Cybersecuritymonitor

2023

Cybersecuritymonitor

2023

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

Samenvatting

In de Cybersecuritymonitor rapporteert het CBS over de meest actuele stand van zaken rond de cyberweerbaarheid van bedrijven en huishoudens in Nederland. Dat gebeurt hoofdzakelijk met CBS-cijfers over het aantal cybercrime-gerelateerde incidenten en maatregelen die genomen worden om deze incidenten te voorkomen. Dit jaar zien we voor het eerst een lichte afname van het aantal bedrijven met twee of meer werknemers dat de helft of meer van de gevraagde Cybersecuritymaatregelen neemt, namelijk van 52 procent in 2021 naar 47 procent in 2022. Toch is ook het aandeel bedrijven dat een incident door een aanval van buitenaf meldt gelijk gebleven: vijf procent van de bedrijven met twee of meer werknemers meldt een incident door een aanval van buitenaf. Van deze aanvallen is het bij minder dan één procent van de bedrijven met twee of meer werknemers een ransomware aanval.

Inhoud

1. Inleiding

Dit is het zevende jaar op rij dat het Centraal Bureau voor de Statistiek (CBS) de Cybersecuritymonitor uitbrengt. Het doel van de monitor is het rapporteren over de meest actuele stand van zaken rond de cyberweerbaarheid van bedrijven en huishoudens in Nederland. Dat gebeurt hoofdzakelijk met CBS-cijfers over het aantal cybercrime-gerelateerde incidenten en maatregelen die genomen worden om deze incidenten te voorkomen.

De Cybersecuritymonitor wordt mede op verzoek van het ministerie van Economische Zaken en Klimaat (EZK) gemaakt. De eerdere edities zijn beschikbaar via (CBS, 2017f, 2018f, 2019f, 2020f, 2022f, 2023h).

De structuur van de monitor is opgezet volgens dezelfde lijnen als in de voorgaande edities. In deze edities werd telkens aandacht besteed aan twee domeinen: de genomen maatregelen en de ICT-veiligheidsincidenten. Bij cybersecuritymaatregelen gaat het om het scala aan mogelijkheden om de veiligheid van computers, smartphones, laptops, servers en netwerken te verhogen. Bij cybersecurityincidenten gaat het juist om de gevolgen van acties of activiteiten die de veiligheid van deze digitale systemen ondermijnen. Cybersecurityincidenten hoeven niet altijd een gevolg van kwaadwillende acties te zijn. Ook een systeemfout waardoor gevoelige data naar buiten gebracht wordt of het verliezen van een onbeveiligde USB-stick in de trein kan als een cybersecurityincident gezien worden. Immers, ook bij dit soort incidenten wordt de digitale veiligheid ondermijnd. Het ontstaan van cybersecurityincidenten als gevolg van kwaadwillenden wordt ook wel aangeduid als cybercrime. Voor een uitgebreidere toelichting op het fenomeen cybersecurity en gerelateerde begrippen zoals door het CBS gehanteerd worden, verwijzen we naar de eerste Cybersecuritymonitor (CBS, 2017f).

Hoofdstuk 2 van dit rapport gaat in op de cybersecuritymaatregelen, dus op de maatregelen die door bedrijven nemen om meer cyberweerbaar te worden. Hoofdstuk 3 gaat in op alle cybersecurityincidenten bij Nederlandse bedrijven. Tot slot gaat hoofdstuk 4 in op de geregistreerde cybercrime, dus op de cybersecurityincidenten door kwaadwillenden die ook daadwerkelijk slachtoffers gemaakt hebben.

2. Cybersecurity-maatregelen

2.1 Bedrijven

Dit hoofdstuk gaat in op de maatregelen die bedrijven in Nederland nemen om zichzelf cyberweerbaar te maken. De cijfers komen uit de CBS-enquêtes 'ICT-gebruik bij bedrijven 2017' (CBS, 2017a,b,c,d,e), 'ICT-gebruik bij bedrijven 2018' (CBS, 2018a,b,c,d,e), 'ICT-gebruik bij bedrijven 2019' (CBS, 2019c,e,d,b,a), 'ICT-gebruik bij bedrijven 2020' (CBS, 2020d,a,e,c,b), 'ICT-gebruik bij bedrijven 2021' (CBS, 2021b,d,c,a,e), 'ICT-gebruik bij bedrijven 2022' (CBS, 2022c,e,d,b,a) en 'ICT-gebruik bij bedrijven 2023' (CBS, 2023d,f,e,c,b).

