Veiligheid van websites van bedrijven 2020

Een statistische analyse van Internet.nl scores

Veiligheid van websites van bedrijven 2020

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
2021–2022	2021 tot en met 2022
2021/2022	Het gemiddelde over de jaren 2021 tot en met 2022
2021/'22	Oogstjaar, boekjaar, schooljaar enz., beginnend in 2021 en eindigend in 2022
2019/'20–2021/'22	Oogstjaar, boekjaar, enz., 2019/'20 tot en met 2021/'22

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

Inhoud

1. Introductie

1.1 Achtergrond

In 2020 is het CBS in opdracht van het Ministerie van Economische Zaken en Klimaat samen met Forum Standaardisatie een onderzoek begonnen naar het gebruik van internetstandaarden bij websites van bedrijven in Nederland. In dit onderzoek heeft het CBS gebruikgemaakt van de website Internet.nl (Platform Internetstandaarden, 2021). De eerste resultaten zijn al beknopt in de CBS (2020b) gepresenteerd. In dit rapport wordt een volledig overzicht van de resultaten gepresenteerd.

De website Internet.nl is een testtool ontwikkeld in opdracht van Platform Internetstandaarden (2021). Het doel is om het gebruik van moderne en veilige Internetstandaarden te vergroten, om daarmee het gebruik van het Internet veiliger en betrouwbaarder te maken. Het idee is dat bedrijven of personen Internet.nl kunnen gebruiken om de domeinnaam van hun website in te voeren om een test (scan) uit te laten uitvoeren waarmee de veiligheid van de website getoetst wordt. Internet.nl toetst op de volgende aspecten:

- IPv6: bereikbaarheid via een modern internetadres.
- DNSSEC: gebruik van een ondertekende domeinnaam.
- https: gebruik van een beveiligde verbinding.
- Beveiligingsopties: gebruik van ingestelde Applicatie-beveiligingsopties.

Nadat de scan afgerond is, wordt een testrapport opgeleverd samen met een eindbeoordeling: een score tussen de 0 en 100 procent. Bedrijven die een 100 procent score halen, worden in de Hall of Fame opgenomen.

Uiteraard kan deze tool al direct door bedrijven gebruikt worden om hun eigen domeinnaam op veiligheid te toetsen. Indien het resultaat tegenvalt, kan dit bedrijven motiveren om extra beveiligingsmaatregelen toe te passen. In principe is het echter ook mogelijk om de tool te gebruiken om een statistische analyse op domeinnamen van bedrijven in Nederland uit te voeren. Op deze manier kan per bedrijfstak en bedrijfsgrootte in kaart worden gebracht hoe het met de veiligheid van websites van bedrijven is gesteld. Bij het onderzoek wordt gebruikgemaakt van de domeinnamen die in de enquête ICT-gebruik bij bedrijven (CBS, 2020a) ingevuld zijn als zijnde de website van het bedrijf. Op die manier wordt het mogelijk de veiligheid van websites van Nederlandse bedrijven te beschrijven op basis van een statistisch representatieve steekproef van bedrijven. De resultaten van dit onderzoek worden in dit rapport gepresenteerd.

In hoofdstuk 2 wordt de methode beschreven die gebruikt is om de internet.nl scans uit te voeren en te analyseren. De resultaten zullen in hoofdstuk 3 worden beschreven. In hoofdstuk 4 zijn ten slotte de belangrijkste conclusies en aanbevelingen opgenomen.

2. Methodebeschrijving

2.1 Domeinnamen

Enquête ICT-gebruik bij bedrijven

De domeinnamen die in dit onderzoek gebruikt worden, zijn verkregen uit de enquête 'ICT-gebruik bij bedrijven' (CBS, 2020a) (kortweg: de ICT-enquête). In deze jaarlijkse enquête onderzoekt het CBS het gebruik van informatie- en communicatietechnologie (ICT) door bedrijven, waarbij wordt ingegaan op verschillende aspecten, zoals ICT-veiligheid, ICT en personeel, software- en hardwaregebruik, enzovoort. De gegevens worden uiteindelijk uitgesplitst naar bedrijfsgrootteklasse en bedrijfstak gepubliceerd op Statline.

In de *ICT-enquête* wordt ook naar de domeinnaam van de website van het bedrijf gevraagd. Op deze manier is van een representatieve steekproef van bedrijven bekend welke websites daarbij behoren. De enquête werd in 2020 naar bijna 22 duizend bedrijven verzonden, wat uiteindelijk 12 duizend domeinnamen opleverde. Van al deze 12 duizend domeinnamen is een scan met de API van Internet.nl gedaan. Doordat gewerkt is met een statistisch representatieve steekproef kunnen de resultaten ook naar landelijke gemiddelden per bedrijfsgrootteklasse en bedrijfstak worden vertaald. De verdeling van de gescande domeinnamen over bedrijfsgrootteklassen en bedrijfstakken wordt in figuur 2.1.1 gegeven.

Ophoging van de eindscore

In de context van dit project is een Python tool (zie CBS, 2021) ontwikkeld om effectief de API van Internet.nl voor 12 duizend domeinnamen aan te roepen en de resultaten binnen te halen. Per domeinnaam levert dit een eindscore op die weergeeft hoe veilig een website van een bedrijf is. Deze eindscore wordt berekend aan de hand van subtesten die opgedeeld zijn in vier 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.

Ieder van deze categorieën bestaat uit verschillende sub-testen. Een overzicht van deze subtesten wordt in tabel A.2.1 gegeven. Meer informatie over de testen is te vinden op de website van Internet.nl.

In dit onderzoek wordt de eindscore gebruikt om de gemiddelden per bedrijfsgrootteklasse en bedrijfstak te berekenen. Hiertoe wordt het gewogen gemiddelde aan de hand van weegfactoren berekend, waarbij de weegfactor berekend wordt door per grootteklasse 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 respectievelijk tabel A.1.1 en A.1.2.

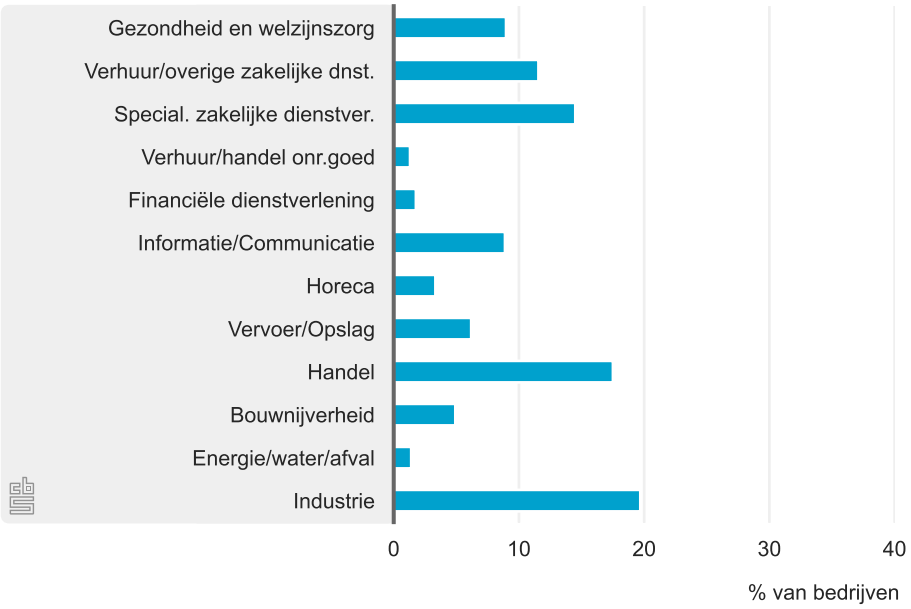
Relatieve score per subgroep

De uiteindelijke score die Internet.nl aan een website geeft, wordt bepaald door de resultaten van de verschillende testen die genoemd zijn. De exacte berekening van de score is niet bekend in dit onderzoek. Toch is geprobeerd een inschatting te krijgen over hoe goed ieder bedrijf per categorie scoort. Hiervoor wordt de relatieve score per subgroep geïntroduceerd. De subgroepen worden ook in tabel A.2.1 gegeven. De categorieën IPv6, DNSSEC, en beveiligingsopties bevatten slechts één subgroep, maar de grotere categorie HTTPS is opgedeeld in vier subgroepen: *https*, *tls*, *cert* en *dane*. De relatieve prestatie van een subgroep wordt uitgedrukt in het percentage van testen uit een subgroep dat een uitslag 'geslaagd' toegekend krijgt. Dit is niet helemaal zuiver, omdat sommige testen alleen conditioneel gedaan worden waardoor een 100 procent relatieve score voor de subgroep niet mogelijk is. Toch geeft de relatieve score per subgroep een goede indicatie hoe goed bedrijven in iedere subgroep scoren. In het volgende hoofdstuk wordt hier dieper op ingegaan.

2.1.1 Verdeling van de 12 duizend gescande domeinnamen over de bedrijfsgrootteklassen (a) en bedrijfstakken (b).

(a) Bedrijfsgrootteklasse

(b) Bedrijfstak



3.
Resultaten

3.1 Introductie

De websitetest van Internet.nl test of websites, emails en internetverbindingen aan de moderne internetstandaarden voldoen. In deze analyse wordt alleen de website-analyse uitgevoerd om de status van websites van bedrijven in Nederland in kaart te brengen. Voor de analyse worden 12 duizend domeinnamen uit een representatieve steekproef van bedrijven genomen.

De website-analyse van Internet.nl bevat 4 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.

De score per categorie wordt weer bepaald aan de hand van een aantal testen per categorie. Een overzicht van de vier categorieën met de bijbehorende subtesten wordt in Tabel A.2.1 gegeven.

In sectie 3.2 wordt eerst naar de eindscoreverdeling per bedrijfsgrootteklasse en bedrijfstak gekeken. Daarna worden de resultaten naar de hierboven genoemde categorieën opgesplitst.

3.2 Resultaten van Internet.nl per bedrijfsgrootteklasse en -tak

Eindscore niet afhankelijk van bedrijfsgrootte, wel van bedrijfstak

In figuur 3.2.1 wordt de verdeling van de eindscore van Internet.nl per bedrijfsgrootteklasse (a) en bedrijfstak (b) getoond. De gemiddelde eindscore per bedrijfsgrootte (figuur 3.2.1a) is vrij constant over de bedrijfsgrootteklassen, met een eindscore van rond de 60 procent. In de Cybersecuritymonitor (CBS, 2020b) wordt geconstateerd dat kleine bedrijven vaak minder maatregelen dan grote bedrijven treffen om hun ICT-systemen te beveiligen, maar op het gebied van de beveiliging van websites 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 wellicht 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 3.2.1b toont de gemiddelde eindscore per bedrijfstak. Hier zijn duidelijkere verschillen in gemiddelde eindscore te zien: de websites van de branch 'Energie/water/afval' scoren gemiddeld zo'n 55 procent op basis van Internet.nl, terwijl dit voor de websites van bedrijven in de Horeca bijna 10 procentpunt hoger is, namelijk een gemiddelde eindscore van

64 procent. In de Cybersecuritymonitor (CBS, 2020b) was eerder geconstateerd dat de Horeca gemiddelde genomen iets minder ICT-veiligheidsmaatregelen neemt voor de beveiliging van hun ICT systemen, dus het is opvallend dat de beveiliging van websites bij de Horeca juist hoger scoort dan gemiddeld. Weer geldt als meest voor de hand liggende verklaring de aanname dat de bouw van veel websites van horeca ondernemingen recenter en vaker door ICT-specialisten is uitgevoerd.

Uitkomsten Internet.nl-test per categorie

De eindscore die we nu bekeken hebben, wordt samengesteld uit de onderliggende testen zoals in tabel A.2.1 gegeven wordt. Deze testen zijn in vier categorieën opgedeeld: *IPv6*, *DNSSEC*, *HTTPS*, en *Beveiligingsopties*. Als een bedrijf voldoende testen binnen een categorie goed heeft, zal de categorie door de Internet.nl-test met 'geslaagd' aangeduid worden. In figuur 3.2.2, figuur 3.2.3, figuur 3.2.4 en figuur 3.2.5 worden per categorie de percentages 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 zijn per categorie. Zo laat figuur 3.2.2 bijvoorbeeld zien dat ruim twee keer zoveel kleine bedrijven slagen voor de categorie IPv6 dan grote bedrijven (respectievelijke 28,3 en 12,5 procent). Ook voor de categorie DNSSEC scoren kleine bedrijven beter dan grote bedrijven, zoals figuur 3.2.3 laat zien.

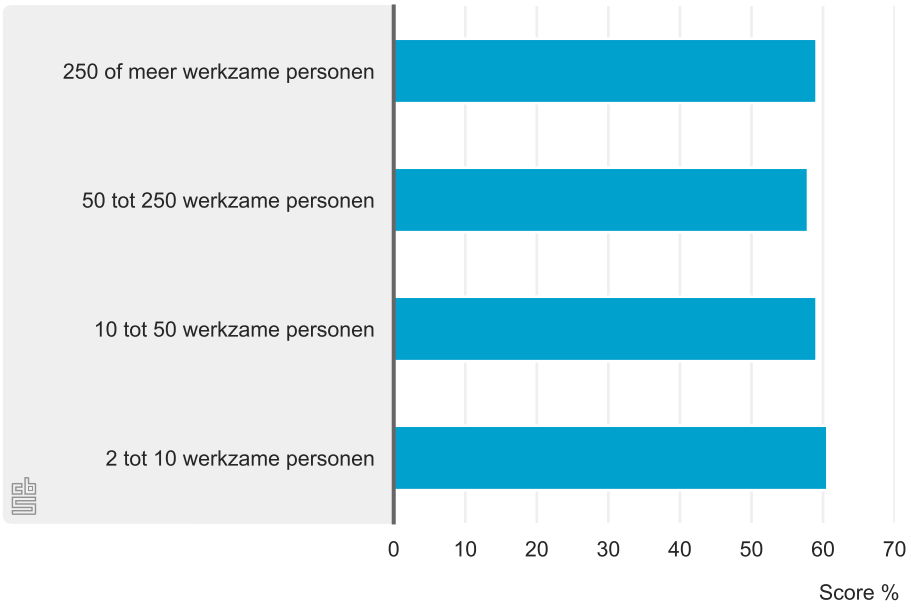
Voor de categorieën *HTTPS* en *Beveiligingsopties* (respectievelijk figuur 3.2.4 en figuur 3.2.5) is de trend juist precies anders: grote bedrijven scoren aanzienlijk beter voor deze categorieën. Dit verklaart ook waarom onder de streep de eindscore voor grote en kleine bedrijven ongeveer gelijk is: voor twee categorieën (IPv6 en DNSSEC) scoren kleine bedrijven beter, voor twee categorieën (HTTPS en Beveiligingsopties) scoren grote bedrijven beter. Het lijkt er op dat de resultaten voor beide categorieen elkaar compenseren, zodat de eindscore per bedrijfsgrootteklasse ongeveer constant is.

Zoals gezegd wordt de uitslag van een categorie bepaald aan de hand van de uitkomsten van de onderliggende testen die door een scan van Internet.nl uitgevoerd worden. De uitkomsten van alle onderliggende testen worden in de appendix B gegeven in de figuren B.1.1 tot en met B.1.32. In deze figuren is terug te vinden voor welke testen de verschillen tussen de verschillende bedrijfsgrootteklassen ontstaan. Zo is het verschil in het percentage van bedrijven dat slaagt voor de IPv6 testen voornamelijk te wijten aan de test 'IPv6-adressen voor webservers' (figuur B.1.3) en IPv6-bereikbaarheid van webservers, (figuur B.1.4). Voor deze testen slaagt ongeveer 30 procent van de kleine bedrijven, tegen 15 procent van de grote bedrijven.

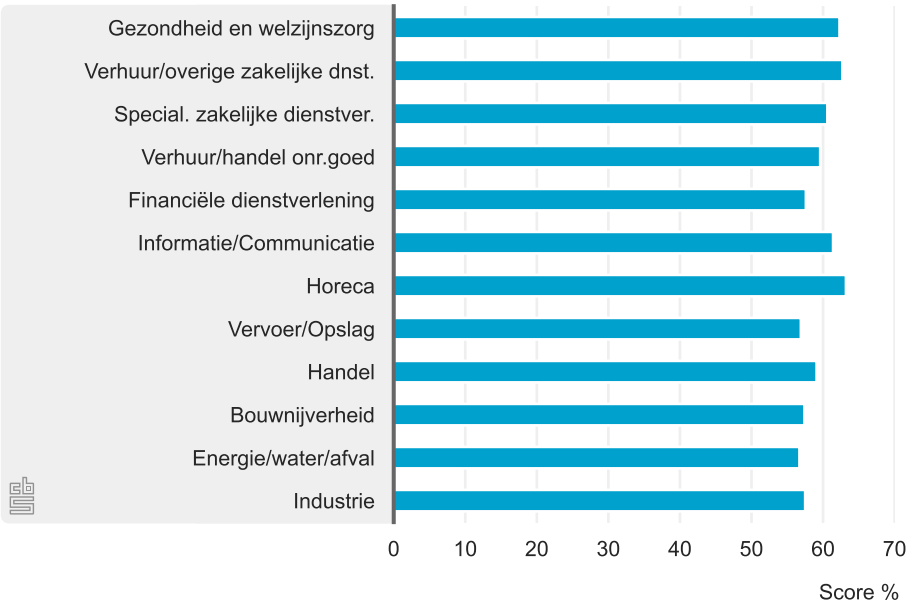
Een test waar grote bedrijven juist beter scoren dan kleine bedrijven is bijvoorbeeld '*HSTS policy* aangeboden' (figuur B.1.11), met een slagingspercentage van meer dan 30 procent tegen zo'n 10 procent voor kleine bedrijven. Voor de test op het gebruik van DANE (B.1.26) scoren kleine bedrijven juist weer een stuk beter dan grote, maar de slagingspercentages van deze test zijn vrij laag: slecht 2,2 procent van de kleine bedrijven gebruikt DANE. Daarom zal de uitkomst van deze test uiteindelijk niet veel bijdragen aan de uitkomst van de categorie HTTPS waar de DANE test onder valt.

