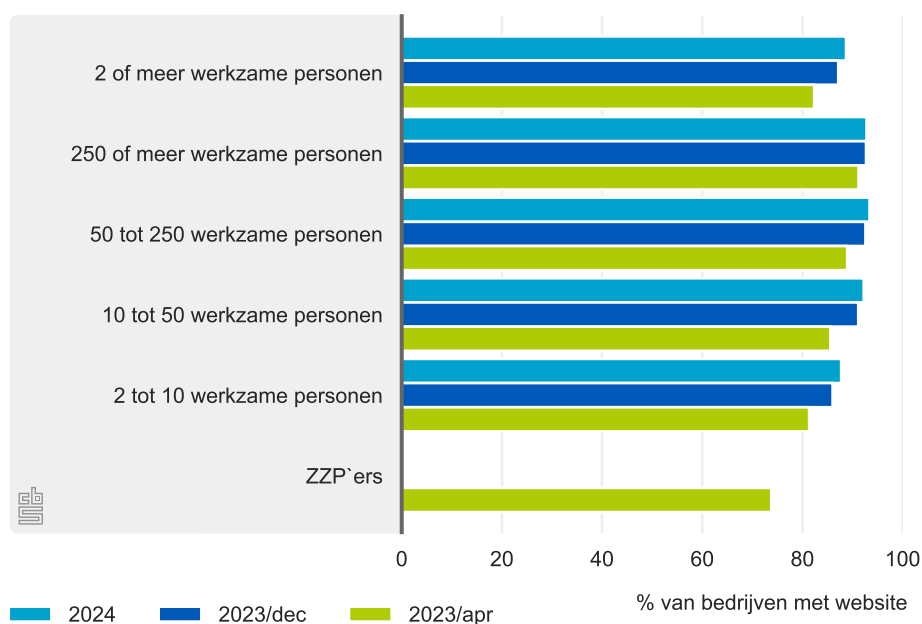


(b) Bedrijfstak

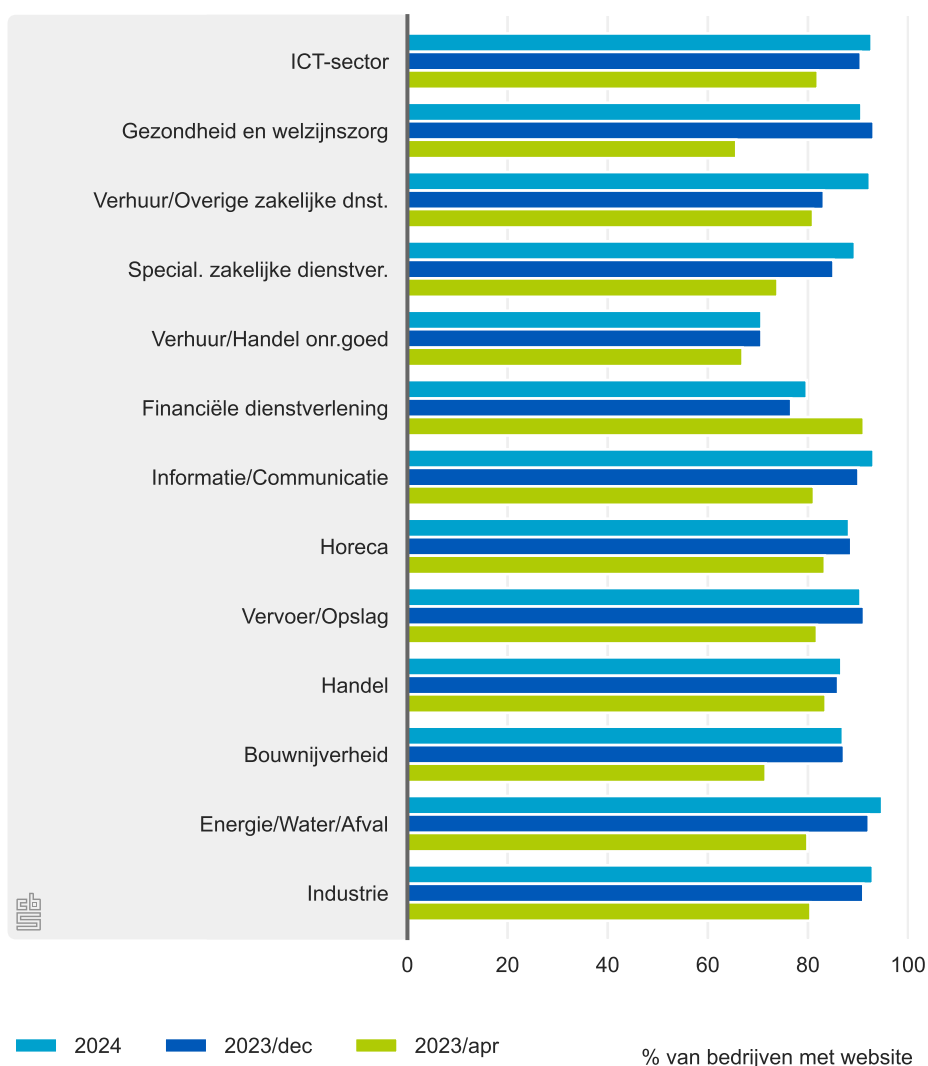


C.5.5 Percentage van bedrijven met website met geslaagde e-mailtest `RPKI bestaat voor mailservers' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse

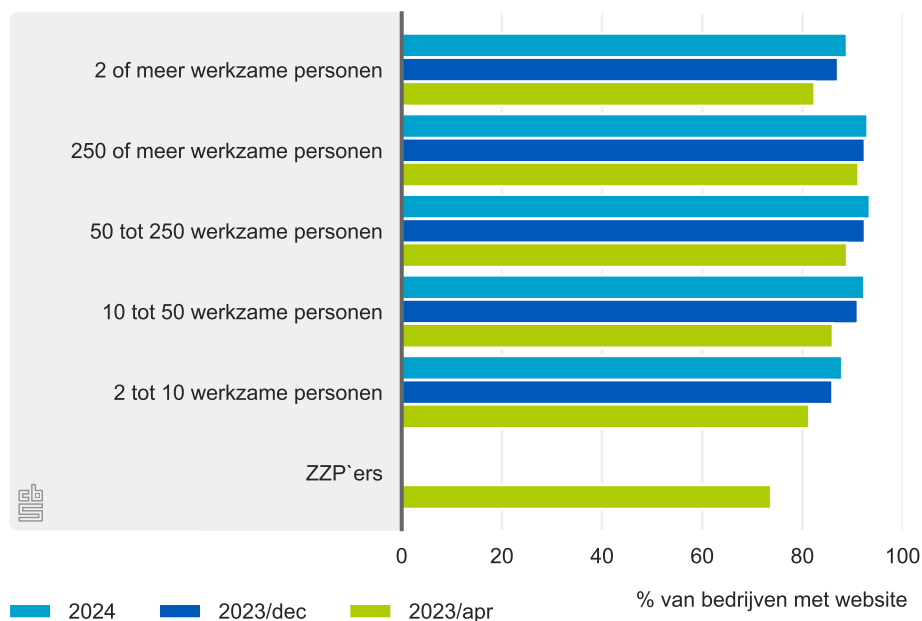


(b) Bedrijfstak

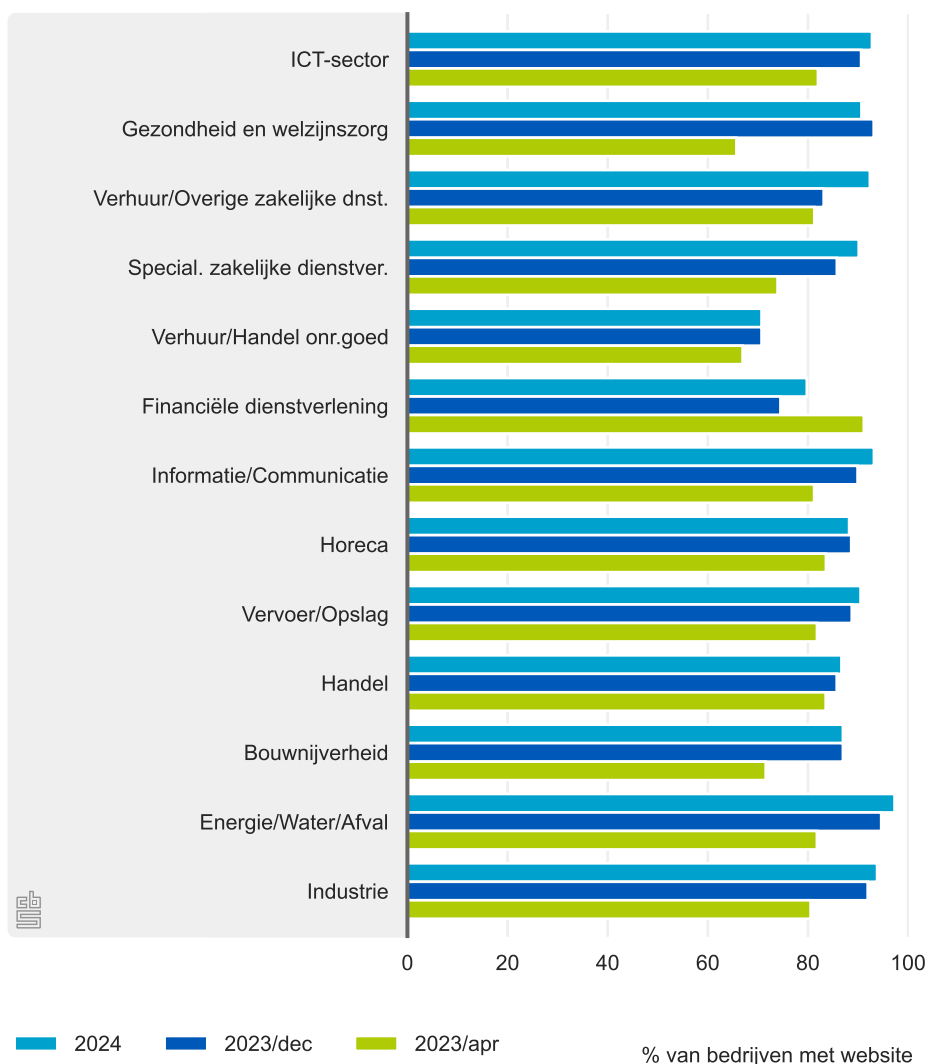


C.5.6 Percentage van bedrijven met website met geslaagde e-mailtest `Geldigheid van RPKI voor mailservers' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse



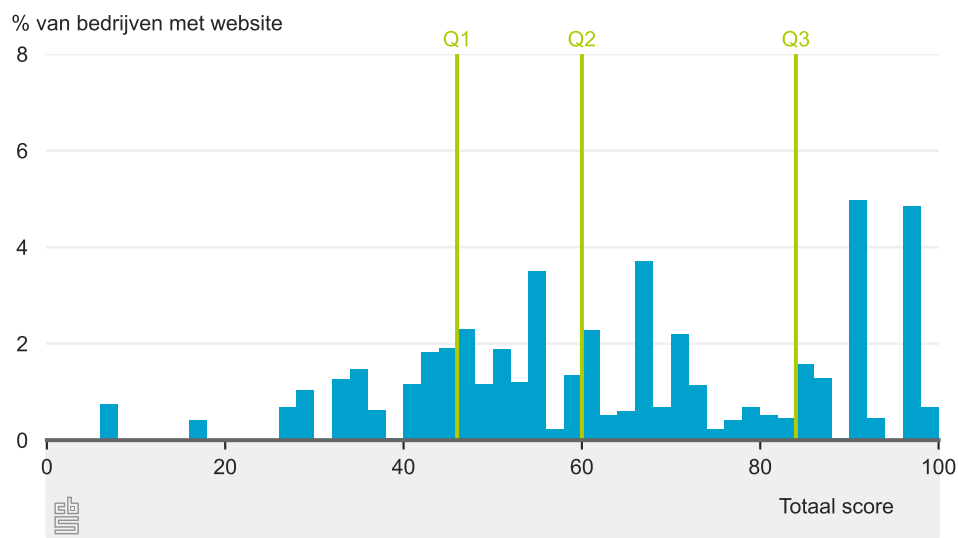