De jaarlijkse enquête 'ICT-gebruik bij bedrijven' (of kortweg: de ICT-enquête) wordt in samenwerking met de andere EU-landen uitgevoerd onder leiding van Eurostat. Een deel van de uitvoeringskosten van de ICT-enquête wordt door Eurostat gefinancierd. Het ministerie van Economische Zaken en Klimaat financiert extra onderdelen van het onderzoek die niet verplicht zijn op basis van EU-regelgeving.

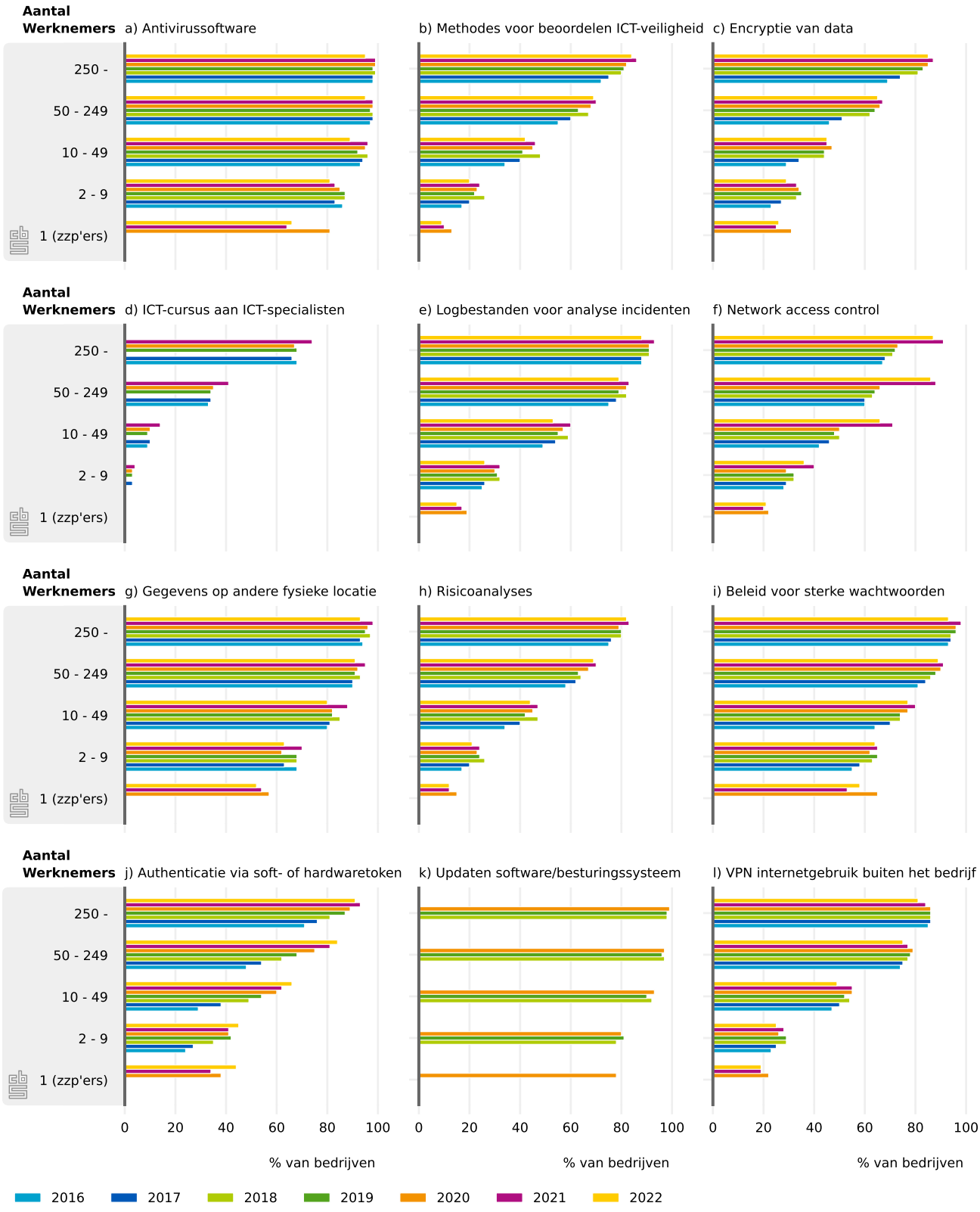
Via de ICT-enquête wordt jaarlijks het ICT-gebruik van bedrijven in Nederland in kaart gebracht. Dit levert ook cijfers op die iets zeggen over de cyberweerbaarheid van bedrijven: de mate waarin zij bedrijfsprocessen en waardevolle data beveiligen tegen cybercriminelen. In deze monitor besteden we afzonderlijk aandacht aan de maatregelen die bedrijven nemen om zich te beveiligen tegen aanvallen van buitenaf en het optreden van ICT-veiligheidsincidenten. De maatregelen worden in dit hoofdstuk beschreven; de incidenten komen in het volgende hoofdstuk aan bod.