3.2.1 Gemiddelde totaal score Internet.nl per bedrijfsgrootteklasse (a) en bedrijfstak (b)

(a) Bedrijfsgrootteklasse

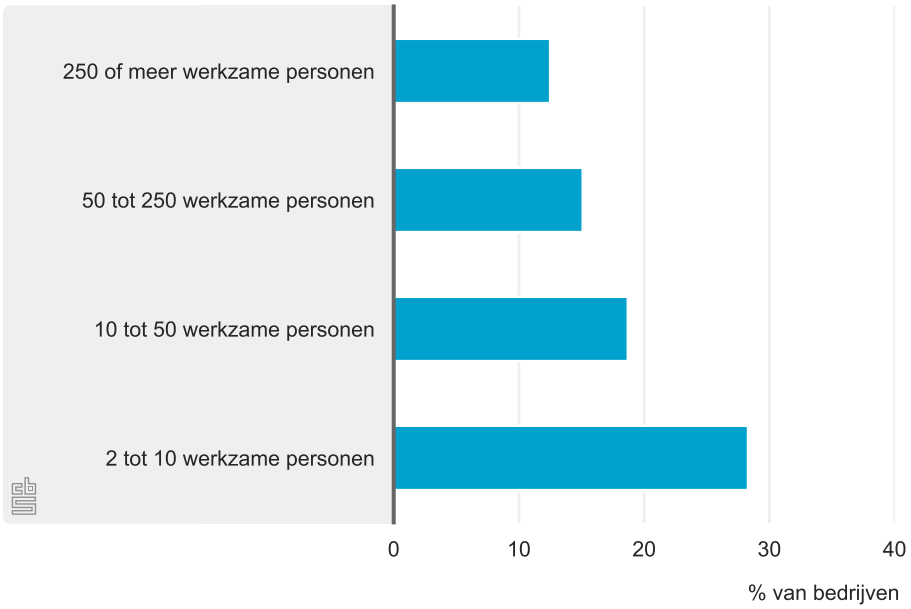


(b) Bedrijfstak

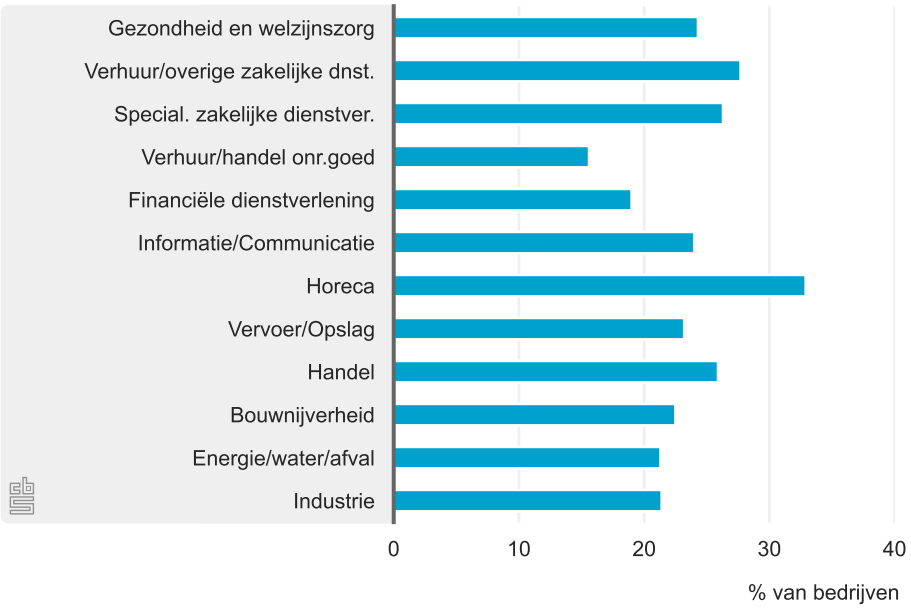


3.2.2 Percentage bedrijven met geslaagde categorie 'IPv6' per bedrijfsgrootteklasse (a) en bedrijfstak (b)

(a) Bedrijfsgrootteklasse

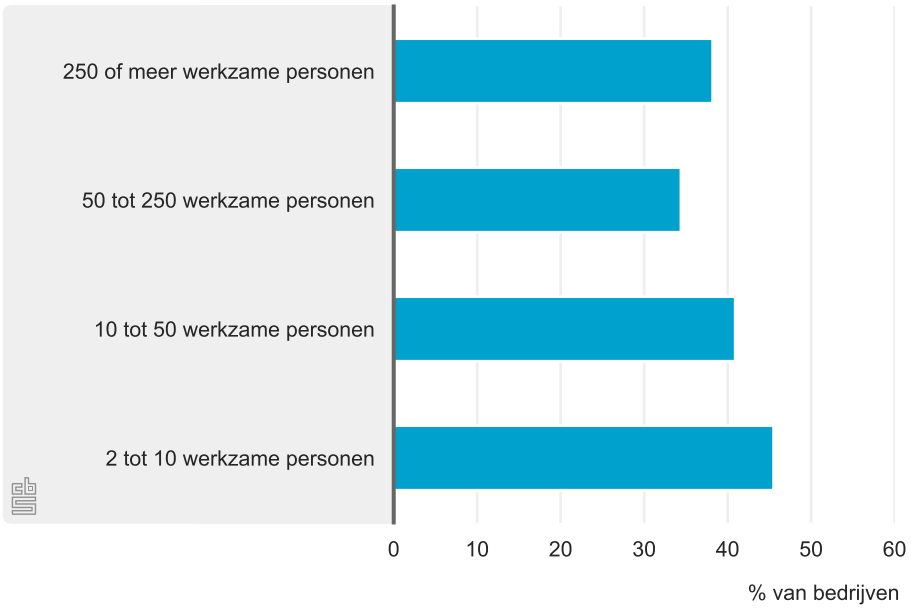


(b) Bedrijfstak

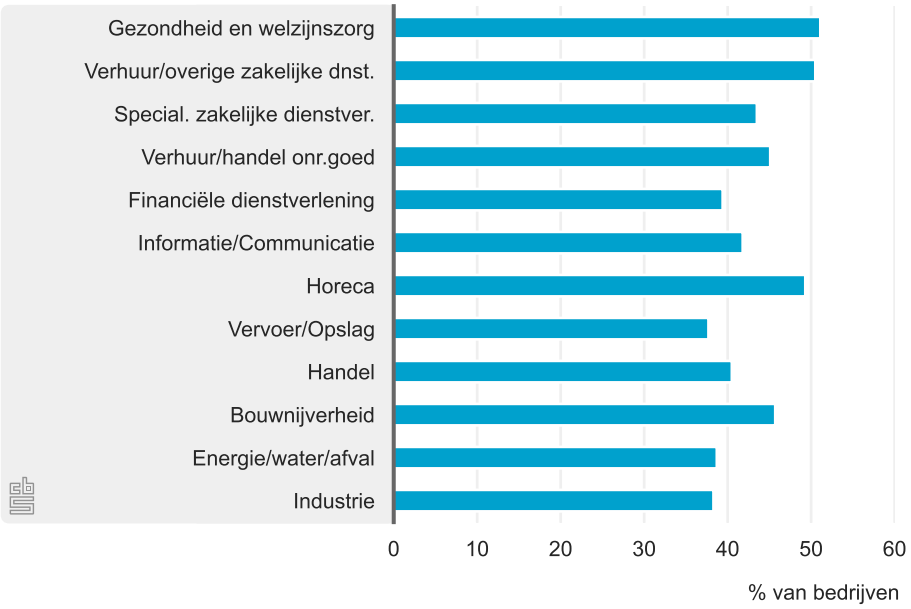


3.2.3 Percentage bedrijven met geslaagde categorie 'DNSSEC' per bedrijfsgrootteklasse (a) en bedrijfstak (b)

(a) Bedrijfsgrootteklasse



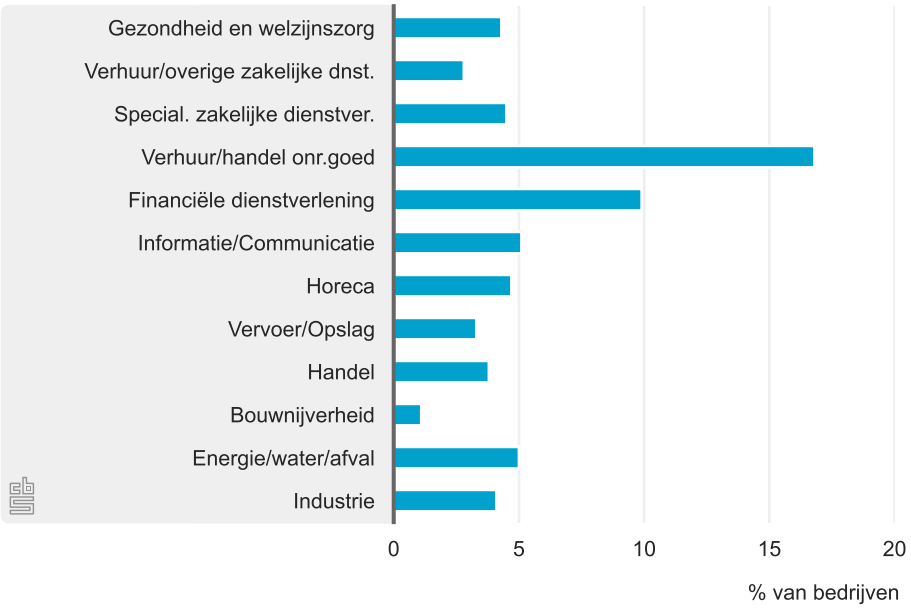
(b) Bedrijfstak



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

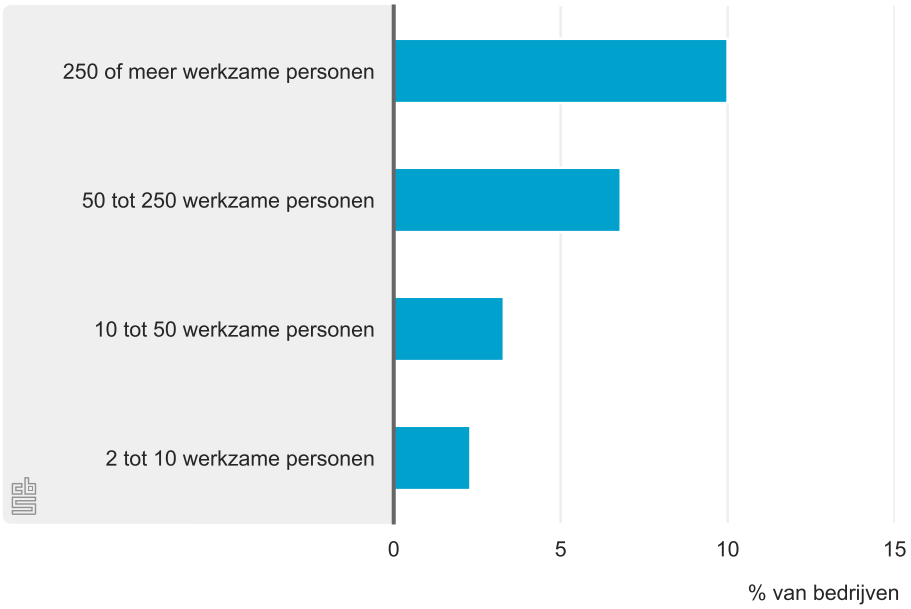
(a) Bedrijfsgrootteklasse

(b) Bedrijfstak

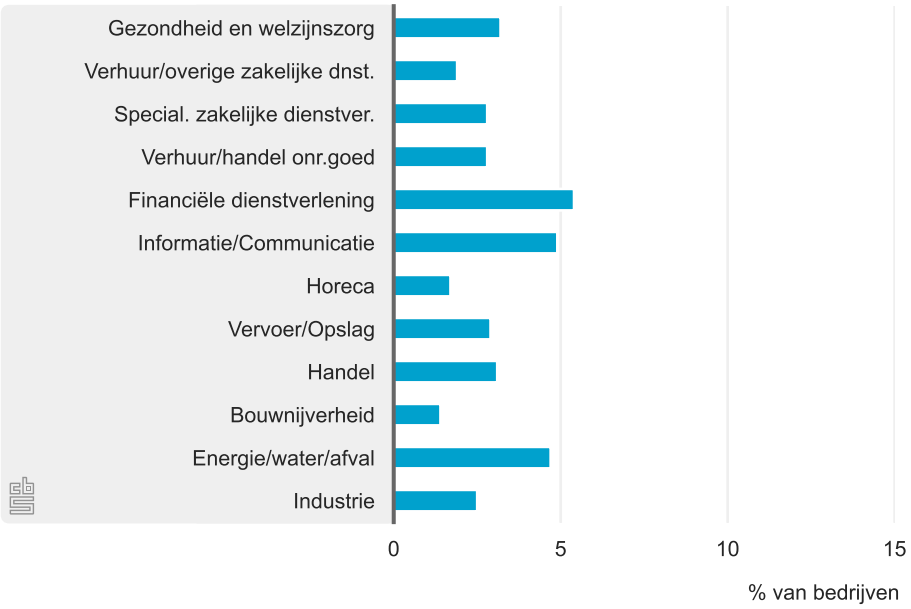


3.2.5 Percentage bedrijven met geslaagde categorie 'Beveiligingsopties' per bedrijfsgrootteklasse (a) en bedrijfstak (b)

(a) Bedrijfsgrootteklasse



(b) Bedrijfstak



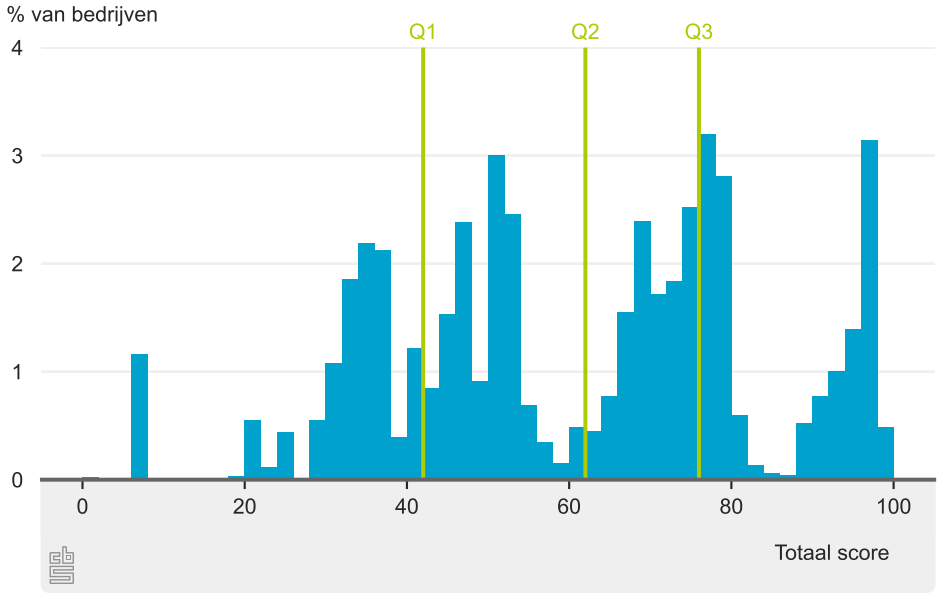
3.3 Verdelingen van de eindscores over alle bedrijven per categorie

Verdeling eindscore is aanzienlijk

Alhoewel de gemiddelde score 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 over alle bedrijven heen.

De verdeling van de eindscore voor alle bedrijven in Nederland is te zien in figuur 3.3.1. De verdeling kent een aantal pieken rond de 30, 50, 70 en 90 procent. In figuur 3.3.1 zijn verder nog drie kwartielen Q1, Q2, en Q3 weergegeven. Het eerste kwartiel Q1 geeft aan dat 25 procent van de bedrijven een eindscore lager dan 44 procent haalt. Het tweede kwartiel Q2, ook bekend als de mediaan, geeft 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 de volgende paragraaf wordt hier nog wat dieper op in gegaan.

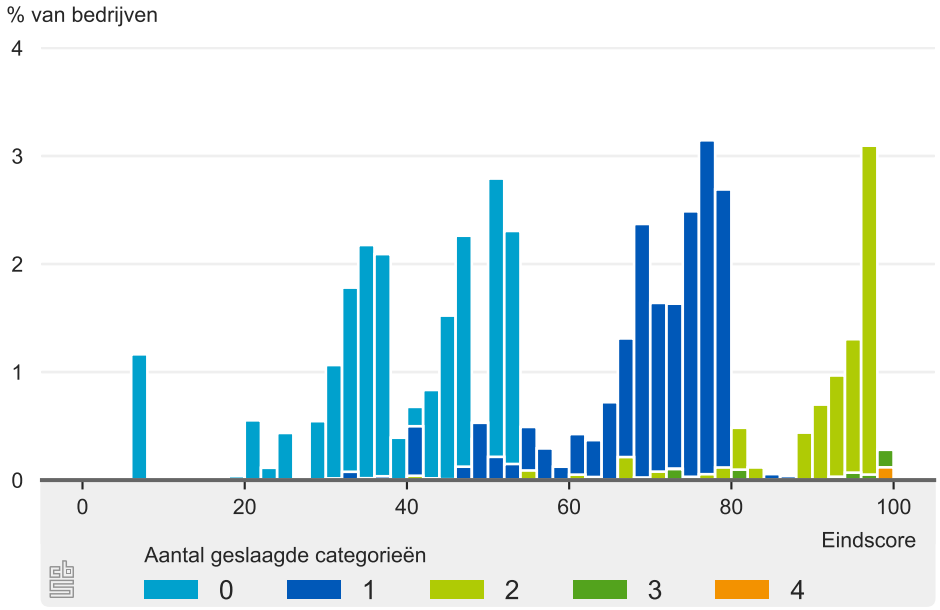
3.3.1 Verdeling van Internet.nl-score voor alle bedrijven van Nederland.



Conditionele eindscoreverdeling

Om te begrijpen waar de pieken in de eindscoreverdeling van figuur 3.3.1 door worden veroorzaakt, wordt de eindscoreverdeling in figuur 3.3.2 nogmaals geplot, maar dit keer als een *conditionele* verdeling: de eindscoreverdeling wordt hier geconditioneerd met het *aantal* geslaagde categorieën. Zo wordt in lichtblauw bijvoorbeeld de eindscoreverdeling getoond voor alleen die bedrijven die voor geen enkele categorie geslaagd zijn. Uiteraard zal dit overeenkomen met de lagere eindscores, wat consistent is met het feit dat we alleen de bedrijven meegenomen hebben die geen enkele geslaagde categorie hebben. Op dezelfde

3.3.2 Verdeling van Internet.nl-score voor alle bedrijven van Nederland opgesplitst naar het aantal geslaagde categorieën.



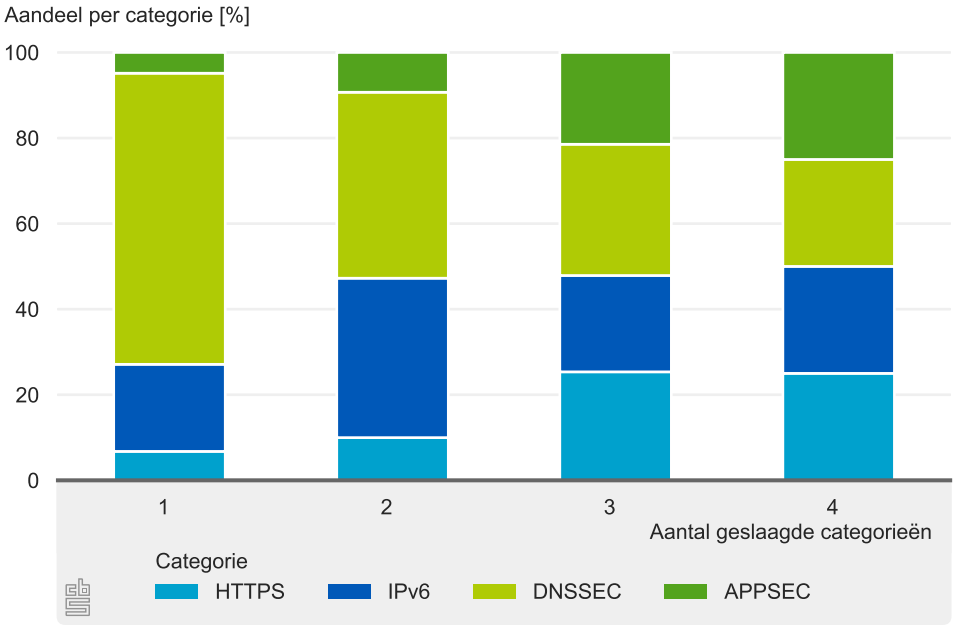
manier worden de bedrijven met slechts één geslaagde categorie in donkerblauw weergegeven, met twee geslaagde categorieën in lichtgroen, met drie geslaagde categorieën in donkergroen, en ten slotte met alle vier de categorieën geslaagd in oranje. Door alle conditionele eindscoreverdelingen cumulatief te plotten, komt de totale scoreverdeling in figuur 3.3.2 exact overeen met de ongeconditioneerde eindscoreverdeling van figuur 3.3.1.

In de conditionele eindscore verdeling is nu duidelijk te zien dat de pieken die we eerder gevonden hebben, min of meer overeenkomen met de verschillende categorieën waaruit de samengestelde plot bestaat. De bedrijven met geen enkele geslaagde categorie komen overeen met de eerste twee pieken met eindscores lager dan vijftig procent. De derde piek in de verdeling (met eindscores tussen de 60 en 80 procent) bestaat voornamelijk uit bedrijven die voor exact één categorie geslaagd zijn. De laatste piek is gelegen tussen de 90 en 98 procent met bijna alleen bedrijven die voor twee categorieën geslaagd zijn. Ten slotte vormen de bedrijven met drie of vier geslaagde categorieën het laatste staafje van de verdelingsplot met eindscores tussen de 98 en 100 procent. Dit suggereert dat de eindscore voor een groot deel bepaald wordt door het *aantal* geslaagde categorieën, met een spreiding rondom de ligging van de piek door verschillen in uitkomsten van de onderliggende testen.

Ten slotte is het opvallend dat er blijkbaar bedrijven zijn die voor drie categorieën geslaagd zijn, maar toch een eindscore lager dan 90 procent behalen. Ze worden dus in feite ingedeeld bij de bedrijven die voor twee categorieën geslaagd zijn. Bedrijven die voor drie categorieën geslaagd zijn hebben dus voor één categorie een onvoldoende gehaald (omdat er in totaal vier categorieën zijn). Inspectie van de data laat zien dat bedrijven met drie geslaagde categorieën, maar toch relatief laag scoren (een eindscore onder de 90 procent), allemaal de categorie DNSSEC (20 procent van de gevallen) *of* de categorie Ipv6 (80 procent van de gevallen) missen. Anders gezegd: dit betekent dat om met drie categorieën een score boven de 90 procent te halen, een bedrijf voor de categorieën DNSSEC *en* IPv6 moet slagen. Alle bedrijven die voor alle vier de categorieën slagen, halen een score van 100 procent.

Verhouding geslaagde categorieën

3.3.3 Relatieve verhouding geslaagde categorieën tegen het aantal geslaagde categorieën.



In figuur 3.3.3 wordt de verhouding tussen de geslaagde categorieën gepresenteerd als we conditioneren per aantal geslaagde categorieën. Het was al eerder aangetoond in figuur 3.3.2 dat bedrijven die voor één categorie geslaagd zijn, een eindscoreverdeling tussen de 60 en 80 procent hebben met uitlopers naar lagere scores. In figuur 3.3.3 is terug te vinden dat bedrijven die met één categorie slagen, dit in 68 procent van de gevallen doen voor de categorie DNSSEC en in 20 procent van de gevallen voor categorie IPv6. De overige 12 procent van de bedrijven die voor exact één categorie slagen, doen dat voor de categorie HTTPS of de categorie APPSEC. Op dezelfde wijze kan gekeken worden naar relatieve verdelingen van de groepen bedrijven die voor 2, 3 en 4 categorieën slagen. Per definitie is de verhouding voor de bedrijven die voor alle vier de categorieën slagen exact gelijk verdeeld met 25 procent per categorie. Maar waar het om gaat, is de constatering dat de categorieën DNSSEC en IPv6 de eerste categorieën zijn waar bedrijven voor slagen. Van deze categorieën was in figuur 3.2.3 en figuur 3.2.2 aangetoond dat kleine bedrijven hiervoor relatief wat vaker slagen dan grote bedrijven.

3.4 Verdelingen van de eindscores over alle bedrijven per subgroep

Relatief aantal geslaagde testen per subgroep

Tot nu toe is naar eindscore en de uitslag per categorie (*IPv6*, *DNSSEC*, *HTTPS* en *APPSEC*) gekeken. Of een categorie wel of niet als 'geslaagd' wordt aangeduid, wordt met behulp van de onderliggende testen bepaald. Als een bedrijf niet voor een categorie slaagt, kan toch iets gezegd worden over de prestatie in deze categorie door te kijken naar het percentage geslaagde testen binnen deze categorie. In tabel A.2.1 worden alle categorieën en

onderliggende testen getoond. Omdat de categorie HTTPS uit veel meer testen bestaat dan de overige categorieën, is deze categorie weer opgedeeld in vier subgroepen: *https*, *tls*, *cert* en *dane*. De overige categorieën hebben allemaal één subgroep met dezelfde naam als de categorie zelf: de *dnssec*, *ipv6* en *appsec* (ook wel beveiligingsopties genoemd).

Voor een bedrijf kan per subgroep een genormaliseerde score gedefinieerd worden als het aantal geslaagde testen in een subgroep gedeeld door het aantal testen in deze groep. Deze genormaliseerde score worden hier verder aangeduid als de subgroepscore. Zo heeft de categorie *HTTPS* bijvoorbeeld de subgroep *http*, met een subgroepscore die volgt uit het percentage geslaagde testen uit de subgroep *http*. Op die manier kan voor ieder bedrijf per subgroep een score toegekend worden, waar vervolgens een gemiddelde over alle bedrijven uit bepaald kan worden.

De subgroepscore is een versimpelde weergave van de prestatie in zo'n subgroep, omdat de score niet altijd op 100 procent hoeft uit te komen. Sommigen testen zijn niet relevant onder bepaalde omstandigheden en worden in een geavanceerdere scoreberekening buiten beschouwing gelaten. Daar wordt met de genormaliseerde subgroepscore geen rekening mee gehouden. Deze score is hier alleen geïntroduceerd om toch wat inzicht te krijgen hoe bedrijven per subgroep voor de verschillende onderliggende testen scoren. Uiteraard kunnen de uitslagen per test, zoals die in appendix B gegeven worden, hier ook bij helpen.

Testen per subgroep voor bedrijven met nul geslaagde categorieën

In figuur 3.4.2a wordt de subgroepscore per aantal geslaagde categorieën gegeven. Als bedrijven nog voor geen enkele categorie geslaagd zijn, dan is te zien dat bedrijven in deze categorie gemiddeld voor 87 procent van de testen in de subgroep *cert* slagen. De bedrijven die voor geen enkele categorie slagen zijn terug te vinden als de lichtblauwe scores in figuur 3.3.2: de eindscores liggen dus tussen de 10 en 60 procent. Toch hebben relatief veel bedrijven dan al HTTPS met valide certificaten. De uitkomsten van de onderliggende testen (https certificaat met vertrouwensketen, publieke sleutel, handtekening en domeinnaam) worden bij bedrijfsgrootteklasse en bedrijfstak in figuur B.1.22, figuur B.1.23, figuur B.1.24 en figuur B.1.25 gegeven. Geconstateerd kan worden dat inderdaad over alle bedrijfsgrootteklassen en takken heen meer dan 80 procent van de bedrijven slagen voor deze testen als alle scores bij elkaar genomen worden, zonder te conditioneren met het aantal geslaagde categorieën.

Na de subgroep *certificaten* uit de categorie *HTTPS*, scoren uit dezelfde categorie de testen uit de subgroepen *http* en *tls* het hoogst. De testen uit de *http* subgroep zijn: HTTPS beschikbaar (figuur B.1.8), HTTPS met doorverwijzing (figuur B.1.9), HTTPS zonder compressie (figuur B.1.10) en HSTS aangeboden (figuur B.1.11). De testen uit de HTTPS/tls subgroep zijn TLS-versie (figuur B.1.12), ciphers (figuur B.1.13), cipher-volgorde (figuur B.1.14), sleuteluitwisselingsparameters (figuur B.1.15), hash-functies (figuur B.1.16), tls zonder compressie (figuur B.1.17), *secure regeneration* (figuur B.1.18), *client initiated regeneration* (figuur B.1.19), 0-RTT (figuur B.1.20) en OCSP-stapeling (figuur B.1.21). Het genormaliseerde aantal geslaagde testen per subgroep in beide groepen is gemiddeld 55 procent, dat wil zeggen dat gemiddeld iets meer dan de helft van de testen van iedere subgroep succesvol was voor bedrijven met geen enkele geslaagde categorie.

De testen uit de categorie IPv6, te weten IPv6 *nameservers* beschikbaar en bereikbaar (respectievelijk figuur B.1.1 en figuur B.1.2) en IPv6 *webservers* beschikbaar en bereikbaarheid (respectievelijk figuur B.1.3 en figuur B.1.4) en gelijke website voor IPv4 en

IPv6 (figuur B.1.5) slagen gemiddeld voor gemiddeld 27 procent van de testen als bedrijven geen enkele categorie geslaagd hebben.