(b) Bedrijfstak



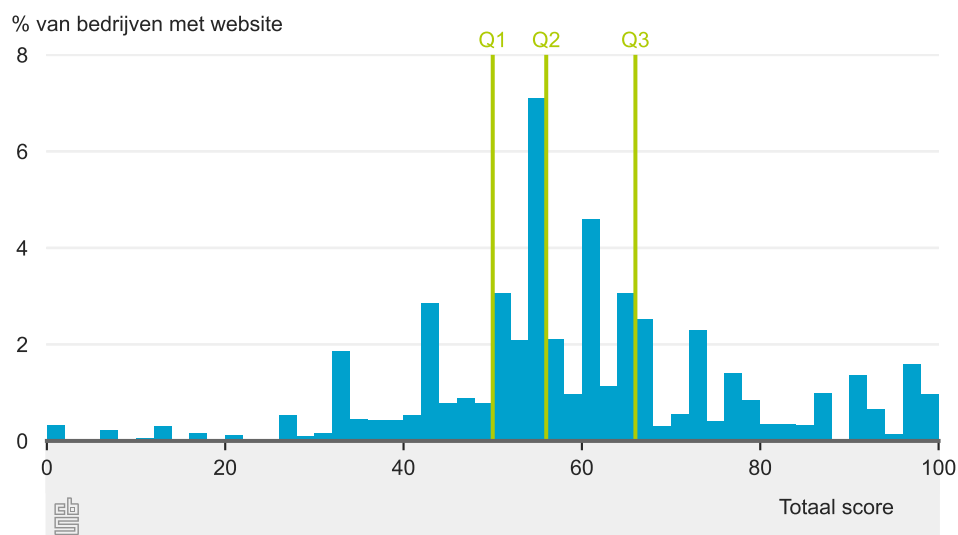
C.6 Email-scan eindscoreverderling

C.6.1 Verdeling van de email-scan Internet.nl-score voor alle bedrijven van Nederland voor 2023 en 2024.

(a) Scoreverdeling voor april, 2023



(b) Scoreverdeling voor december, 2023



(c) Scoreverdeling voor april, 2024