De ICT-enquête wordt gehouden onder ongeveer 20 duizend aselect getrokken Nederlandse bedrijven uit verschillende grootteklassen en bedrijfstakken. De afgelopen drie jaar werd ook een beknopte versie van de ICT-enquête naar zo'n 22 duizend zelfstandigen zonder personeel (zzp'ers) uitgestuurd. Deze beknopte versie bevat voornamelijk de ICT-veiligheidsvragen uit de enquête die naar de grote bedrijven gestuurd wordt. De resultaten van de zzp'ers worden de afgelopen drie jaar in deze monitor meegenomen en vergeleken met die van bedrijven met twee of meer werknemers.

In de bijlagen wordt in tabellen A.1.1 en A.1.2 een overzicht van respectievelijk alle grootteklassen en bedrijfstakken gegeven. In het huidige hoofdstuk worden de cijfers van vijf grootteklassen uitgelicht: zzp'ers (1 werkzame persoon), bedrijven met 2 tot 10 werkzame personen, bedrijven met 10 tot 50 werkzame personen, bedrijven met 50 tot 250 werkzame personen en bedrijven met 250 of meer werkzame personen. Daarnaast laten we nog voor vijf bedrijfstakken de cijfers zien: 1) Gezondheid en welzijnszorg (Zorg), 2) Financiële dienstverlening (Finan.Dnst.), 3) Horeca, 4) ICT-sector en 5) Industrie. Deze bedrijfstakken zijn gekozen omdat de resultaten van de genomen ICT-veiligheidsmaatregelen en de voorgekomen ICT-veiligheidsincidenten in deze bedrijfstakken het meest uiteenlopen. Bij de bespreking van de kosten laten we andere bedrijfstakken zien, namelijk de bedrijfstakken die de hoogste kosten van incidenten hebben gemeld.