De testen uit de categorie Beveiligingsopties (ook wel APPSEC) zijn: *X-Frame opties* (figuur B.1.28), *X-Content-Type options* (figuur B.1.29), *Content-Security-Policy* (figuur B.1.29) en *Reference-Policy* (figuur B.1.31). In deze subgroep wordt voor de bedrijven met geen enkele geslaagde categorie gemiddeld slechts 9 procent van de testen gehaald.

Uit de categorie DNSSEC met één gelijknamige subgroup, slaagt voor de bedrijven die geen geslaagde categorieën hebben, gemiddeld geen van de testen in de subgroep. Het gaat in deze subgroep om slechts 2 testen: *DNSSEC aanwezig* (figuur B.1.6) en *DNSSEC geldig* (figuur B.1.7), dus de mogelijke uitkomsten voor de genormaliseerde testscores in deze subgroep zijn per bedrijf 0, 50 of 100 procent. Hetzelfde geldt voor de subgroep DANE (uit de categorie HTTPS) waarvoor ook bedrijven met nul geslaagde categorieën voor geen van de testen slaagt voor DANE aanwezig (figuur B.1.26) en DANE valide (figuur B.1.27).

Testen per subgroep voor bedrijven met één of twee geslaagde categorieën

In figuur 3.4.2a is verder te zien dat bedrijven die voor precies één categorie slagen, de gemiddelde subgroepscore voor de groepen http, cert en tls uit de categorie HTTPS alle slechts een paar procent toenemen. De gemiddelde subgroepscore van DNSSEC neemt echter toe van nul procent naar 68 procent. Dit duidt er al op dat de stap van nul naar één geslaagde categorie voornamelijk bepaald wordt door het gebruik van DNSSEC. In figuur 3.3.2 is te zien dat bedrijven die voor één categorie slagen, bijna allemaal een eindscore behalen tussen de 60 en 80 procent. Uit figuur 3.3.3 was hierboven geconcludeerd dat bedrijven die voor maar één categorie slagen, voornamelijk slagen voor de categorie DNSSEC en daarmee in de eindscoreverdeling opschuiven naar de hogere scores boven de 60 procent. De drie subgroepen die vallen onder HTTPS hebben een vergelijkbare score, maar omdat ze samen met een vrij laag scorende subgroep DANE in de categorie HTTPS vallen, zal deze categorie nog steeds niet als geslaagd scoren. Als gevolg zal de score van de bedrijven die voor één categorie slagen voornamelijk bepaald worden door het wel of niet slagen voor de categorie DNSSEC, die maar uit twee onderliggende subtesten bestaat.

Testen per subgroep voor bedrijven met drie of vier geslaagde categorieën

Voor bedrijven die voor drie categorieën slagen is te zien dat voornamelijk Beveiligingsopties (APPSEC) een grote sprong maakt van gemiddeld 22 procent naar 58 procent. De subgroep DANE (uit de categorie HTTPS) begint net op te komen met slechts een gemiddelde van 4 procent van de testen die slagen uit deze categorie.

Ten slotte bereiken de subgroepen HTTPS/cert, IPv6 en DNSSEC de gemiddelde score van 100 procent voor bedrijven die voor alle categorieën slagen. De subgroepscore van *DANE* blijft rond de 10 procent hangen, wat impliceert dat deze subgroep niet essentieel is om een eindscore van 100 procent te halen (alle bedrijven met vier geslaagde categorieën hebben een eindscore van 100 procent).

Testen per subgroep voor bedrijven geconditioneerd per eindscorecategorie

In voorgaande paragrafen is aan de hand van figuur 3.4.2a de subgroepscore geconditioneerd naar het aantal geslaagde categorieën besproken. Hoe de eindscores per aantal geslaagde categorieën verdeeld zijn, is in figuur 3.4.2b terug te vinden. Deze manier van analyseren heeft het nadeel dat de eindscores voor de verschillende categorieën toch wat overlap vertonen. Daarom worden de gemiddelde subgroepscores ook geconditioneerd naar eindscorecategorieën die gegeven worden aan de hand van eindscore-intervallen: bedrijven

3.4.1 Overzicht van de vier eindscorecategorieën.

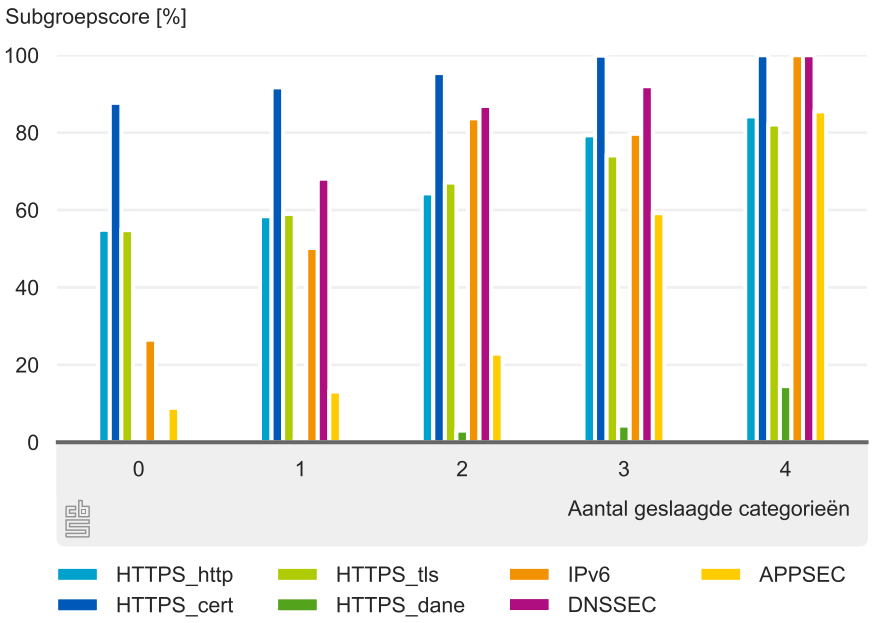
Scorecategorie	Eindscores
Low	lager dan 40
Medium	40 tot 60
High	60 tot 80
Very High	hoger dan 80

met een eindscore lager dan 40 zitten in de eindscorecategorie *Low*; met een eindscore tussen de 40 en 60 zit je in de score categorie *Medium*, tussen de 60 en 80 in de scorecategorie *High* en met een eindscore boven de 80 val je in de eindscorecategorie *Very High*. Zie tabel 3.4.1 voor een overzicht van deze eindscorecategorieën. Merk op dat deze scorecategorieën ongeveer overeen komen met de pieken die in de scoreverdeling 3.3.2 zijn terug te vinden.

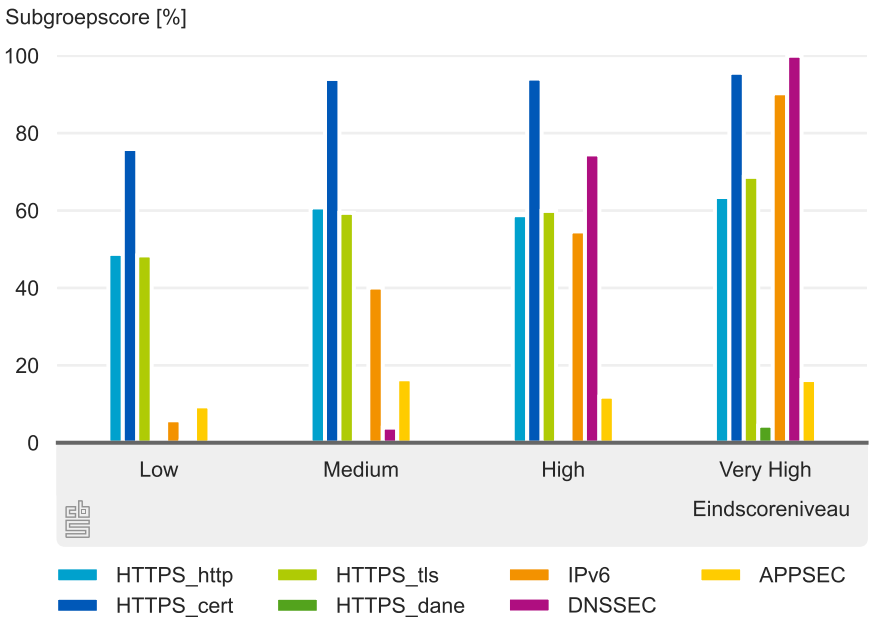
De subgroepscores per eindscore-interval in figuur 3.4.2b zijn gelijksoortig met de observaties die aan de hand van figuur 3.4.2a gedaan zijn. Voor lage en medium eindscores (categorieën *Low* en *Medium*, dus eindscores onder de 60 procent) halen de subgroepen *http*, *cert* en *tls* de hoogste subgroepscores. Voor de eindscore-categorie *High* komt dnssec ineens op, en domineert daarmee de groep bedrijven die de eerste geslaagde categorie halen.

3.4.2 Subgroepscore tegen het aantal geslaagde categorieën (a) en het eindscoreniveau (b).

(a) Subgroepscore tegen aantal geslaagde categorieën



(b) Subgroepscore tegen het eindscoreniveau



3.5 Kruiscorrelatie tussen de testcategorieën

Als laatste wordt hier nog gekeken welke testen met elkaar gecorreleerd zijn, dat wil zeggen, voor welke testen de uitkomsten onderling met elkaar samenhangen. De mate waarin variabelen met elkaar samenhangen wordt weergegeven met de correlatiematrix in figuur 3.5.1. De correlatiematrix toont de onderlinge paarsgewijze correlatiecoëfficiënten van alle testvariabelen die op de assen staan. De betekenis van alle variabelen op de assen kan terug gevonden worden in tabel A.2.1. In deze correlatiematrix worden de variabelen op de assen die bij één categorie/subgroep horen bij elkaar gezet. De kleur van de subgroeplabels komt overeen met de kleur zoals deze ook in tabel A.2.1 terug te vinden is, en zoals deze ook in figuur 3.4.2 voor de subgroepen gebruikt is.

Correlatiematrix

De correlatiematrix zet de paarsgewijze correlatiecoëfficiënten van alle testen van een Internet.nl scan tegen elkaar uit. Een correlatiecoëfficiënt tussen twee testen kan waardes innemen tussen -1 (als de ene test slaagt, slaagt de andere per definitie niet) en +1 (als de ene test slaagt, slaagt de andere per definitie ook) en alle waardes daartussen. Een correlatiecoëfficiënt van 0 geeft aan dat er geen samenhang tussen twee testen is: de uitkomst van bij testen zal onafhankelijk van elkaar zijn. Let wel: het gaat bij correlatiecoëfficiënten om *verwachtingswaarden*, dus voor een individueel bedrijf kan bij een correlatiecoëfficiënt van 0 voor twee testen A en B best beide keren slagen, maar *gemiddeld genomen* zal bij een correlatiecoëfficiënt van nul, B even vaak niet slagen als wel slagen als A geslaagd is. De diagonaal van een correlatiematrix geeft de samenhang van een testuitkomst met zichzelf weer en zal dus per definitie 1 zijn. Verder is een correlatiematrix symmetrisch over de diagonaal, omdat de samenhang tussen twee paarsgewijze variabelen niet door de volgorde bepaald wordt: de samenhang tussen variabele A en variabele B is per definitie gelijk aan de samenhang van variabele B met variabele A.

In de correlatiematrix is te zien dat uitkomsten van testen uit dezelfde subgroep vaak samenhangen, wat wil zeggen dat onderlinge variabelen een correlatiecoëfficiënt groter dan 0 hebben (voor een behoorlijke positieve correlatie zou je een correlatiecoëfficiënt tussen de 0,5 en 1 kunnen aannemen; negatieve correlaties met waardes tussen de -1 en -0,5 zijn theoretisch mogelijk, maar worden in dit onderzoek niet gevonden). Zo is te zien dat bijvoorbeeld de paarsgewijze correlatiecoëfficiënten van de testen uit de subgroep *cert*, onderdeel van de categorie *HTTPS*, allemaal een waarde van groter dan 0,5 hebben. Dit is niet heel verrassend: zodra een bedrijf investeert om een certificaat aan te vragen zullen gemiddeld genomen alle testen die met het certificaat samenhangen vaker slagen en andersom: als een bedrijf geen certificaat heeft zullen alle testen die met het certificaat samengaan ook niet slagen. Het is echter nog steeds mogelijk dat een bedrijf wel een certificaat heeft met een publieke sleutel van het certificaat (tests_web_https_cert_pubkey_verdict is geslaagd) maar bijvoorbeeld niet slaagt voor de test of het bedrijf een vertrouwensketen voor het certificaat heeft (tests_web_https_cert_chain_verdict). De verdeling van het gemiddelde slagingspercentages per bedrijfsgrootteklasse en bedrijfstak van beide testen wordt in figuren B.1.22 en B.1.23 gegeven. Hierin is inderdaad af te lezen dat beide verdelingen bijna overeenkomen, maar dat de verdeling van de gemiddelde slagingspercentages van de vertrouwensketens iets onder de uitkomsten van de test naar de publieke sleutel van het

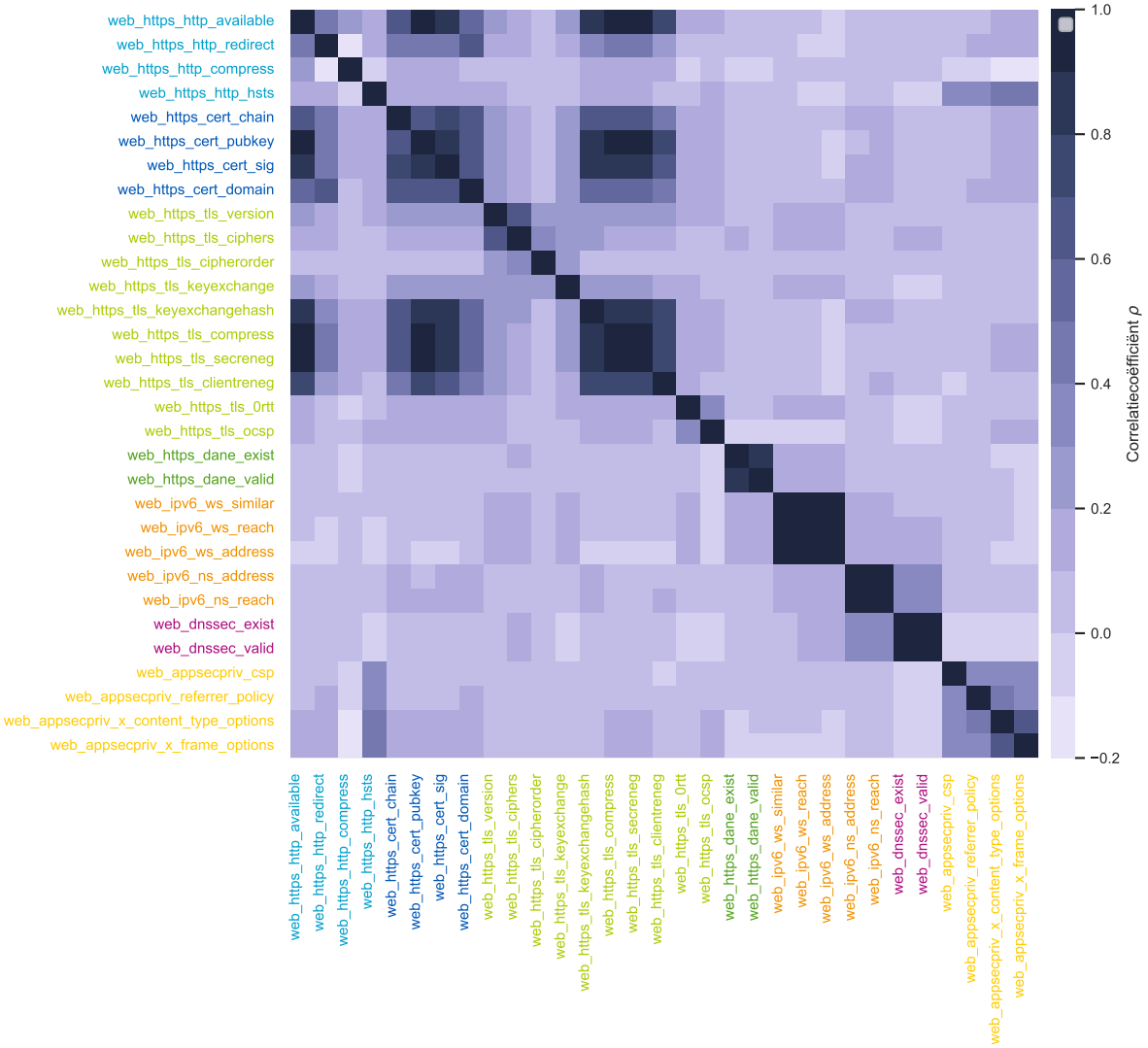
certificaat ligt.

Op dezelfde manier is te zien dat de testen van de subgroep *dane* (uit de categorie *HTTPS*) met een correlatiecoëfficiënt tussen de testvariabelen tests_web_https_dane_exist_verdict en tests_web_https_dane_valid_verdict van 0,82 sterk met elkaar samenhangen. De verdelingsfuncties met de gemiddelde slagingspercentages in figuren B.1.26 en figuren B.1.27 en zijn weer erg gelijkvormig verdeeld over de bedrijfsgrootteklassen en bedrijfstakken. De slagingspercentages van de test of DANE bestaat liggen allemaal iets boven de test of DANE ook geldig is, wat natuurlijk het gevolg is van het feit dat de tweede test alleen kan slagen als de eerste test ook geslaagd is. Opvallend is dat het slagingspercentage van beide testen voor de bedrijfstak met het hoogste gebruik van DANE, namelijk de Horeca, aan elkaar gelijk is. Dit impliceert dat de Horeca niet alleen relatief vaak DANE gebruikt (nog steeds nog maar 3,8 procent van de bedrijven), maar ook in alle gevallen zorgt voor een valide DANE-gebruik.

In de subgroep *ipv6* is te zien dat er wel een sterke correlatie is tussen de variabelen voor een IPv6 voor een *webserver* (als bedrijven een IPv6 voor een webserver hebben dan slagen ze vaak ook voor de bereikbaarheid van de IPv6 webserver en slagen ze ook relatief vaak gelijk voor een website op IPv6 en IPv4) en de variabelen voor IPv6 voor een *nameserver*, maar dat de variabelen voor de IPv6 *webserver* en *nameserver* weer (bijna) ongecorreleerd zijn.

Ten slotte is te zien dat er ook een samenhang kan bestaan tussen testen uit verschillende subgroepen. Er was al aangetoond dat de testen van de subgroep *cert* (uit de categorie *HTTPS*) onderling gecorreleerd zijn, maar uit figuur 3.5.1 is ook op te maken dat er een correlatie bestaat tussen de testen uit deze subgroep met een aantal variabelen uit de subgroep *tls*, namelijk te testen voor TLS met een hashfunctie voor sleuteluitwisseling (*web_https_tls_keyexchangehash*, zie ook figuur B.1.16), TLS zonder compressiemogelijkheid (*web_https_tls_compress*, zie ook figuur B.1.17), TLS met (*web_https_tls_secreneg*, zie ook figuur B.1.18) en (*web_https_tls_clientreneg* , zie ook figuur B.1.19).

3.5.1 Correlatiematrix met als elementen de paarsgewijze correlatiecoëfficiënten van de verschillende testonderdelen van internet.nl.



4.
Conclusies

In dit onderzoek is in samenwerking met Internet.nl een analyse gemaakt van de veiligheid van websites van Nederlands bedrijven. Hiertoe is voor zo'n 12 duizend bedrijven een scan van de website van het bedrijf gemaakt met de website Internet.nl. Doordat de 12 duizend bedrijven voorkomen in een representatieve steekproef kunnen uitspraken gedaan worden over de veiligheid van websites van Nederlands bedrijven in het algemeen. Internet.nl kent per domeinnaam een eindscore tussen de 0 en 100 procent toe. Dat wordt gedaan aan de hand van testen die onder te verdelen zijn in vier verschillende categorieën: HTTPS, IPv6, DNSSec en beveiligingsopties. Geconcludeerd kan worden dat

- de gemiddelde eindscore van bedrijven in Nederland per bedrijfsgrootte en bedrijfstak vrij constant is en ligt rond de 60 procent;
- kleine bedrijven beter scoren op de categorieën IPv6 en DNSSEC, grote bedrijven beter scoren op de categorieën HTTPS en beveiligingsopties;
- de verdeling van de eindscores voor alle bedrijven laat zien dat er behoorlijke verschillen zijn tussen domeinnamen onderling; en
- de verdeling van eindscores 4 pieken vertoont die gerelateerd zijn aan het aantal categorieën waarvoor een bedrijf geslaagd is.

Bibliografie

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

CBS (2020b). Cybersecuritymonitor 2020.

CBS (2021). Python code internet.nl scan tool.