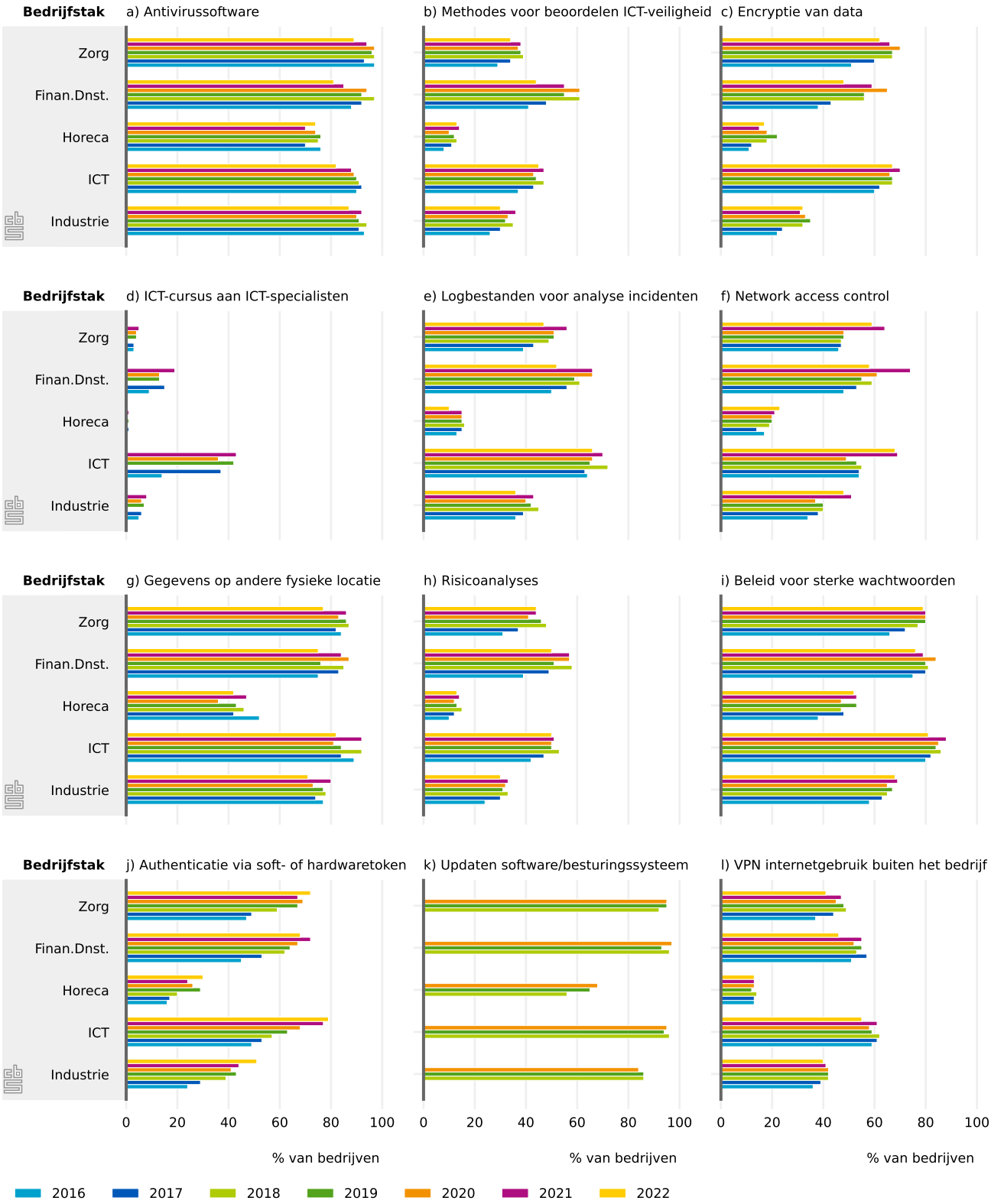
Een compleet overzicht van de cijfers voor alle grootteklassen en bedrijfstakken kan in bijlage A.2 en bijlage A.3 gevonden worden, of zijn online beschikbaar op Statline (CBS, 2023g).

2.1.1 Genomen ICT-veiligheidsmaatregelen per bedrijfsgrootteklasse.



Bron: CBS (2017e, 2018e, 2019a, 2020b, 2021e, 2022a, 2023b)

2.1.2 Genomen ICT-veiligheidsmaatregelen per bedrijfstak met 2 of meer werkzame personen.



Bron: CBS (2017e, 2018e, 2019a, 2020b, 2021e, 2022a, 2023b)

Maatregelen ter verbetering van de cyberweerbaarheid

In de ICT-enquête worden verschillende vragen gesteld over de cyberweerbaarheid van bedrijven. Zo is aan bedrijven gevraagd welke ICT-veiligheidsmaatregelen zijn getroffen. Ook is gevraagd wie de ICT-veiligheidsmaatregelen binnen het bedrijf uitvoert: het eigen personeel, een extern bedrijf, of een combinatie van beide.