Platform Internetstandaarden (2021). Internet.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 Overzicht kenmerken scan Internet.nl

A.2.1 Vier categorieën met de subtesten

Categorie	Subgroep	Testomschrijving	Testuitkomsten	Variabelenaam
HTTPS	https	HTTPS beschikbaar	*good/bad/other*	tests_web_https_http_available_verdict
		HTTPS-doorverwijzing	*good/bad/other/not tested*	tests_web_https_http_redirect_verdict
		HTTPS-compressie	*good/bad/not tested*	tests_web_https_http_compress_verdict
		HSTS aangeboden	*good/bad/other/not tested*	tests_web_https_http_hsts_verdict
	cert	Vertrouwensketen van certificaat	*good/bad/not tested*	tests_web_https_cert_chain_verdict
		Publieke sleutel van certificaat	*good/bad/not tested*	tests_web_https_cert_pubkey_verdict
		Handtekening van certificaat	*good/bad/not tested*	tests_web_https_cert_sig_verdict
		Domeinnaam op certificaat	*good/bad/not tested*	tests_web_https_cert_domain_verdict
	tls	TLS Versie	*good/bad/phase out/not tested*	tests_web_https_tls_version_verdict
		TLS ciphers	*good/bad/phase out/not tested*	tests_web_https_tls_ciphers_verdict
		TLS cipher-volgorde	*good/bad/other/not tested*	tests_web_https_tls_cipherorder_verdict
		TLS sleuteluitwisselingsparameters	*good/bad/phase out/not tested*	tests_web_https_tls_keyexchange_verdict
		Hashfunctie voor sleuteluitwisseling	*good/bad/phase out/not tested*	tests_web_https_tls_keyexchangehash_verdict
		TLS-compressie	*good/bad/not tested*	tests_web_https_tls_compress_verdict
		Secure renegotiation	*good/bad/not tested*	tests_web_https_tls_secreneg_verdict
		Client initiated renegotiation	*good/bad/not tested*	tests_web_https_tls_clientreneg_verdict
		0-RTT	*good/bad/N.A./not tested*	tests_web_https_tls_0rtt_verdict
		TLS OCSP-stapeling	*good/ok/bad/not tested*	tests_web_https_tls_ocsp_verdict
	dane	DANE aanwezig	*good/bad/not tested*	tests_web_https_dane_exist_verdict
		DANE geldigheid	*good/bad/not tested*	tests_web_https_dane_valid_verdict
IPv6	ipv6	IPv6-adressen voor *nameservers*	*good/bad/other*	tests_web_ipv6_ns_address_verdict
		IPv6-bereikbaarheid van *nameservers*	*good/bad/not tested*	tests_web_ipv6_ns_reach_verdict
		IPv6-adressen voor *webserver*	*good/bad*	tests_web_ipv6_ws_address_verdict
		IPv6-bereikbaarheid van *webservers*	*good/bad/not tested*	tests_web_ipv6_ws_reach_verdict
		Gelijke website op IPv6 en IPv4	*good/bad/not tested*	tests_web_ipv6_ws_similar_verdict
DNSSEC	dnssec	DNSSEC aanwezig	*good/bad/server failed*	tests_web_dnssec_exist_verdict
		DNSSEC geldigheid	*good/bad/not tested*	tests_web_dnssec_valid_verdict
Beveiligings-opties	appsec	*X-Frame-options*	*good/bad/phase out/not tested*	tests_web_appsecpriv_x_frame_options_verdict
		X-Content-Type-Options	*good/bad/phase out/not tested*	tests_web_appsecpriv_x_content_type_options_verdict
		Content-Security-Policy	*good/bad/not tested*	tests_web_appsecpriv_csp_verdict
		Referrer-Policy aanwezig	*good/bad/not tested*	tests_web_appsecpriv_referrer_policy_verdict

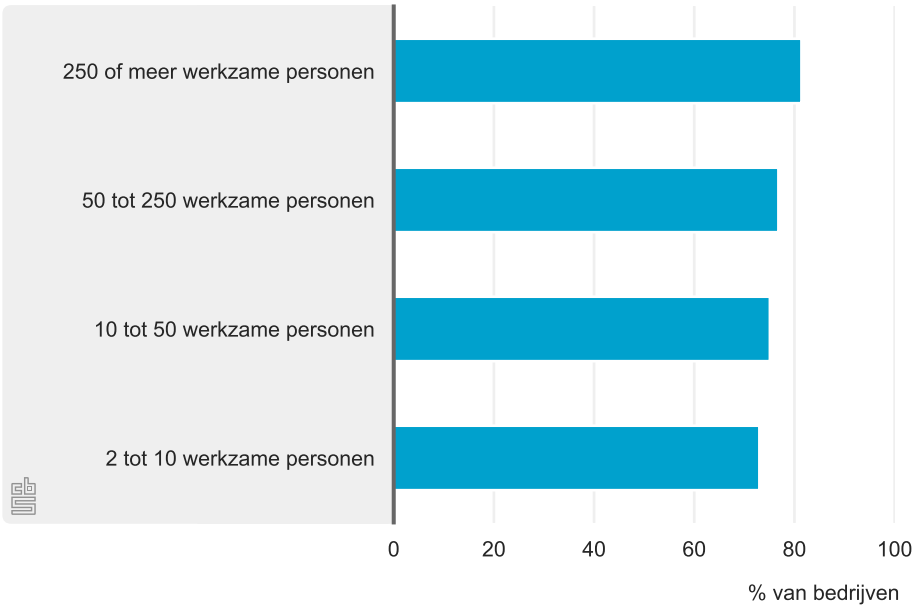
Bijlage B

Overzicht van alle kenmerken

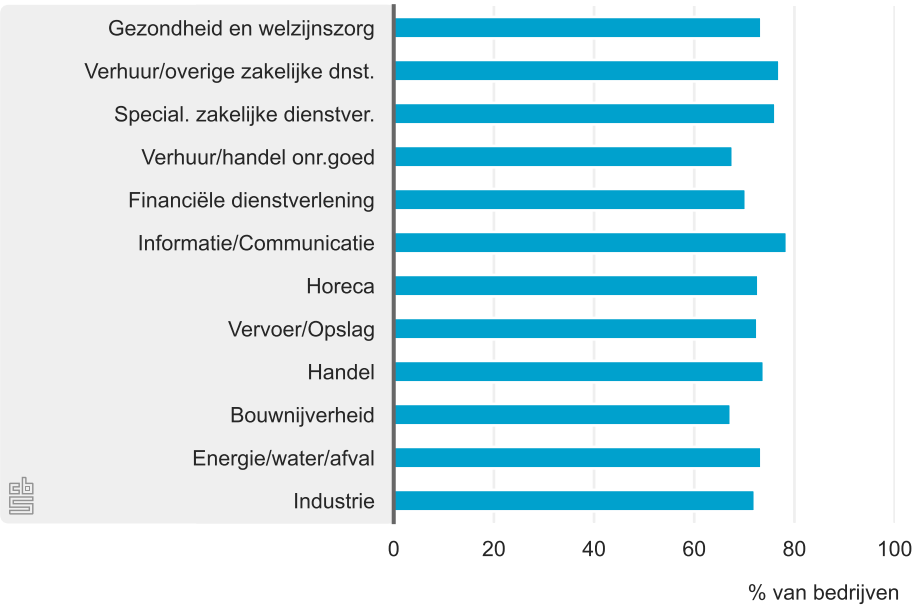
B.1 Figurenlijst

B.1.1 Categorie IPv6: percentage bedrijven met geslaagde test 'IPv6-adressen voor nameservers' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse

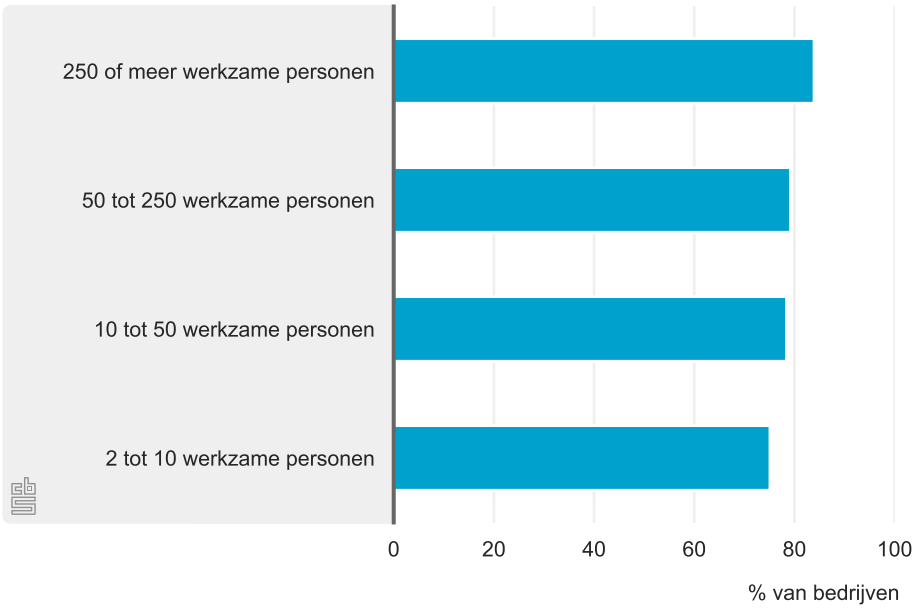


(b) Bedrijfstak

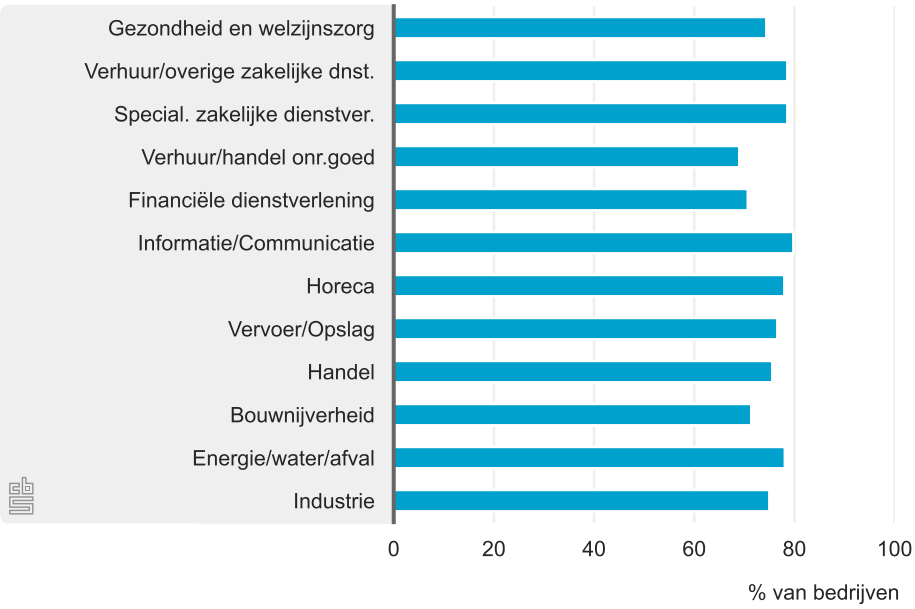


B.1.2 Categorie IPv6: percentage bedrijven met geslaagde test 'IPv6-bereikbaarheid van nameservers' per bedrijfsgrootteklasse (a) en bedrijfstak (b)

(a) Bedrijfsgrootteklasse

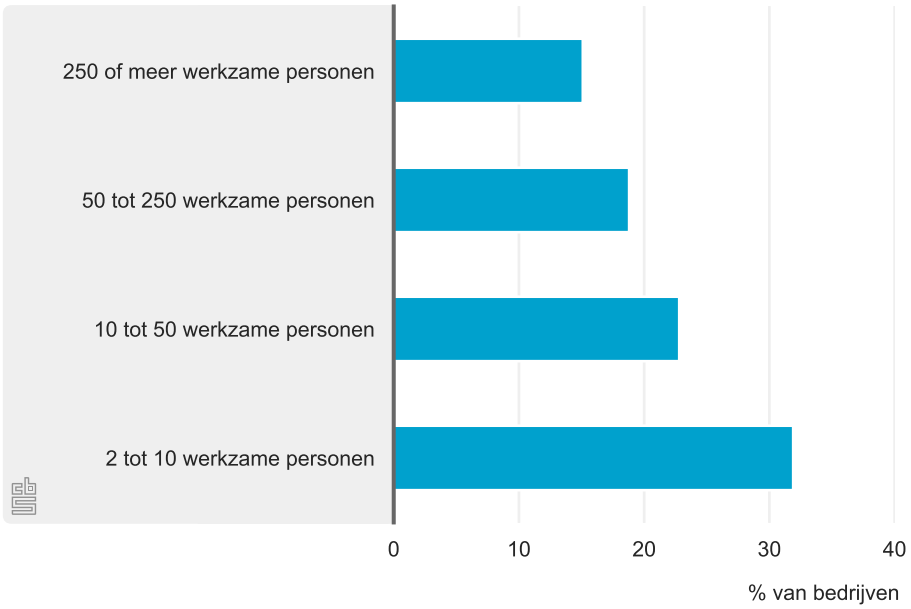


(b) Bedrijfstak

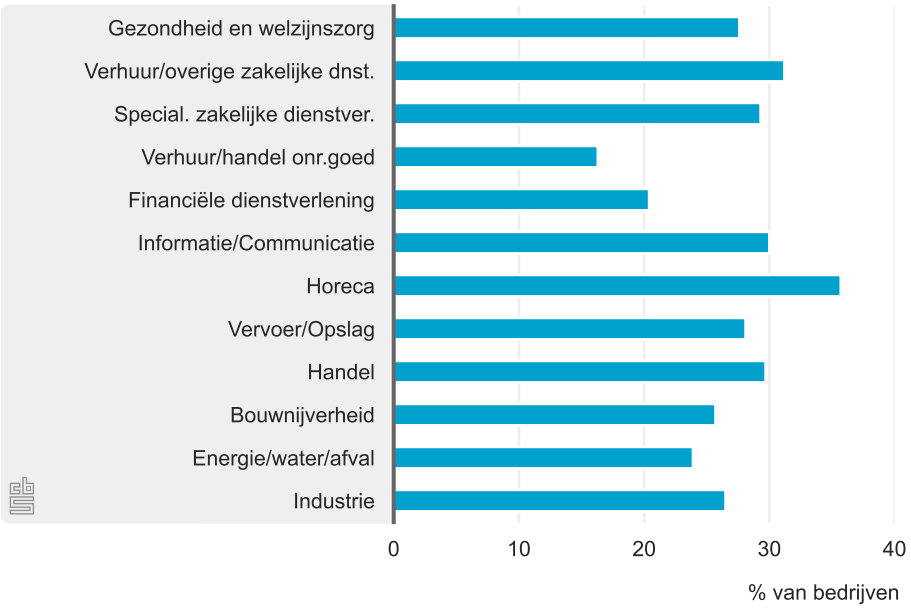


B.1.3 Categorie IPv6: percentage bedrijven met geslaagde test 'IPv6-adressen voor webserver' per bedrijfsgrootteklasse (a) en bedrijfstak (b)

(a) Bedrijfsgrootteklasse

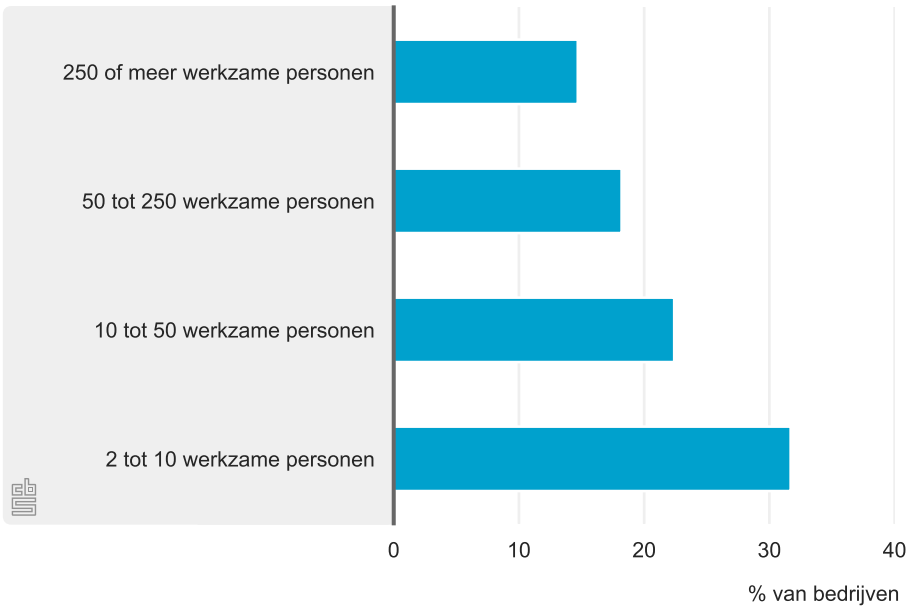


(b) Bedrijfstak

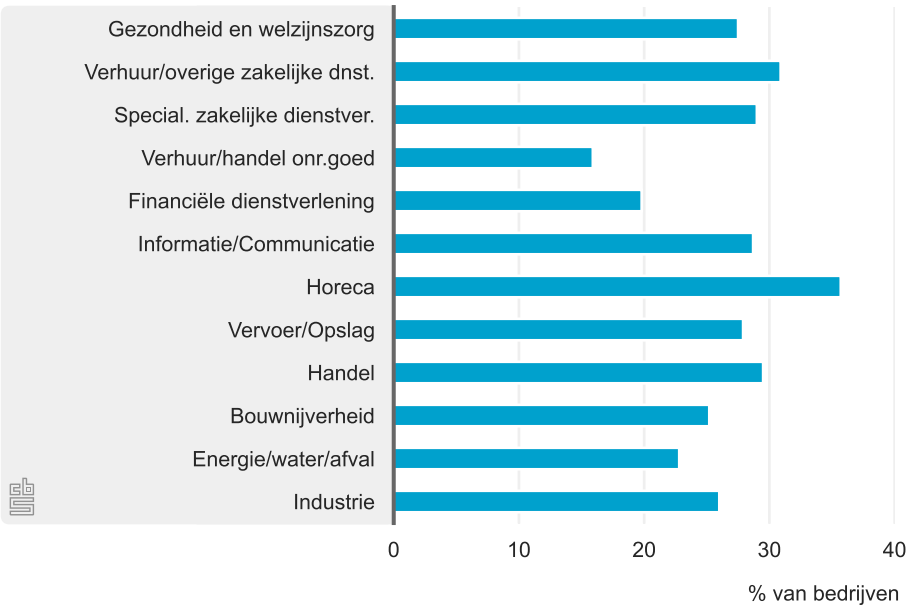


B.1.4 Categorie IPv6: percentage bedrijven met geslaagde test 'IPv6-bereikbaarheid van webservers per bedrijfsgrootteklasse (a) en bedrijfstak (b)

(a) Bedrijfsgrootteklasse

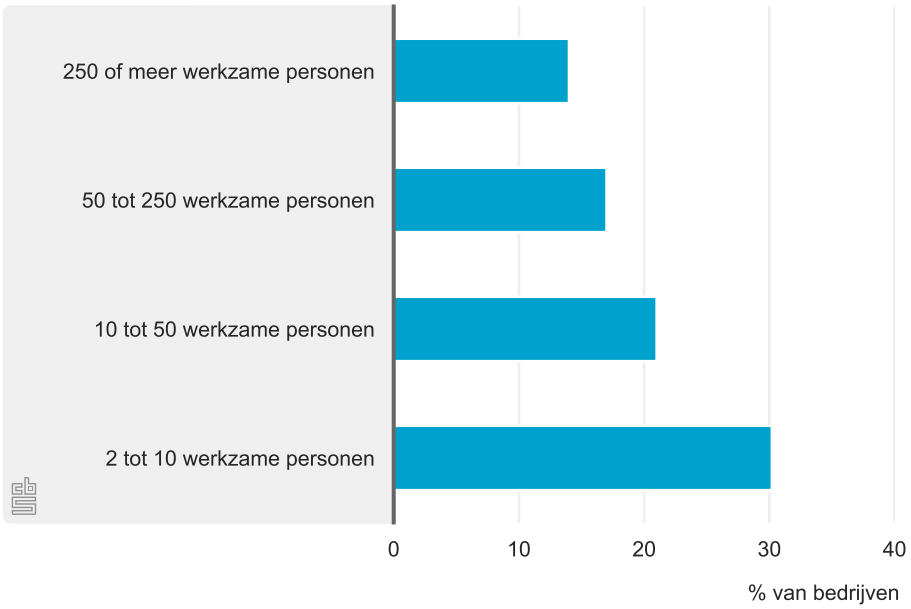


(b) Bedrijfstak

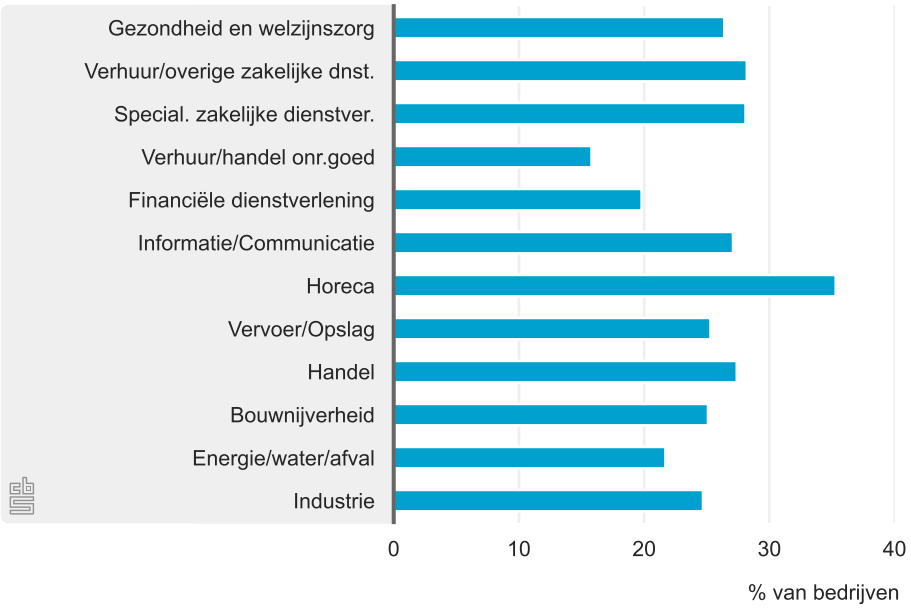


B.1.5 Categorie IPv6: percentage bedrijven met geslaagde test 'Gelijke website op IPv6 en IPv4' per bedrijfsgrootteklasse (a) en bedrijfstak (b)

(a) Bedrijfsgrootteklasse

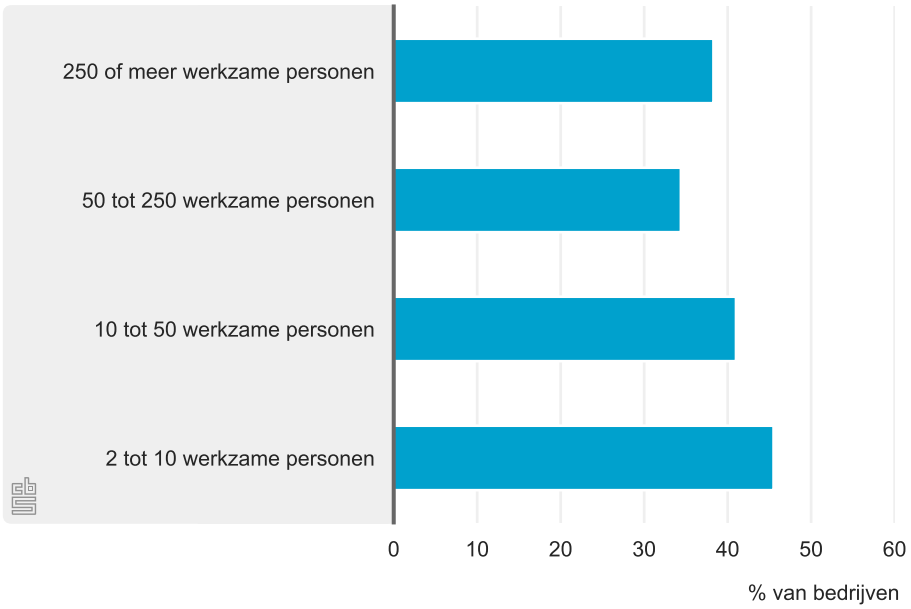


(b) Bedrijfstak

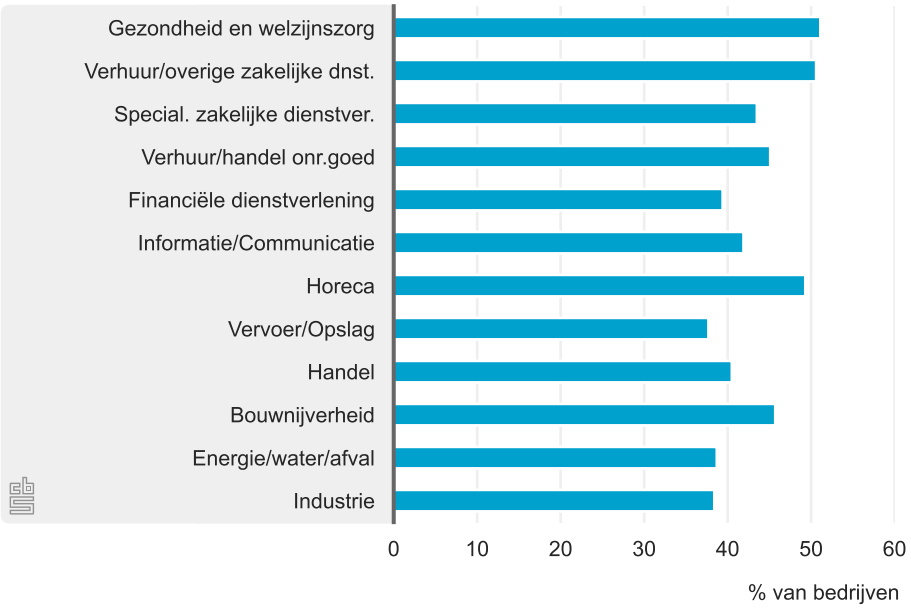


B.1.6 Categorie DNSSEC: percentage bedrijven met geslaagde test 'DNSSEC aanwezig' per bedrijfsgrootteklasse (a) en bedrijfstak (b)