In dit deel bekijken we eerst hoe vaak verschillende cybersecuritymaatregelen door bedrijven toegepast worden. Figuren 2.1.1(a–l) en 2.1.2(a–l) tonen het aandeel bedrijven dat in de periode 2016–2022 verschillende cybersecuritymaatregelen toepast, naar grootteklasse en bedrijfstak.[1)] Voor de duidelijkheid worden slechts vier grootteklassen en vier bedrijfstakken uitgelicht. Het volledige overzicht wordt in tabellen A.2.1 en A.2.2 gegeven en is terug te vinden op StatLine (CBS, 2023g). Uiteraard kan met deze twaalf maatregelen nooit een compleet beeld van het ICT-beveiligingsniveau van bedrijven gegeven worden. Toch ontstaat hierdoor wel een globale indruk, omdat elke extra maatregel die een bedrijf neemt een extra bijdrage levert aan de cyberweerbaarheid van het bedrijf.

Grotere bedrijven nemen meer maatregelen tegen cyberdreigingen

Over het algemeen kan gezegd worden dat het ICT-beveiligingsniveau van een bedrijf hoger is naarmate er meer maatregelen tegelijkertijd genomen worden. Figuur 2.1.1 laat zien dat elke maatregel vaker wordt genomen door grotere bedrijven dan door kleinere bedrijven. Voor sommige maatregelen is dit patroon sterker dan voor andere.

Voor bijvoorbeeld een gangbare maatregel als het gebruik van antivirussoftware zijn de verschillen tussen grotere en kleinere bedrijven niet zo groot: meer dan 80 procent van alle bedrijven met meer dan 2 werknemers gebruikt antivirussoftware, ongeacht de grootteklasse (figuur 2.1.1(a)). Bij een moeilijker toe te passen maatregel zoals het gebruik van een Virtual Private Netwerk (VPN) zijn er wel grotere verschillen te zien: 25 procent van de microbedrijven (2 tot 10 werknemers) maakte in 2022 gebruik van VPN, tegenover 81 procent van de grote bedrijven (250 of meer werknemers) (figuur 2.1.1(l)). Het is begrijpelijk dat grote bedrijven meer maatregelen treffen, omdat zij vaak een grotere en complexere ICT-infrastructuur hebben die een breder spectrum aan beveiligingsmaatregelen vereist.

Figuur 2.1.1 toont ook het percentage zzp'ers dat in 2020, 2021 en 2022 ICT-veiligheidsmaatregelen nam. Er kan geconcludeerd worden dat bij alle ICT-veiligheidsmaatregelen het percentage zzp'ers dat deze maatregelen neemt net iets lager is dan dat voor bedrijven in de bovenliggende grootteklasse van 2 tot 10 werknemers. Dit is consistent met de constatering dat kleinere bedrijven minder ICT-veiligheidsmaatregelen nemen dan grote bedrijven.

1) Let op dat data van een bepaald jaar vaak komt uit de ICT-enquête van het jaar daarna. Zo komt de data die betrekking heeft op 2022 uit de ICT-enquête van 2023 (CBS, 2023d).

Toename authenticatie met soft- of hardwaretoken

Figuur 2.1.1(j) laat zien dat het gebruik van een soft- of hardwaretoken voor het inloggen door een bedrijf sinds 2016 flink is toegenomen. Bij deze zogenaamde tweefactorauthenticatie[2)] moet naast een wachtwoord een extra code ingevoerd worden die per inlogsessie verandert. Deze code wordt verkregen via een specifiek apparaatje of via een app op de smartphone. Dit maakt inloggen een stuk veiliger, want zelfs als een wachtwoord onderschept wordt, biedt de vereiste extra code bescherming tegen inloggen door ongeautoriseerde gebruikers.

Het gebruik van soft- of hardwaretokens komt vanaf 2016 in alle grootteklassen steeds vaker voor. Bij grote bedrijven (250 of meer werknemers) is deze manier van inloggen bijvoorbeeld toegenomen van 71 procent in 2016 tot 91 procent in 2022. Bij microbedrijven (twee tot tien werknemers) is dit zelfs bijna verdubbeld van 23 procent in 2016 naar 45 procent in 2022.

ICT-veiligheidsmaatregelen per bedrijfstak

Figuur 2.1.2 laat het aantal maatregelen voor enkele bedrijfstakken met twee of meer werknemers zien (de zzp'ers zijn hier dus niet in meegenomen). Bedrijven die meer met ICT bezig zijn of die een groot belang hebben bij het beveiligen van hun data, zoals respectievelijk de ICT-sector en de gezondheidszorg, scoren beter op het gebied van cybersecurity dan sectoren waar dit minder belangrijk lijkt, zoals de horeca. De horeca heeft wel relatief meer kleinere bedrijven, waarvan we eerder zagen dat deze minder cybersecuritymaatregelen nemen dan grote bedrijven. Maar het ligt ook voor dat hand de horeca minder cybersecuritymaatregelen neemt omdat ze voor hun werkzaamheden minder van ICT afhankelijk zijn. Dit blijkt bijvoorbeeld uit eerder op Statline gepubliceerde cijfers over de mate van digitalisering van bedrijven (CBS, 2021d).

Aantal genomen ICT-veiligheidsmaatregelen

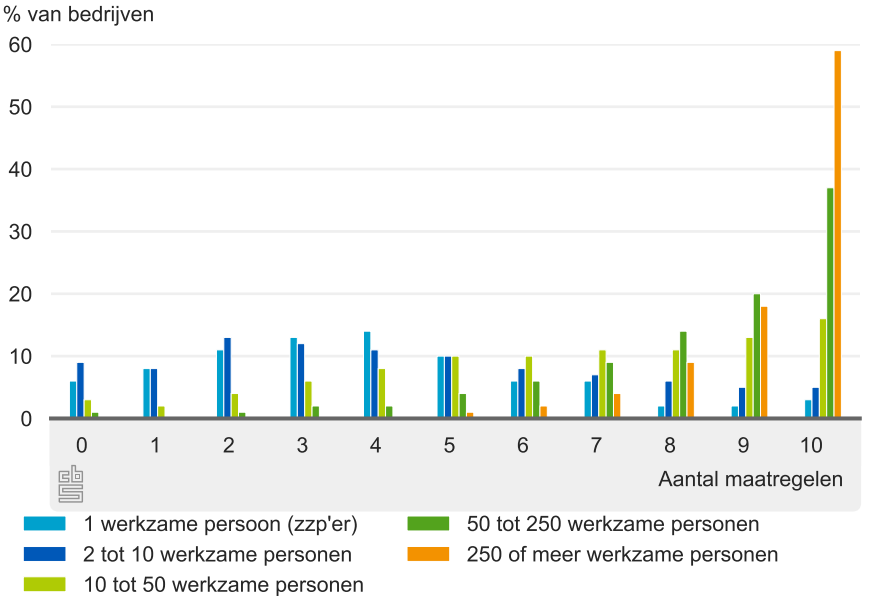
Dat grote bedrijven vaker verschillende ICT-maatregelen nemen dan kleinere bedrijven komt nogmaals terug in figuren 2.1.3(a) en 2.1.3(b). In deze figuren wordt per bedrijfsgrootte en bedrijfstak het percentage bedrijven getoond dat een zeker aantal maatregelen neemt. De resultaten laten zien dat kleinere bedrijven hoger scoren op een kleiner aantal maatregelen, terwijl grotere bedrijven juist vaker meerdere maatregelen tegelijk nemen (figuur 2.1.3(a)). Van de grote bedrijven (250 of meer werknemers) neemt zelfs bijna 60 procent van de bedrijven alle tien de uitgevraagde maatregelen.[3)] In figuur 2.1.3(b) is te zien dat bedrijven in de ICT-sector over het algemeen de meeste maatregelen nemen, terwijl in de horeca vaker minder maatregelen genomen worden.

2) Strikt genomen is er nog een onderscheid te maken tussen tweefactorauthenticatie en tweestapsverificatie, maar dat laten we verder buiten beschouwing omdat beide vormen sowieso een extra beveiliging opleveren ten opzichte van het inloggen met enkel een wachtwoord.