(a) Bedrijfsgrootteklasse

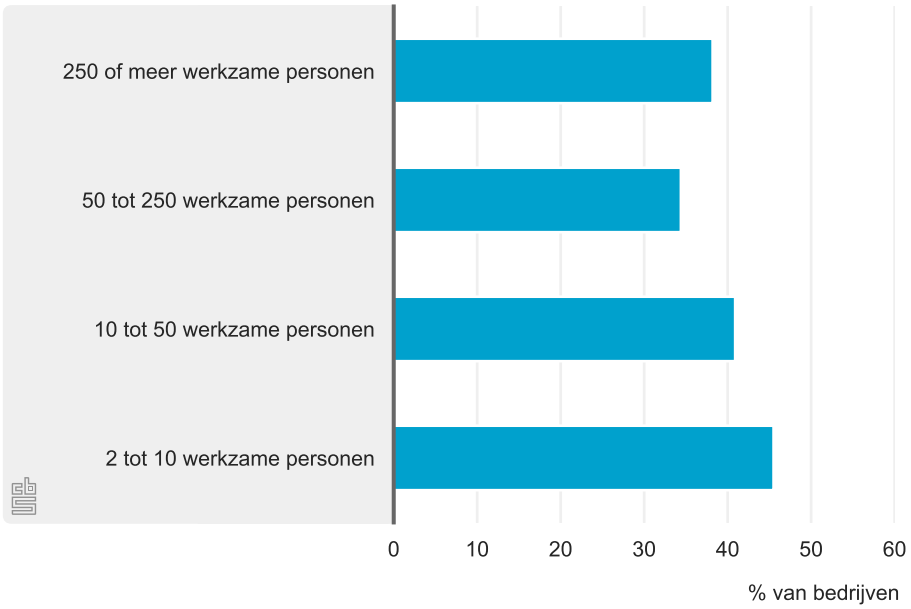


(b) Bedrijfstak

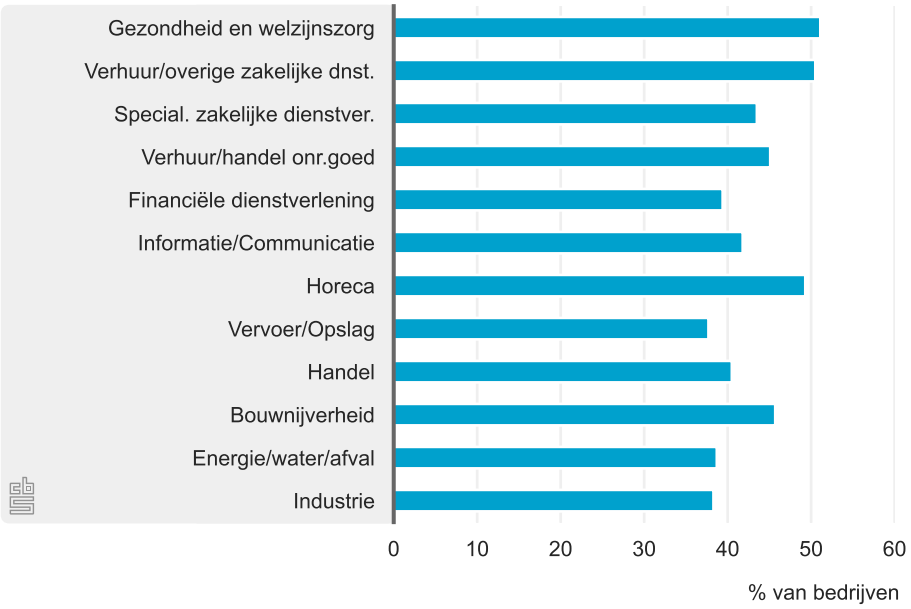


B.1.7 Categorie DNSSEC: percentage bedrijven met geslaagde test 'DNSSEC geldigheid' per bedrijfsgrootteklasse (a) en bedrijfstak (b)

(a) Bedrijfsgrootteklasse

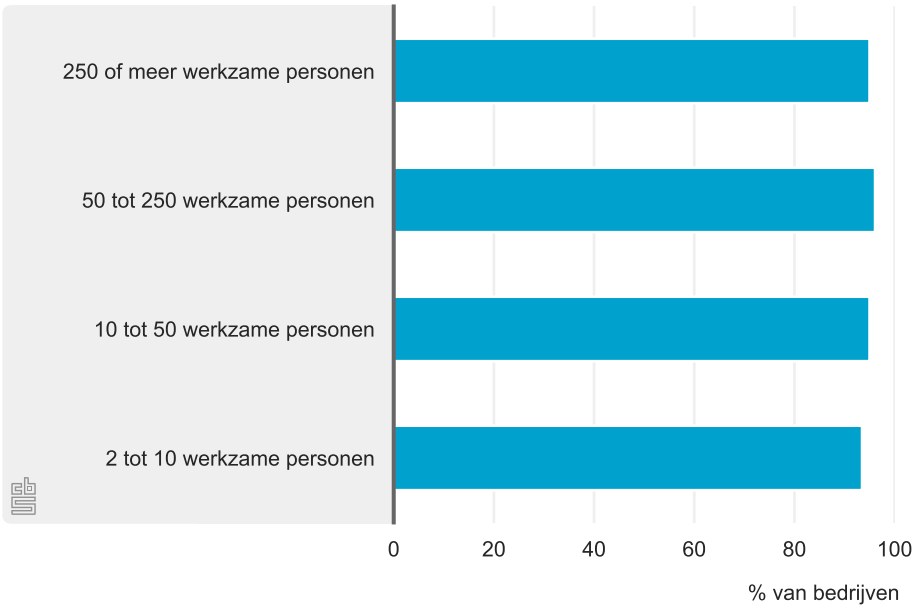


(b) Bedrijfstak

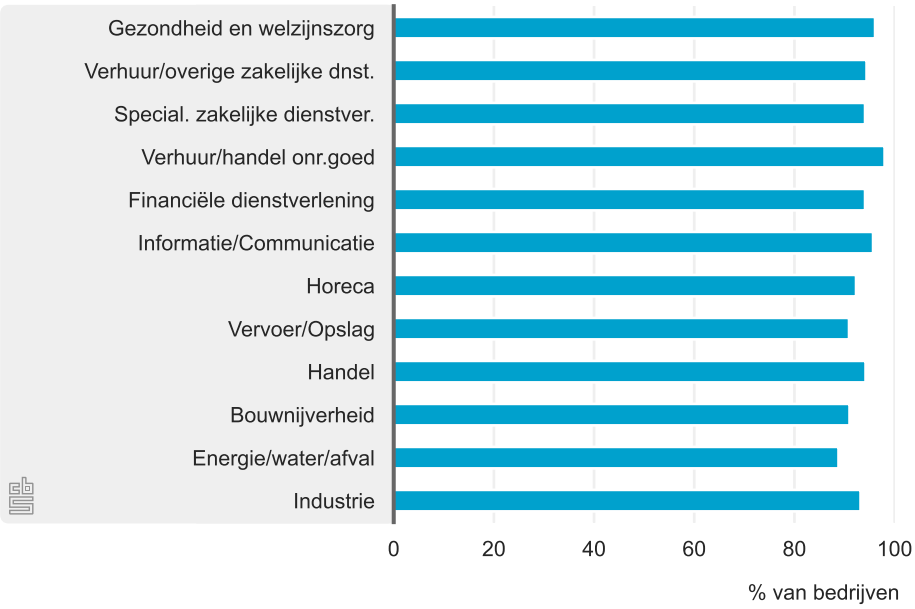


B.1.8 Categorie HTTPS: percentage bedrijven met geslaagde test 'HTTPS beschikbaar' per bedrijfsgrootteklasse (a) en bedrijfstak (b)

(a) Bedrijfsgrootteklasse

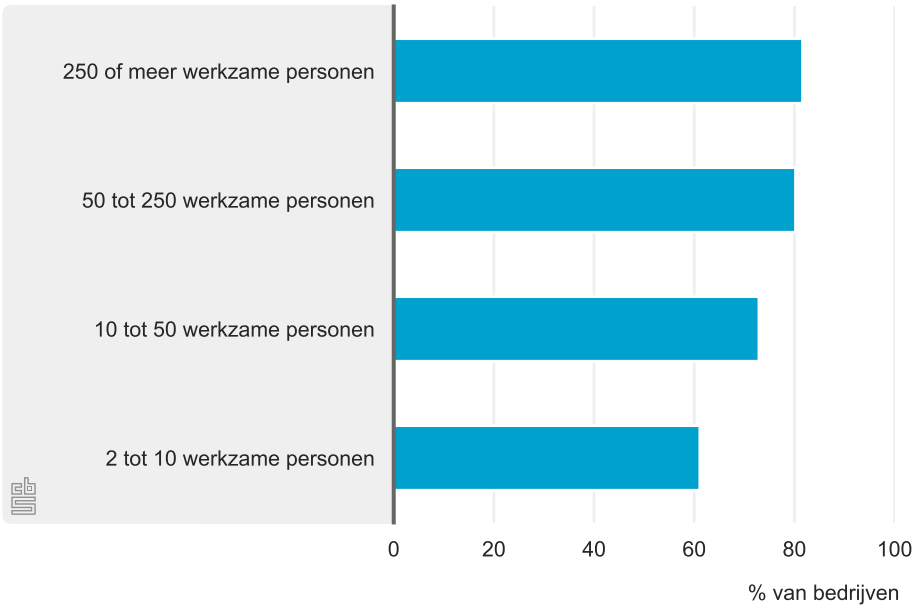


(b) Bedrijfstak

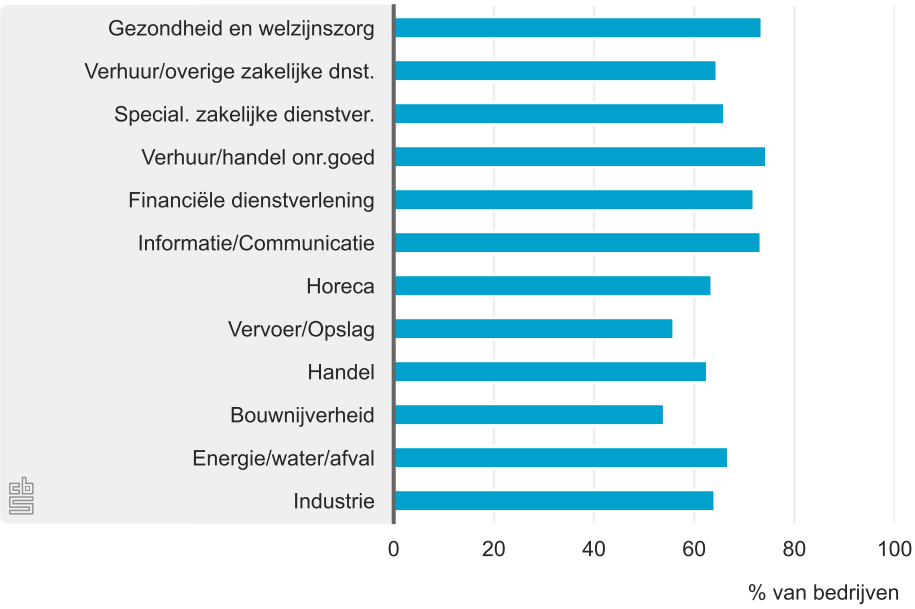


B.1.9 Categorie HTTPS: percentage bedrijven met geslaagde test 'HTTPS-doorverwijzing' per bedrijfsgrootteklasse (a) en bedrijfstak (b)

(a) Bedrijfsgrootteklasse

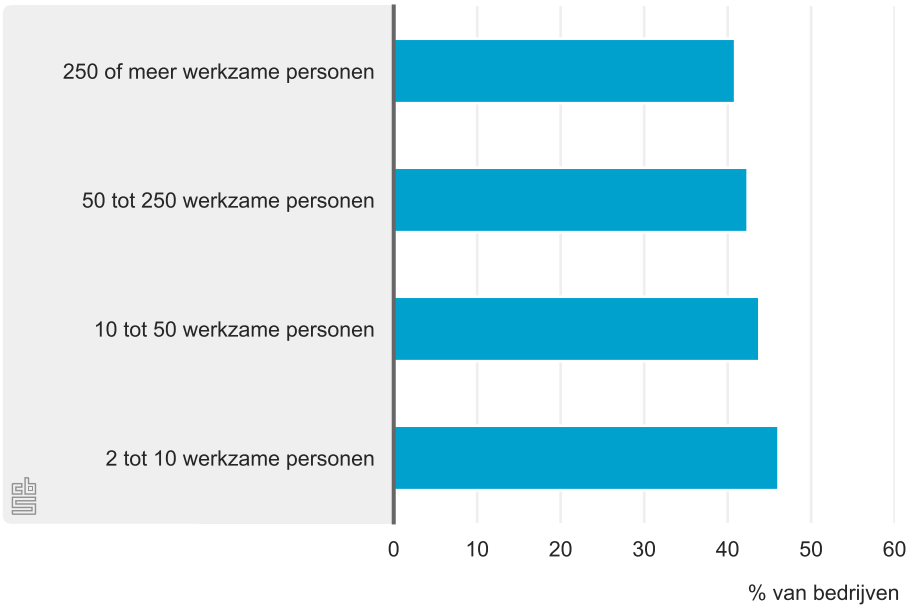


(b) Bedrijfstak

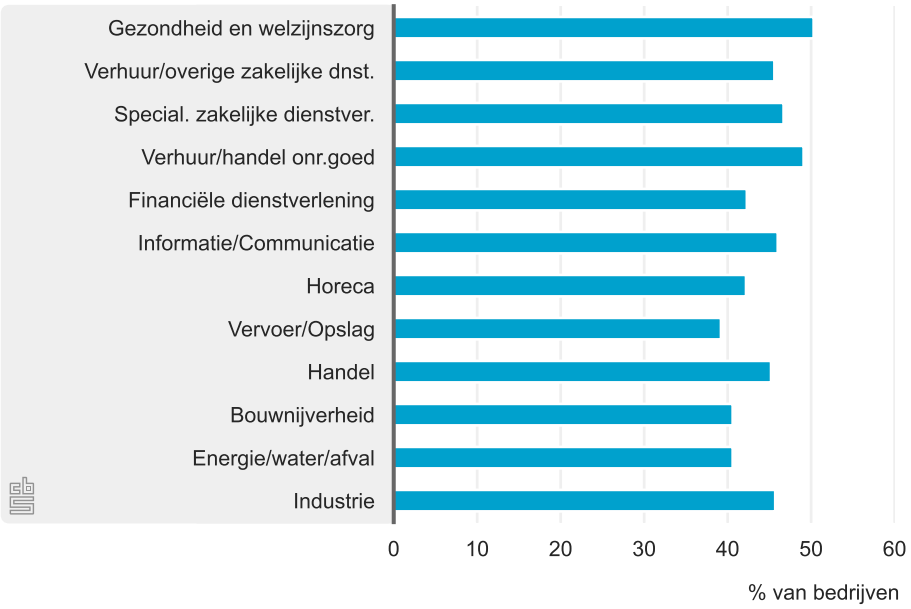


B.1.10 Categorie HTTPS: percentage bedrijven met geslaagde test 'HTTPS compressie niet ondersteund' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse

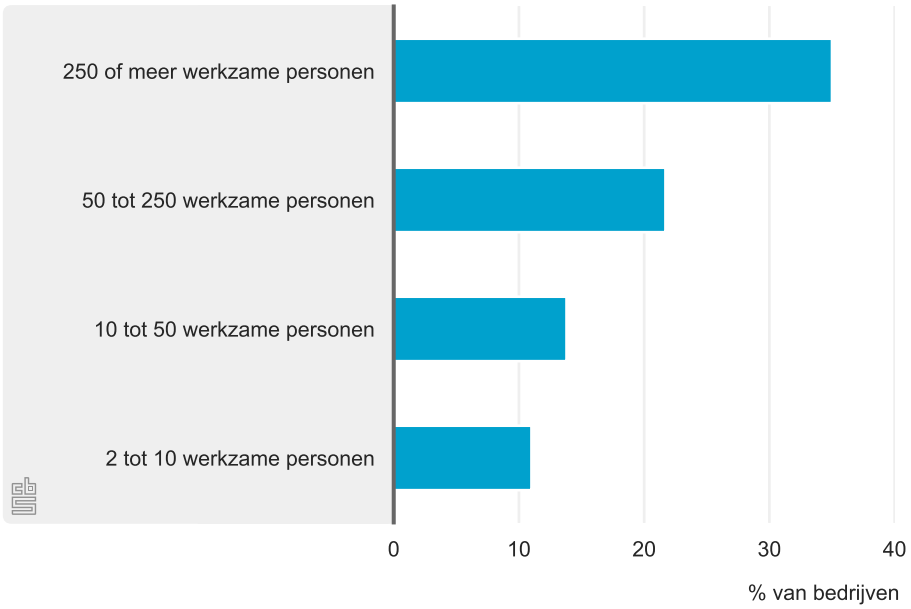


(b) Bedrijfstak

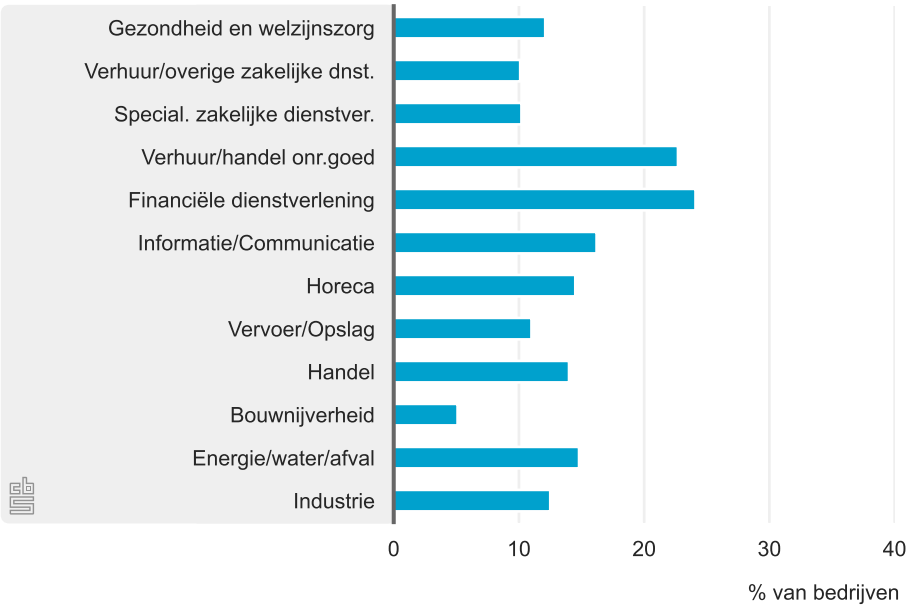


B.1.11 Categorie HTTPS: percentage bedrijven met geslaagde test 'HSTS policy aangeboden' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse

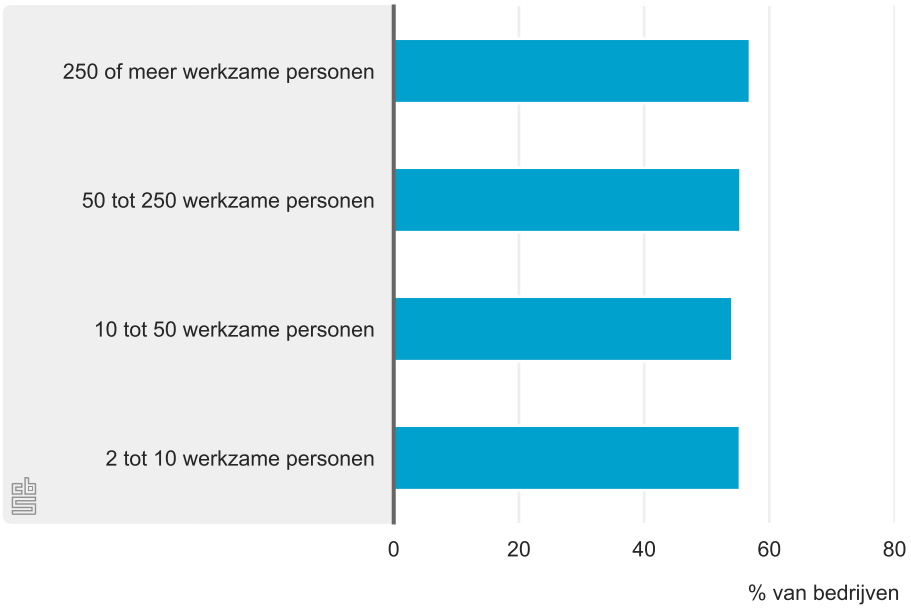


(b) Bedrijfstak

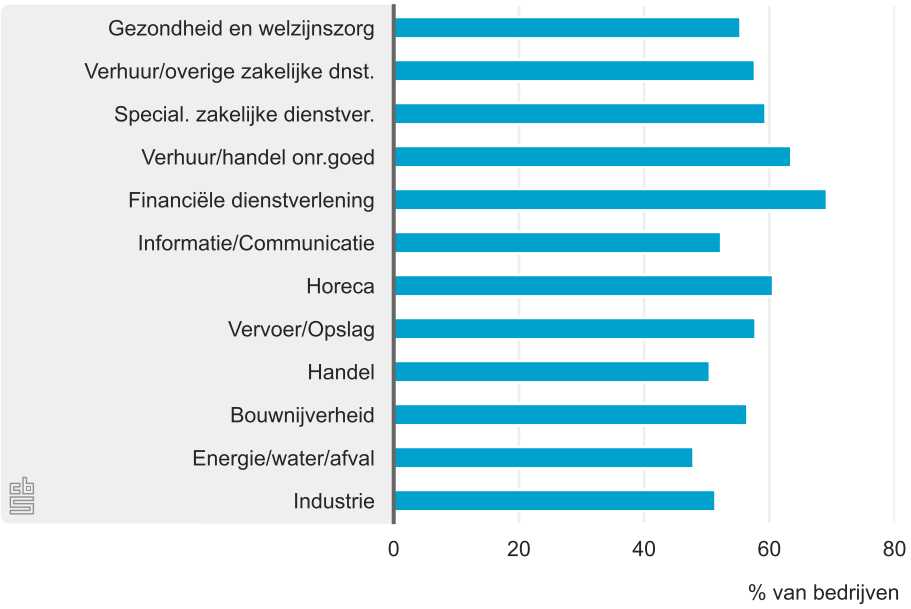


B.1.12 Categorie HTTPS: percentage bedrijven met geslaagde test 'TLS versie' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse

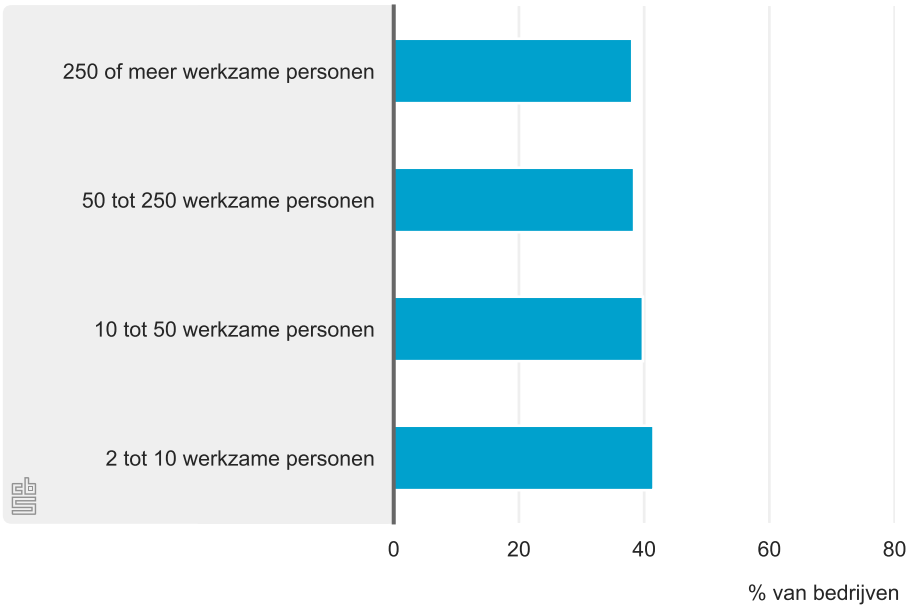


(b) Bedrijfstak

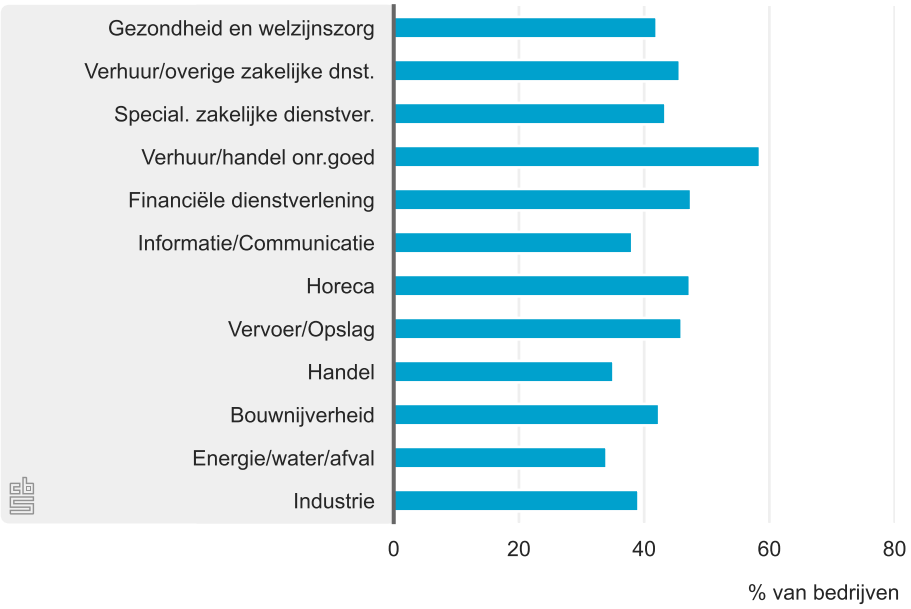


B.1.13 Categorie HTTPS: percentage bedrijven met geslaagde test 'TLS ciphers' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse

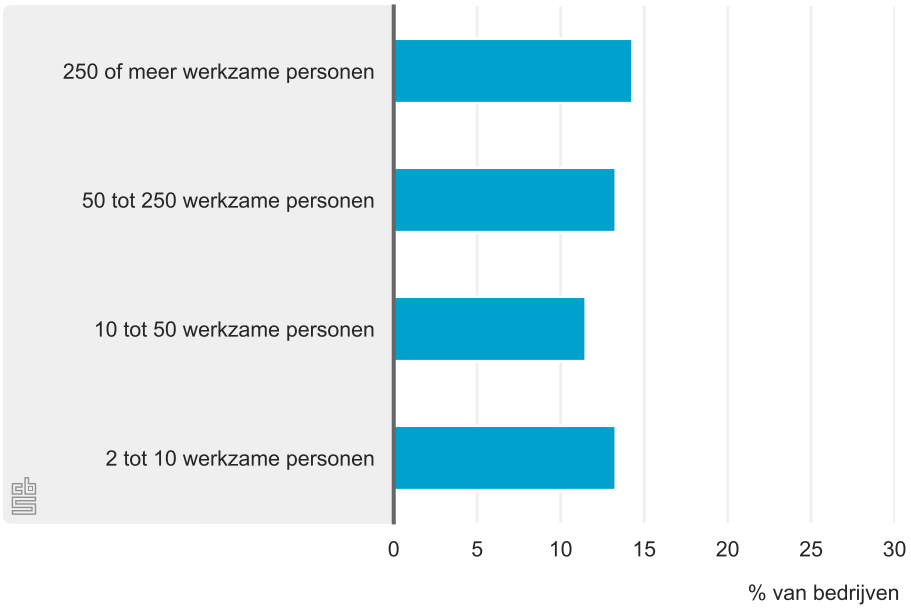


(b) Bedrijfstak

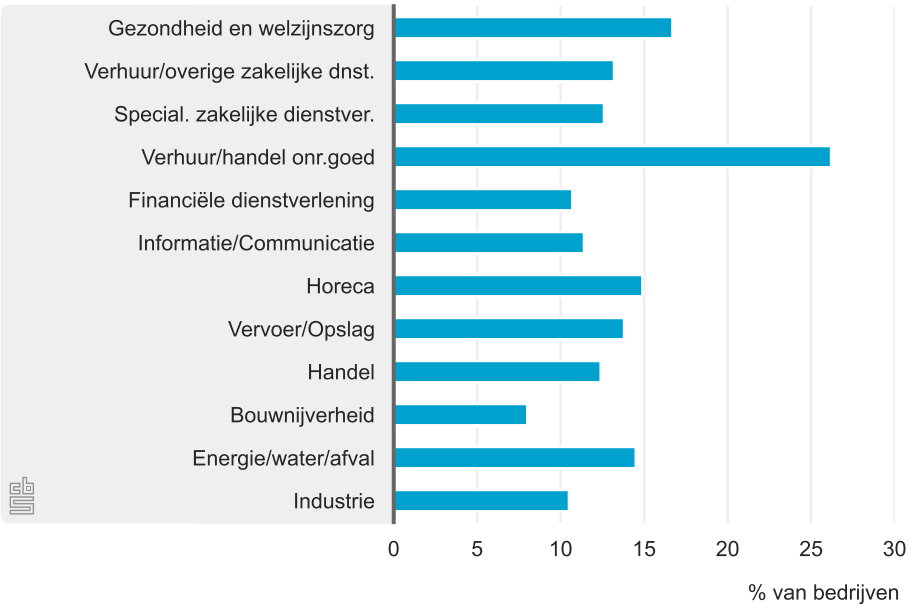


B.1.14 Categorie HTTPS: percentage bedrijven met geslaagde test 'TLS ciphers-volgorde' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse

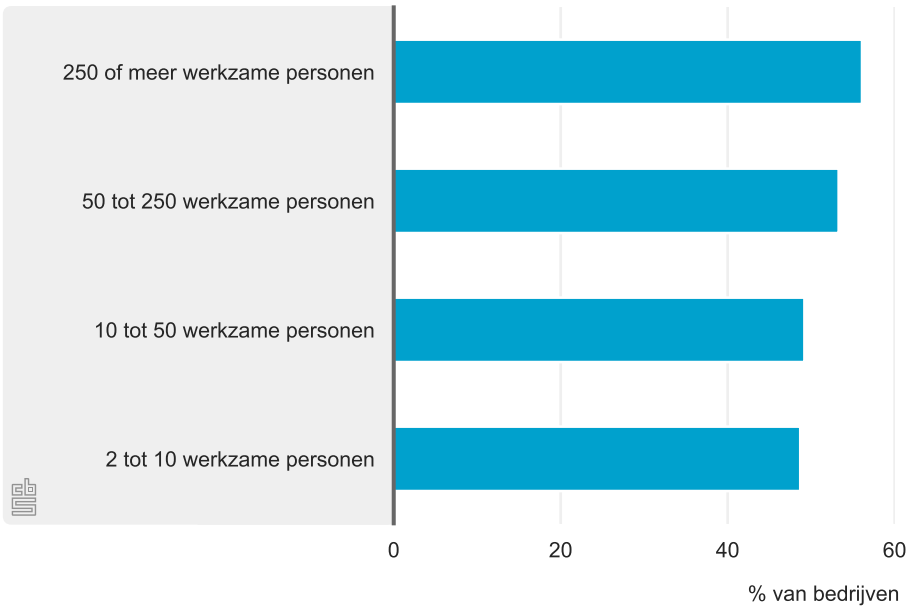


(b) Bedrijfstak

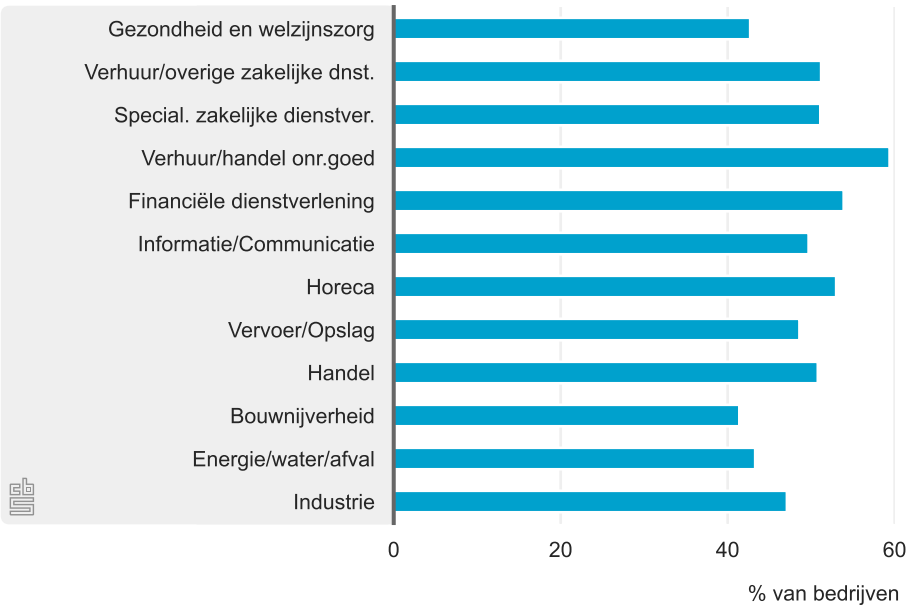


B.1.15 Categorie HTTPS: percentage bedrijven met geslaagde test 'TLS sleuteluitwisselingsparameters' per bedrijfsgrootteklasse (a) en bedrijfstak(b).

(a) Bedrijfsgrootteklasse

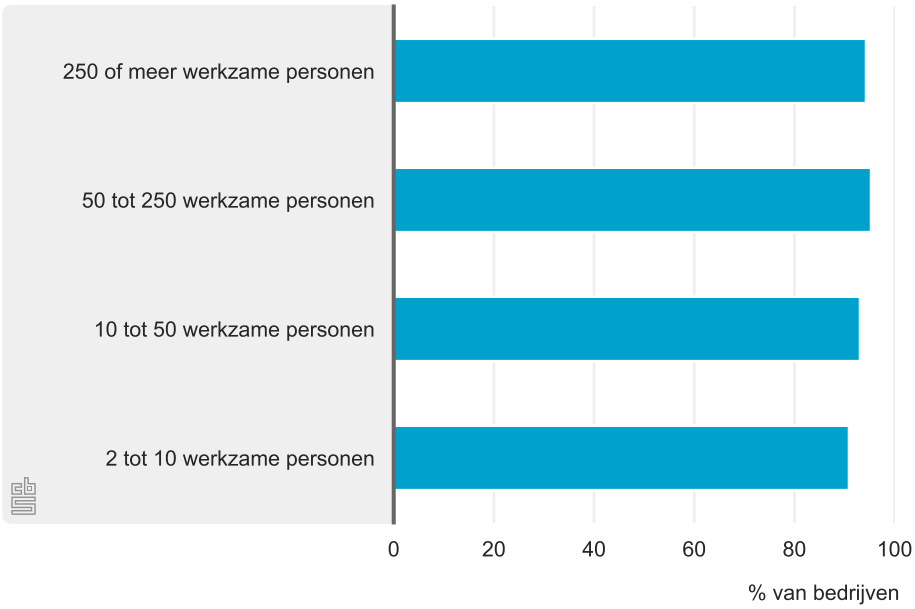


(b) Bedrijfstak

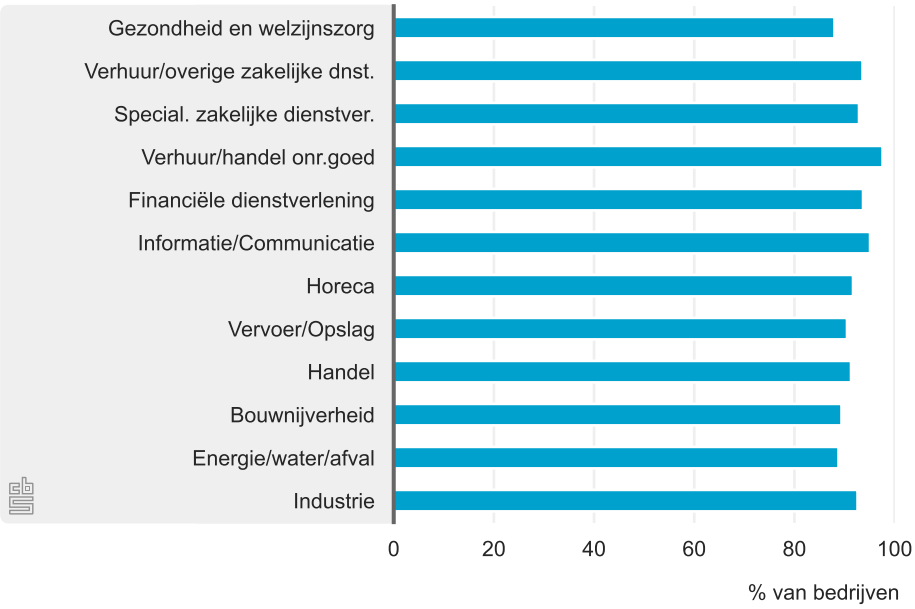


B.1.16 Categorie HTTPS: percentage bedrijven met geslaagde test 'Hashfunctie voor sleuteluitwisseling' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse

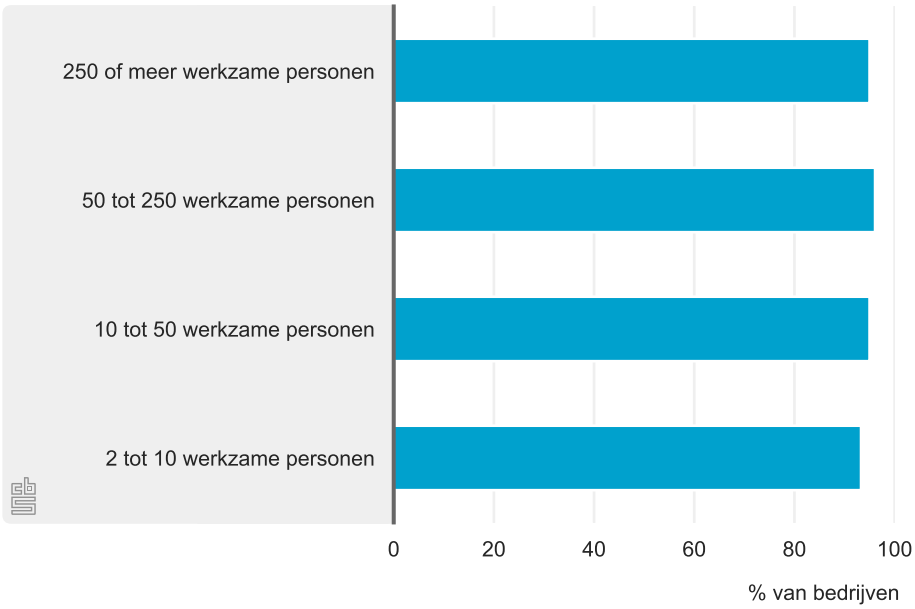


(b) Bedrijfstak

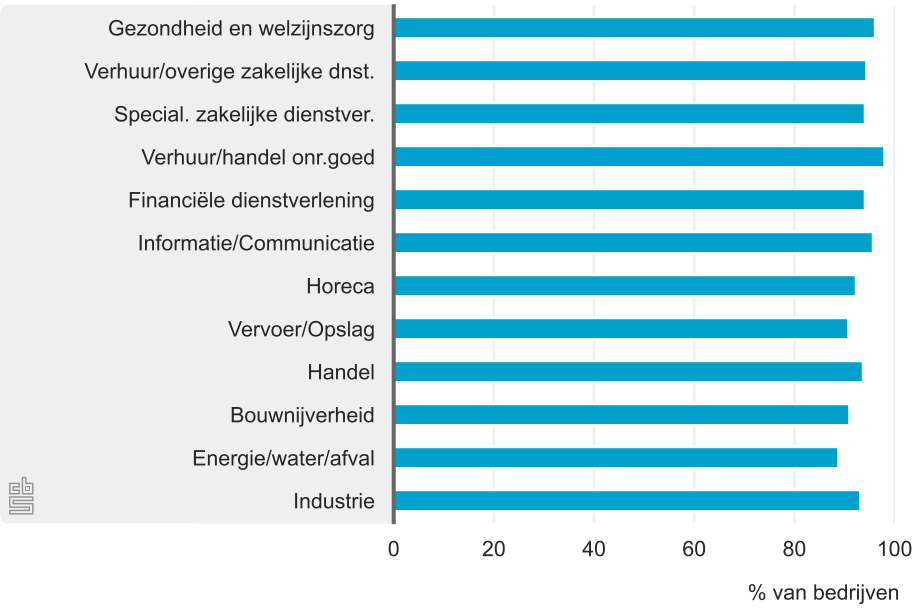


B.1.17 Categorie HTTPS: percentage bedrijven met geslaagde test 'TLS-compressie niet ondersteund' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse

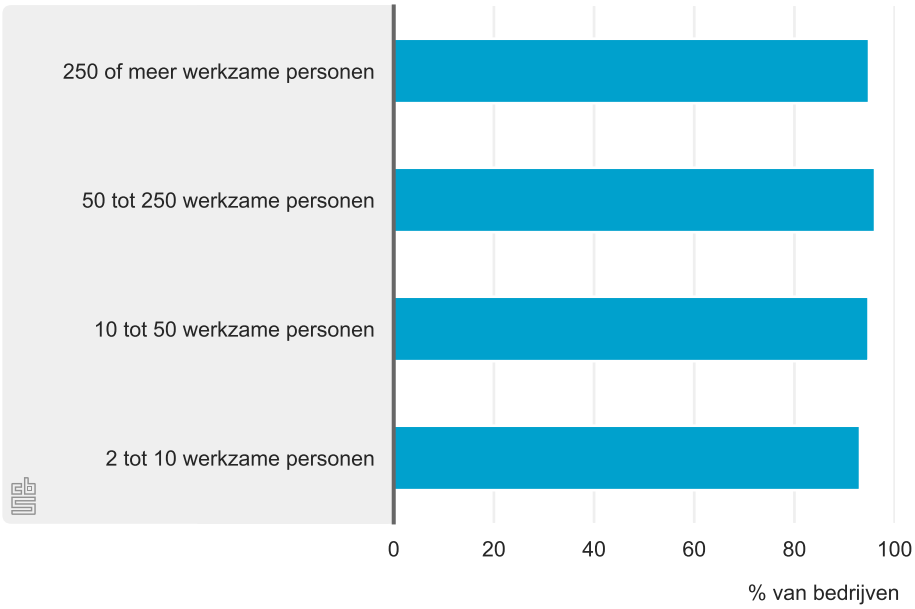


(b) Bedrijfstak

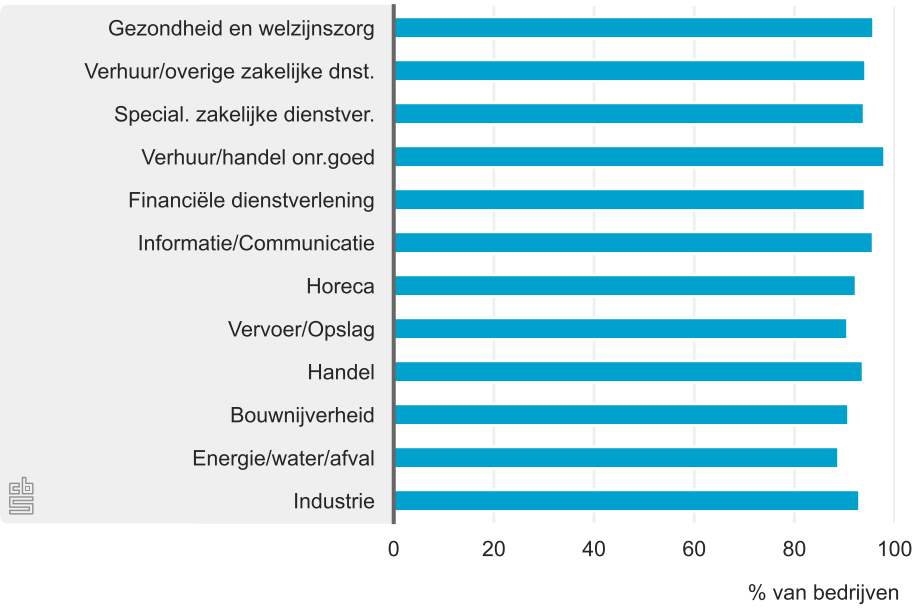


B.1.18 Categorie HTTPS: percentage bedrijven met geslaagde test 'TLS secure renegotiation' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse

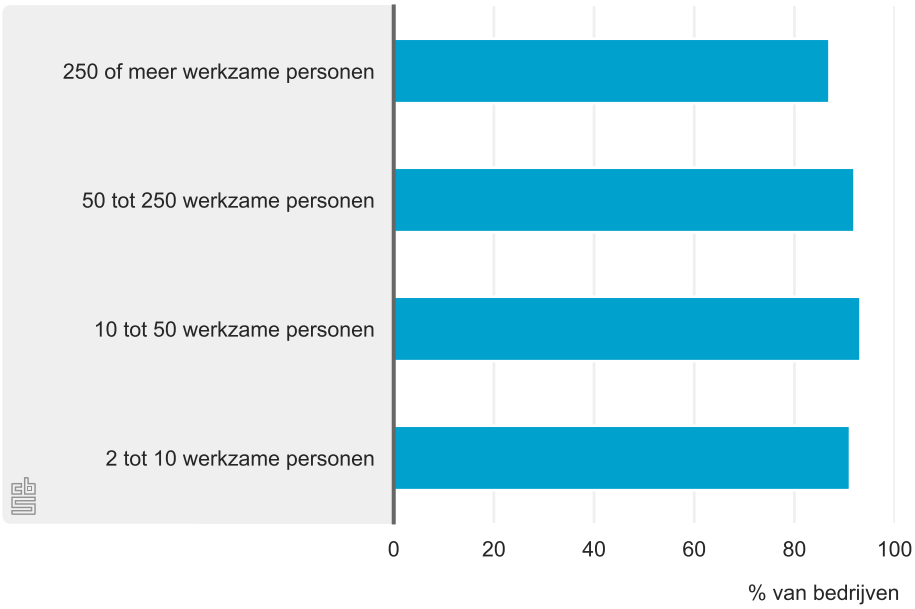


(b) Bedrijfstak

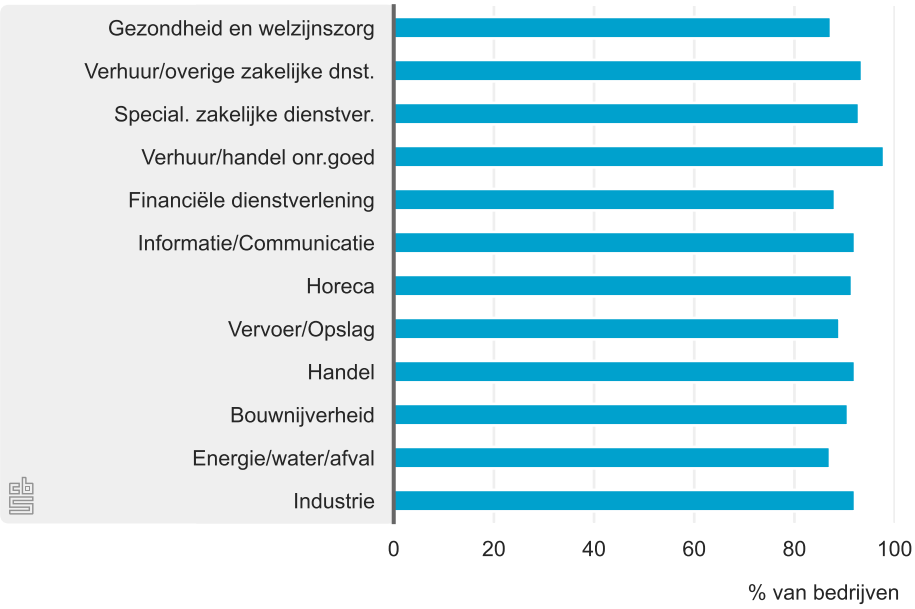


B.1.19 Categorie HTTPS: percentage bedrijven met geslaagde test 'TLS client-initiated renegotiation' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse

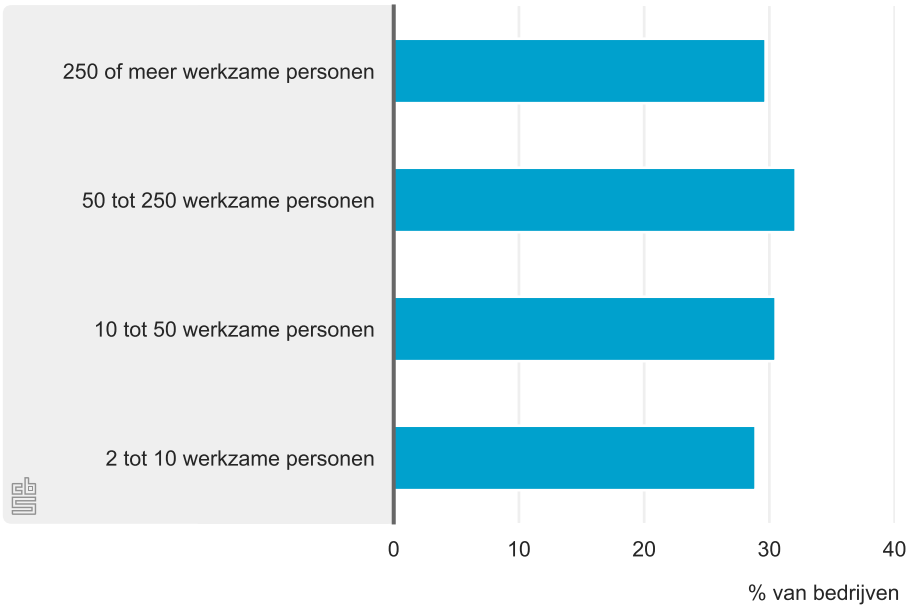


(b) Bedrijfstak

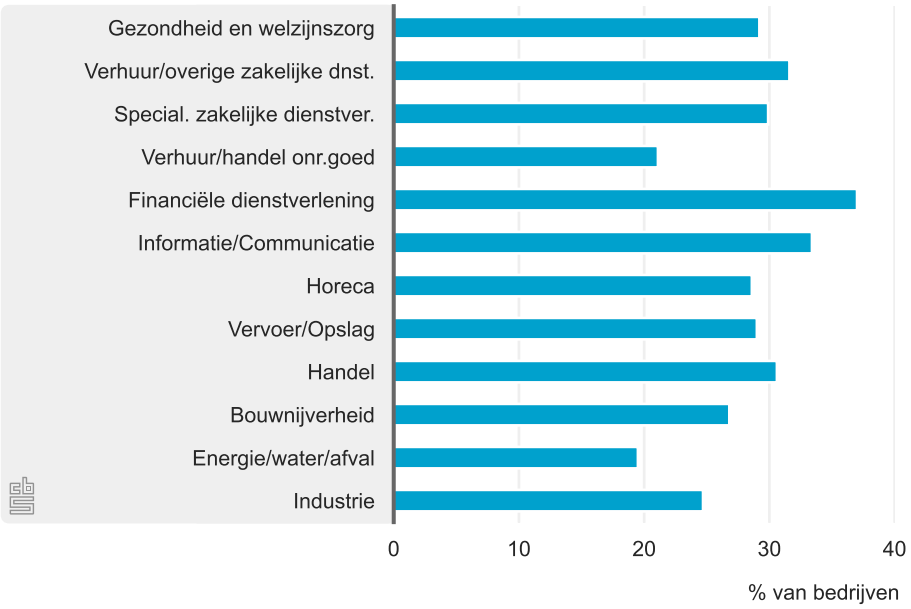


B.1.20 Categorie HTTPS: percentage bedrijven met geslaagde test 'TLS 0-RTT' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse

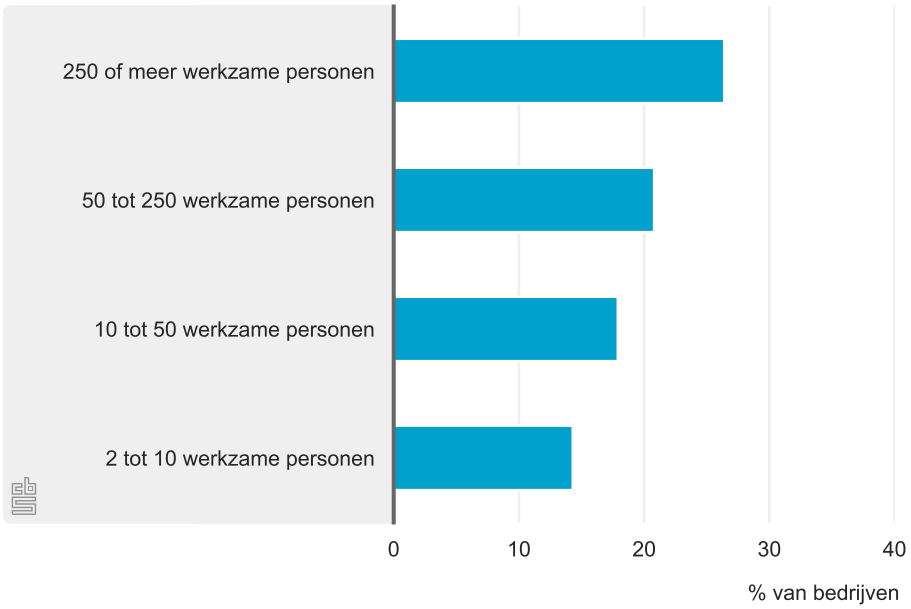


(b) Bedrijfstak

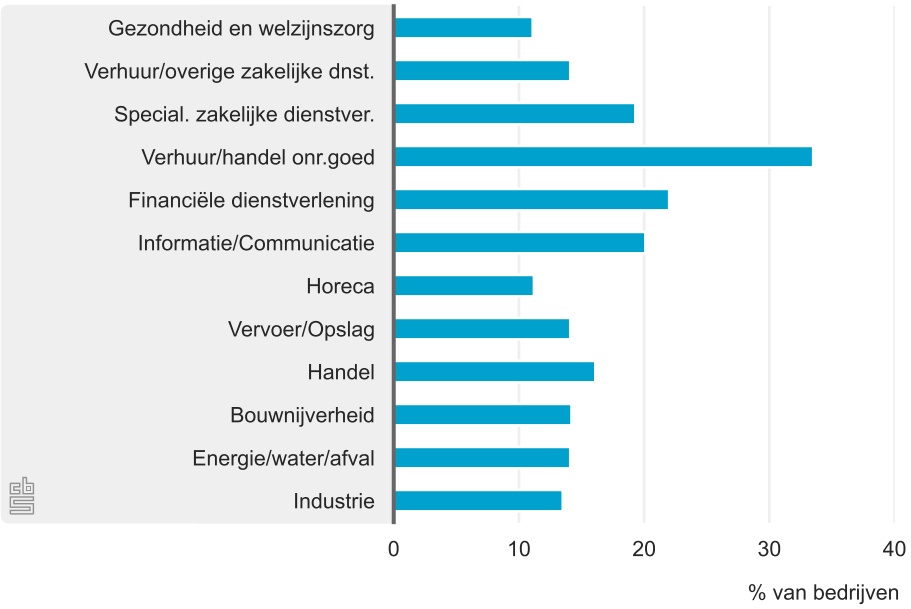


B.1.21 Categorie HTTPS: percentage bedrijven met geslaagde test 'TLS OCSP stapeling' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse



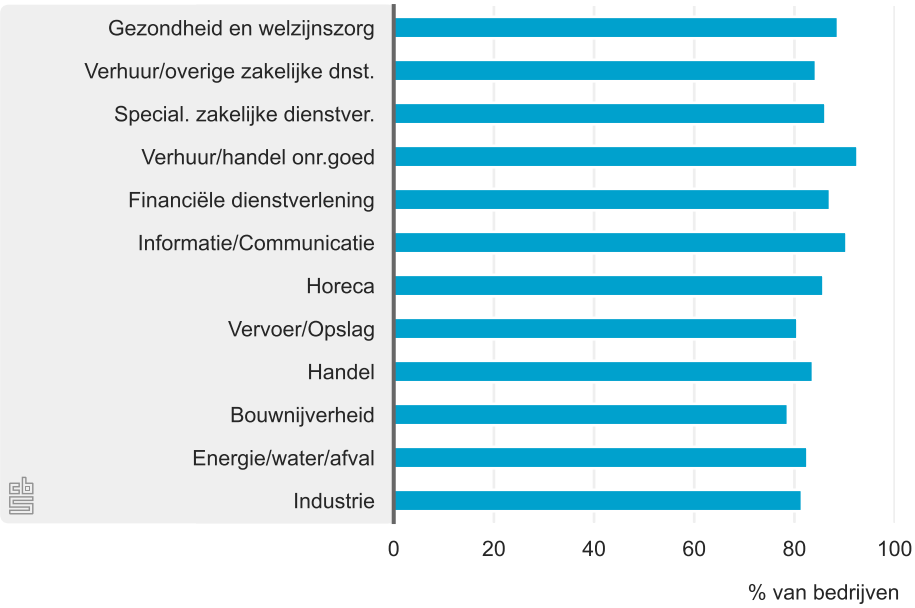
(b) Bedrijfstak



B.1.22 Categorie HTTPS: percentage bedrijven met geslaagde test 'Vertrouwensketen van certificaat' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

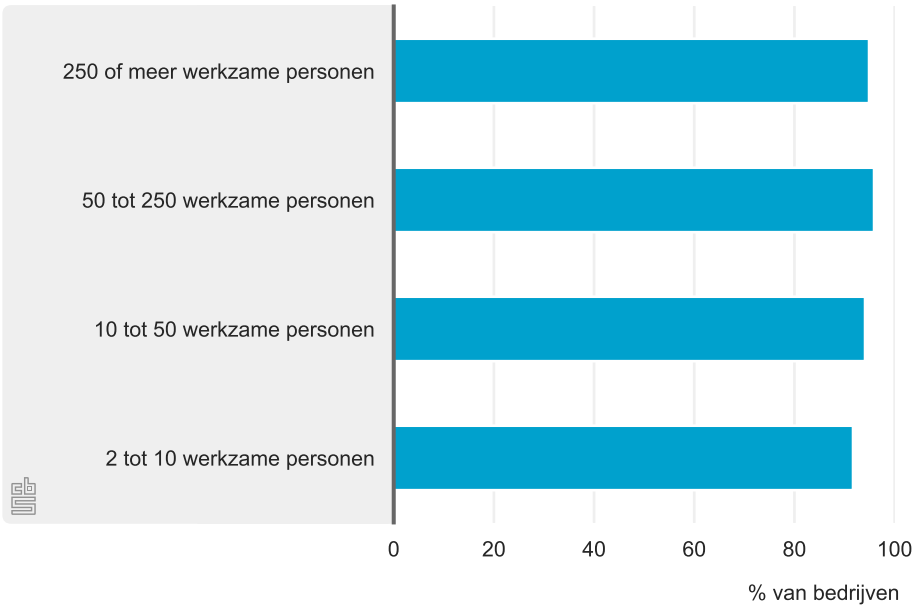
(a) Bedrijfsgrootteklasse

(b) Bedrijfstak

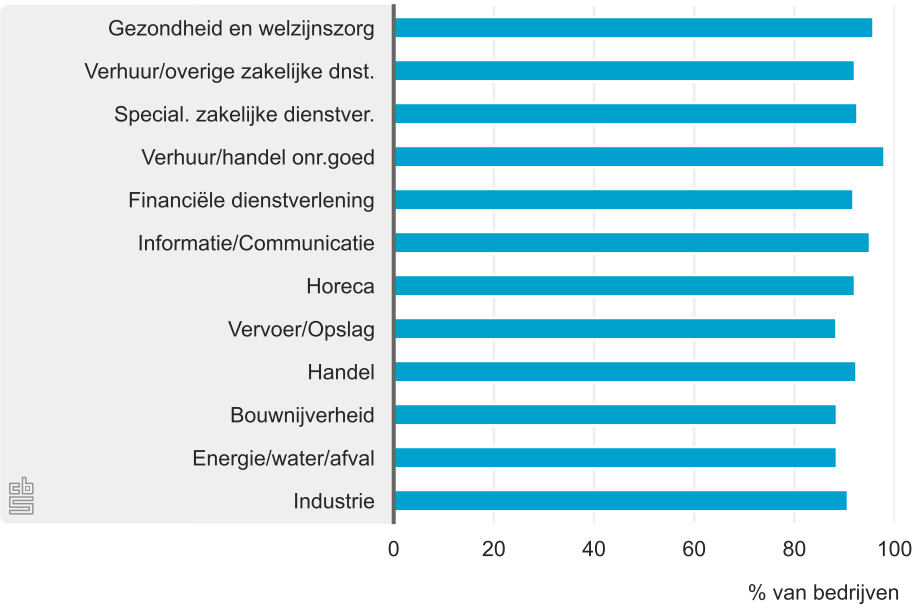


B.1.23 Categorie HTTPS: percentage bedrijven met geslaagde test 'Publieke sleutel van certificaat' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse

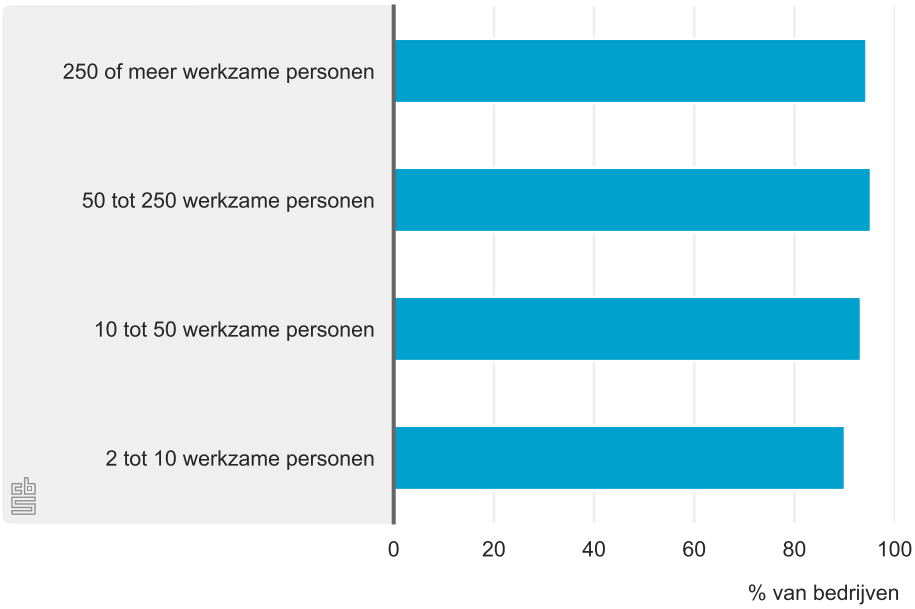


(b) Bedrijfstak

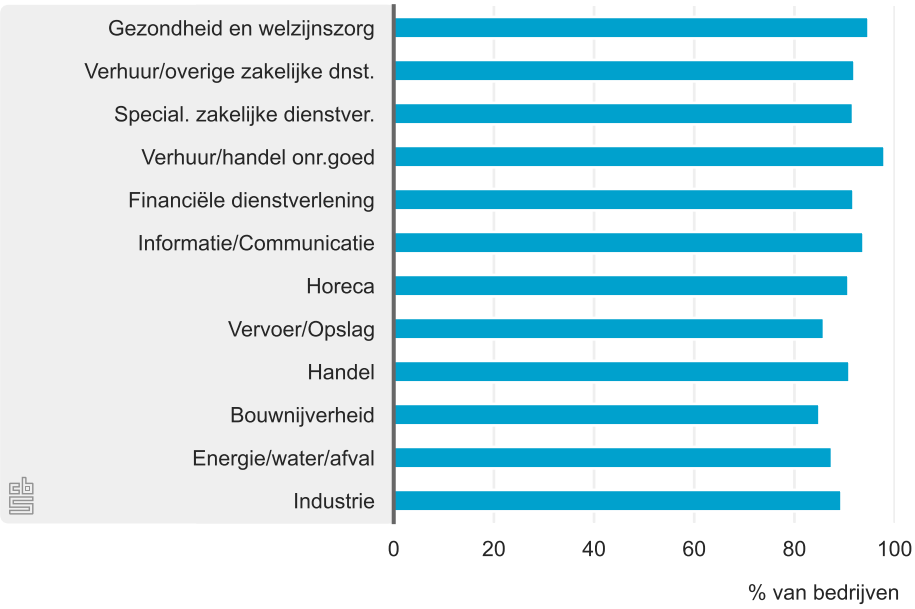


B.1.24 Categorie HTTPS: percentage bedrijven met geslaagde test 'Handtekening van certificaat' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse

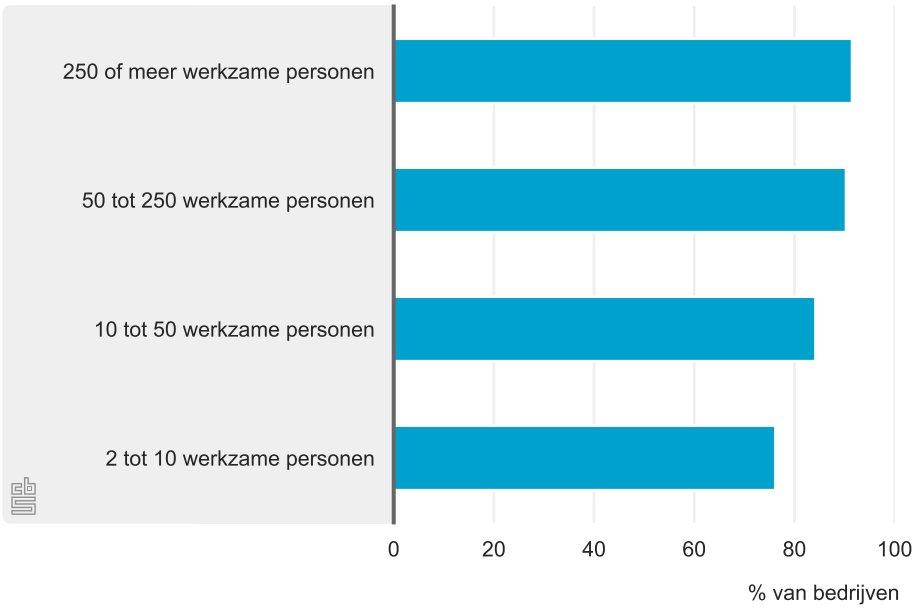


(b) Bedrijfstak

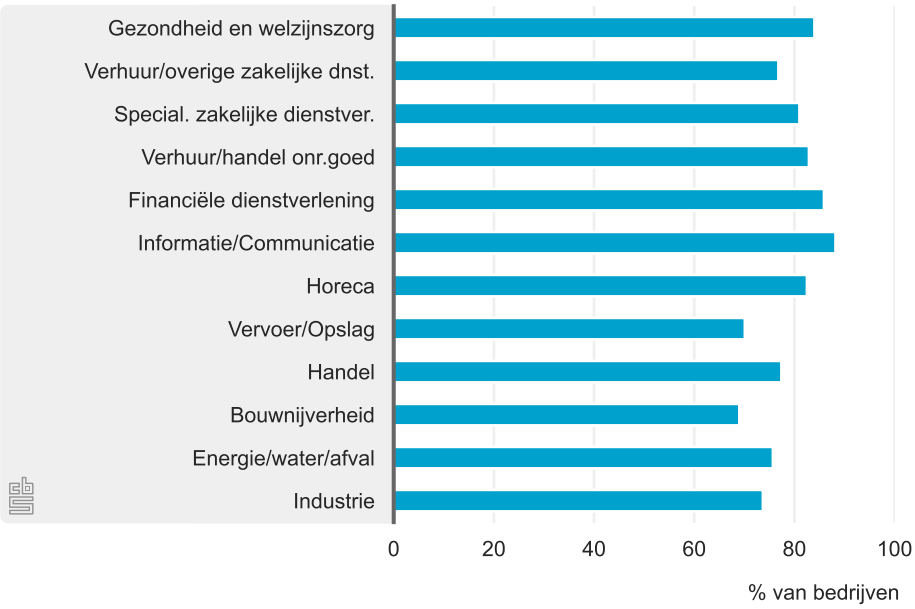


B.1.25 Categorie HTTPS: percentage bedrijven met geslaagde test 'Domeinnaam op certificaat' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse

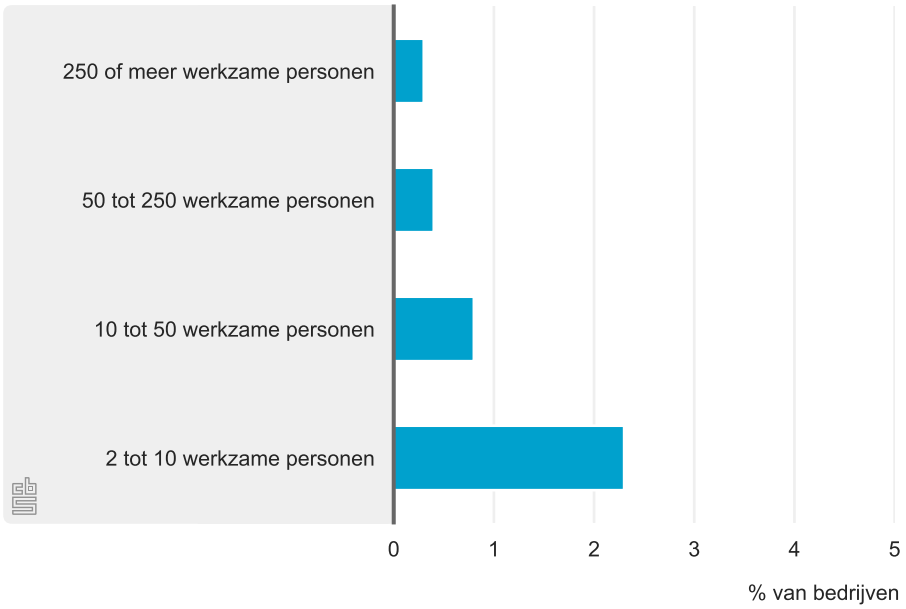


(b) Bedrijfstak

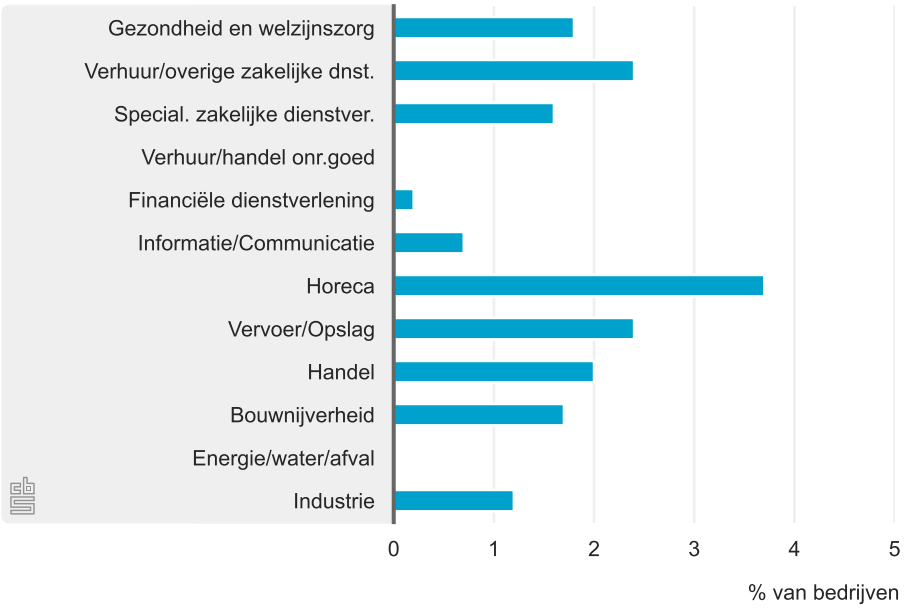


B.1.26 Categorie HTTPS: percentage bedrijven met geslaagde test 'DANE aanwezig' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse

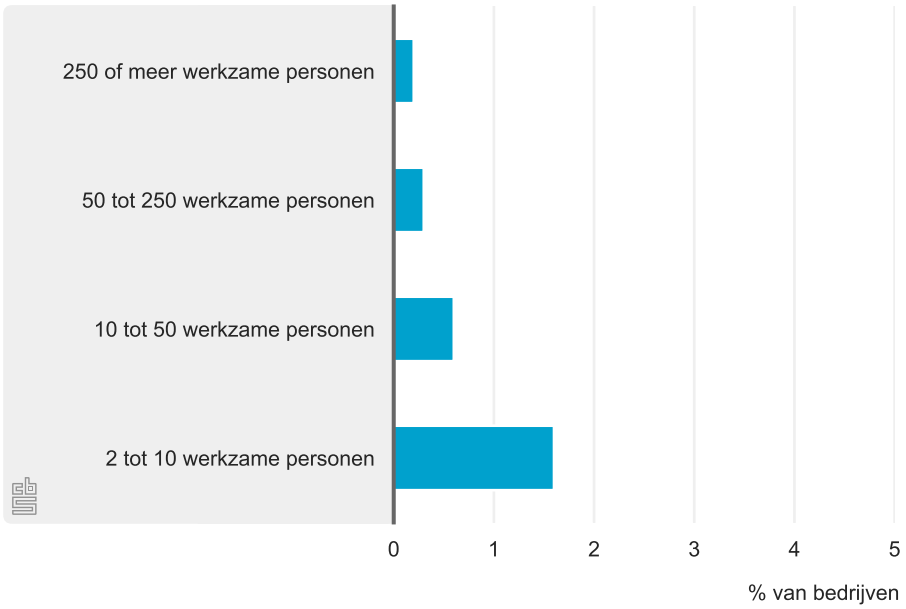


(b) Bedrijfstak

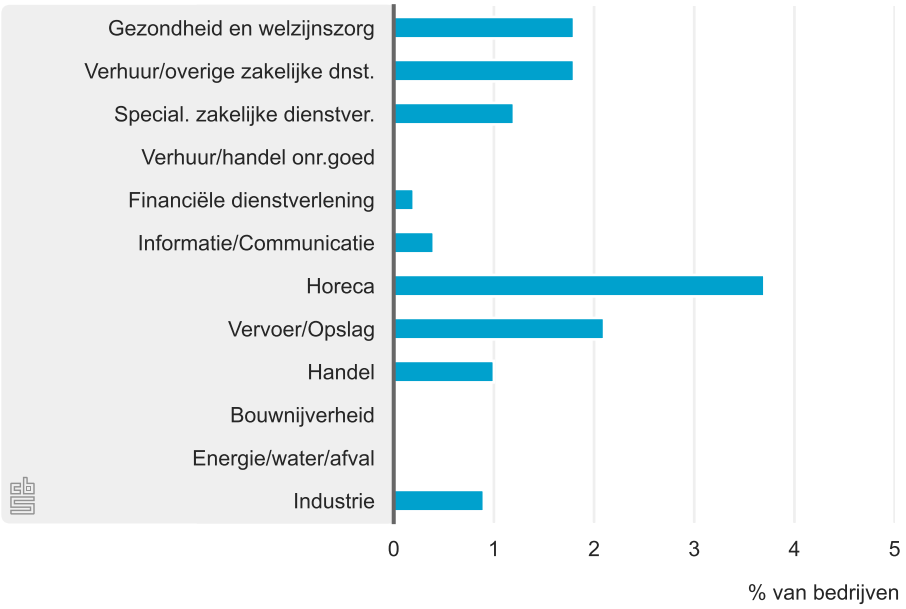


B.1.27 Categorie HTTPS: percentage bedrijven met geslaagde test 'DANE geldigheid' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse

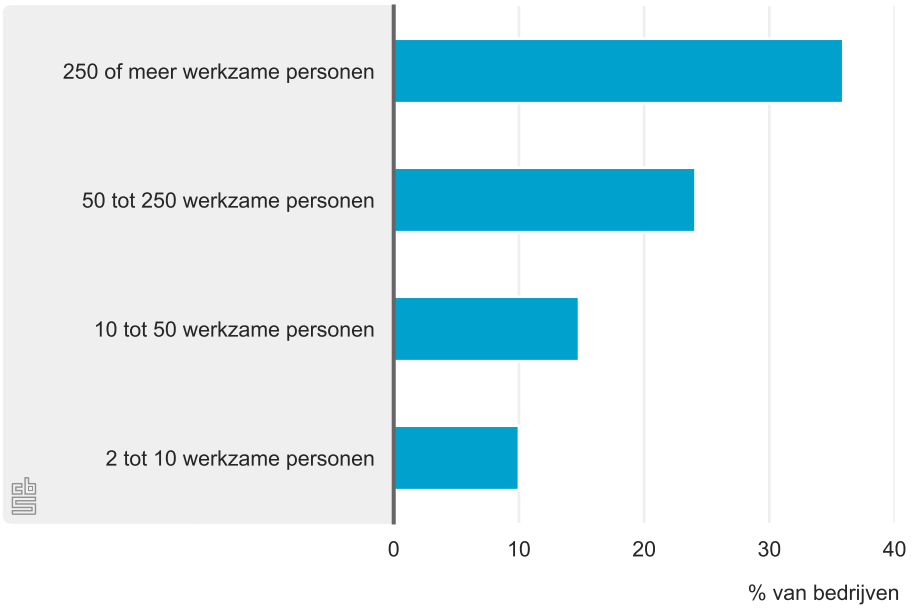


(b) Bedrijfstak

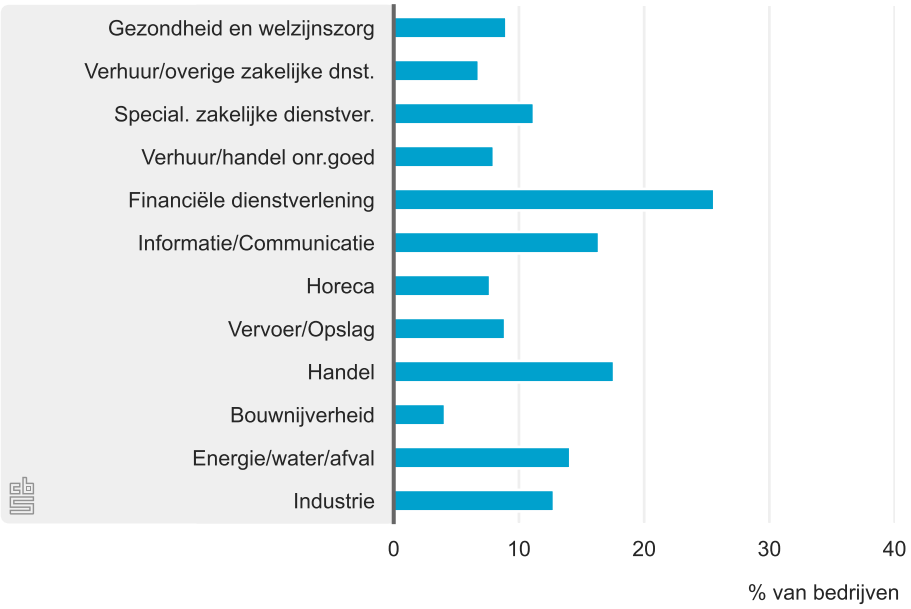


B.1.28 Categorie Beveiligingsopties: percentage bedrijven met geslaagde test 'X-Frame options' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse

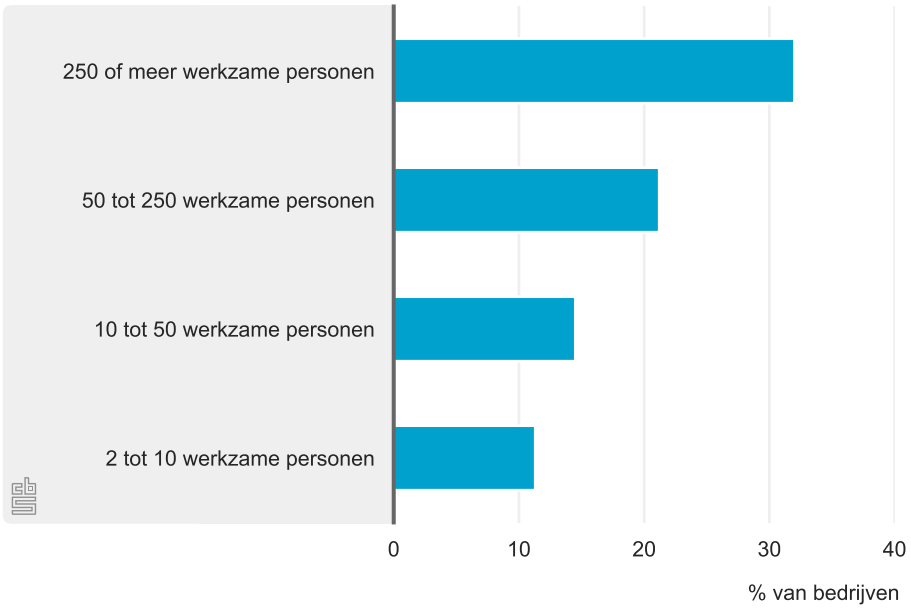


(b) Bedrijfstak

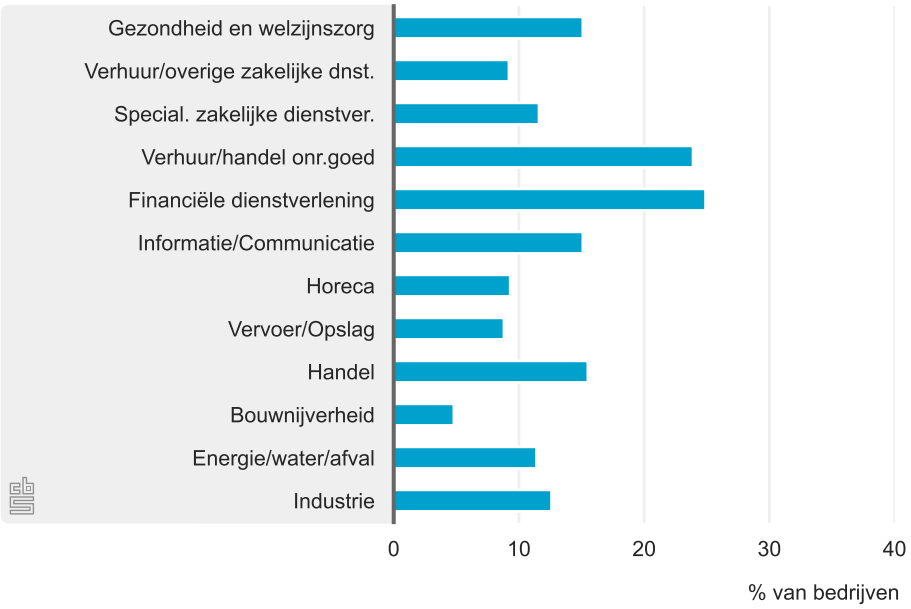


B.1.29 Categorie Beveiligingsopties: percentage bedrijven met geslaagde test 'X-Content-Type options' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse

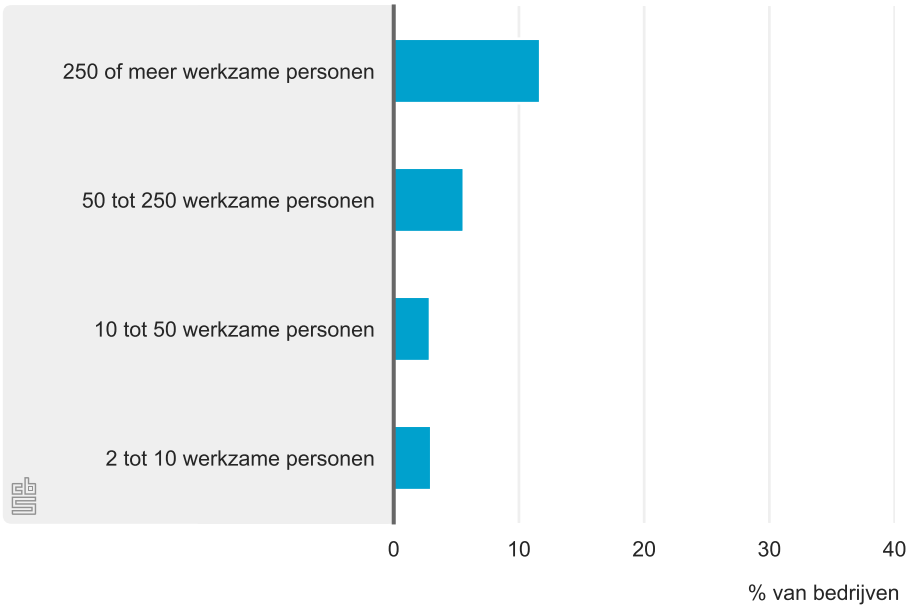


(b) Bedrijfstak

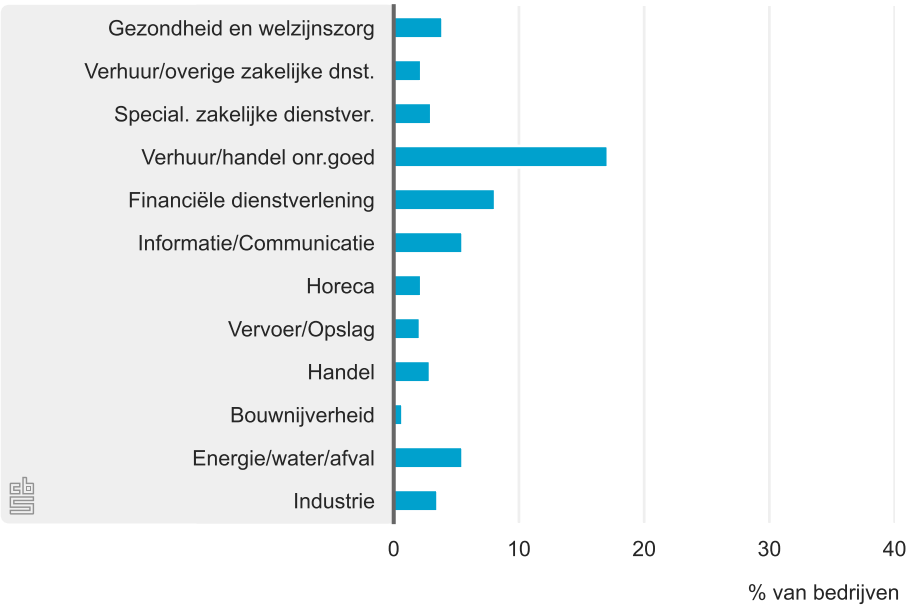


B.1.30 Categorie Beveiligingsopties: percentage bedrijven met geslaagde test 'Content-security policy' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse

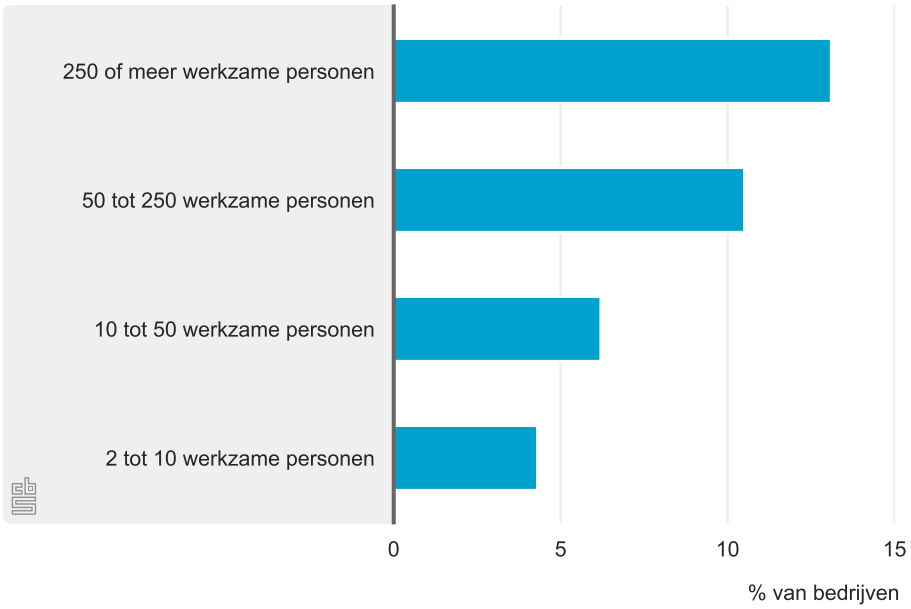


(b) Bedrijfstak

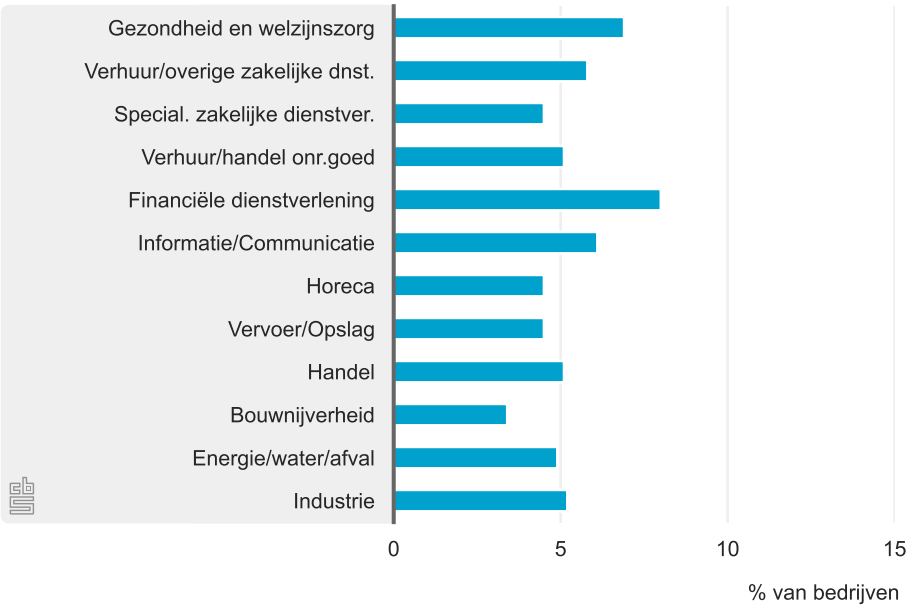


B.1.31 Categorie Beveiligingsopties: percentage bedrijven met geslaagde test 'Referred Policy aanwezig' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse

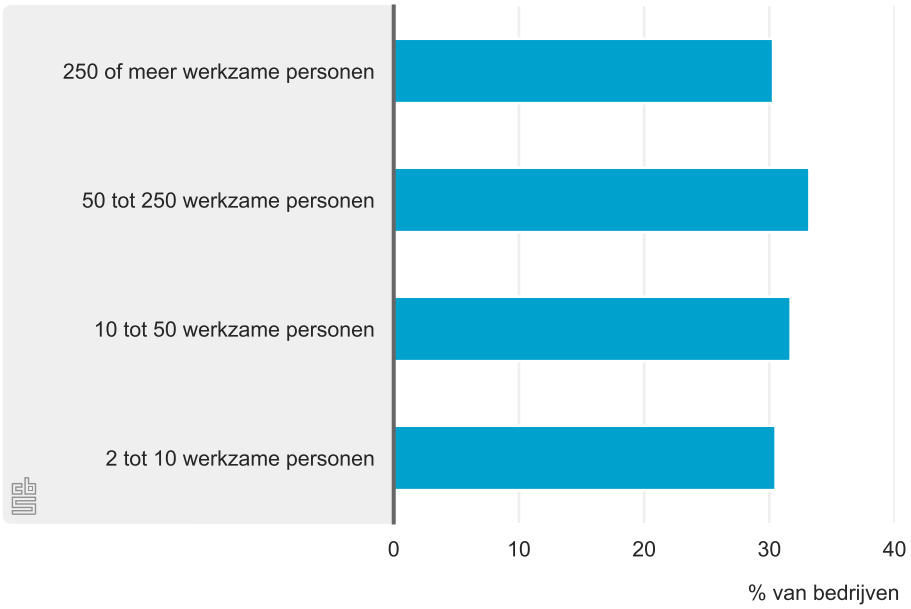


(b) Bedrijfstak

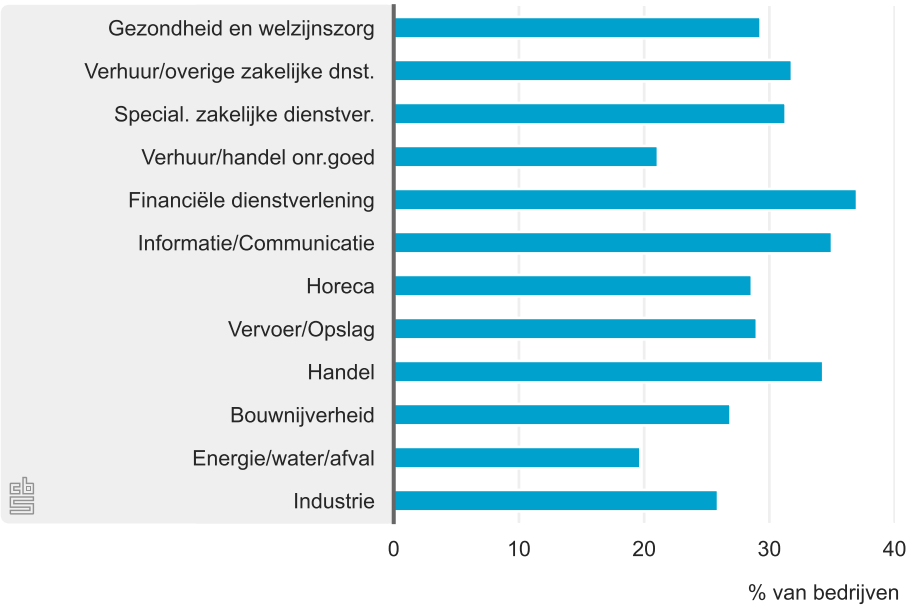


B.1.32 Categorie Beveiligingsopties: percentage bedrijven met geslaagde test 'Custom Tls 1.3 support' per bedrijfsgrootteklasse (a) en bedrijfstak (b).

(a) Bedrijfsgrootteklasse



(b) Bedrijfstak



Uitgave 2022