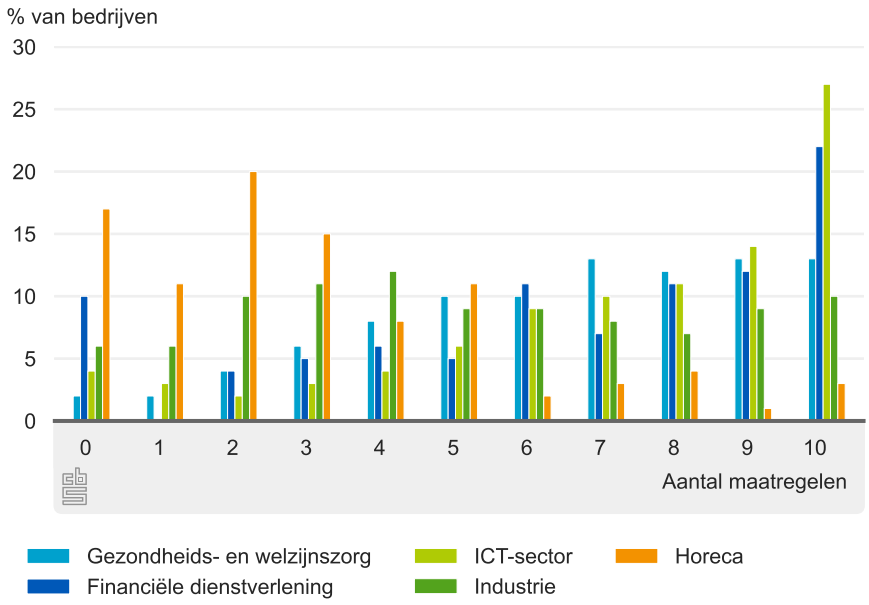
3) Van de twaalf maatregelen die in figuur 2.1.1 en figuur 2.1.2 getoond worden, nemen we er maar tien mee in figuur 2.1.3a en figuur 2.1.3b waar we het totaal aantal genomen maatregelen tonen. De reden hiervoor is dat de maatregelen 'ICT-cursus aan specialisten' (d) en 'Updaten software' (k) niet over alle jaren beschikbaar zijn.

2.1.3 Verdeling van het aantal genomen cybersecuritymaatregelen per grootteklasse (a) en bedrijfstak (b), 2022.

(a) Grootteklasse



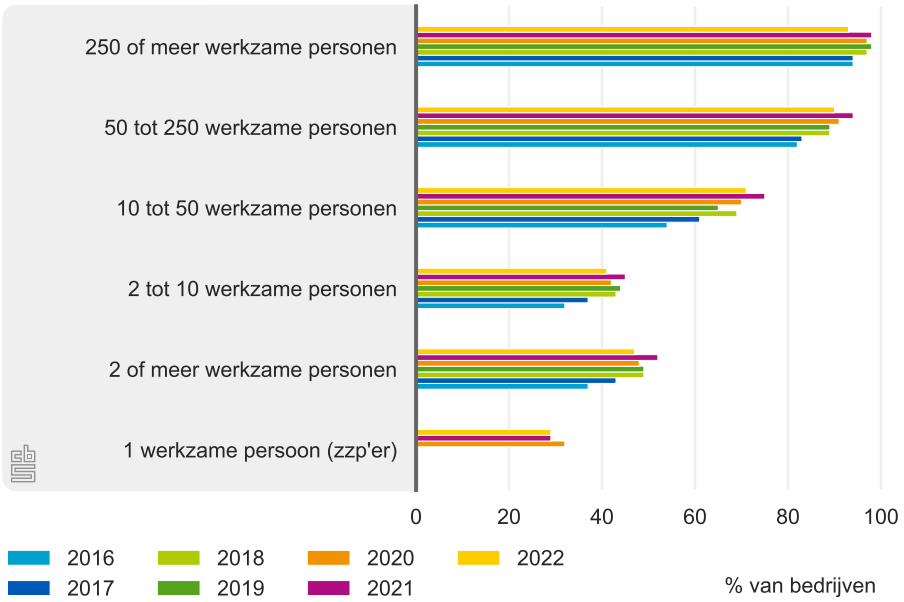
(b) Bedrijfstak



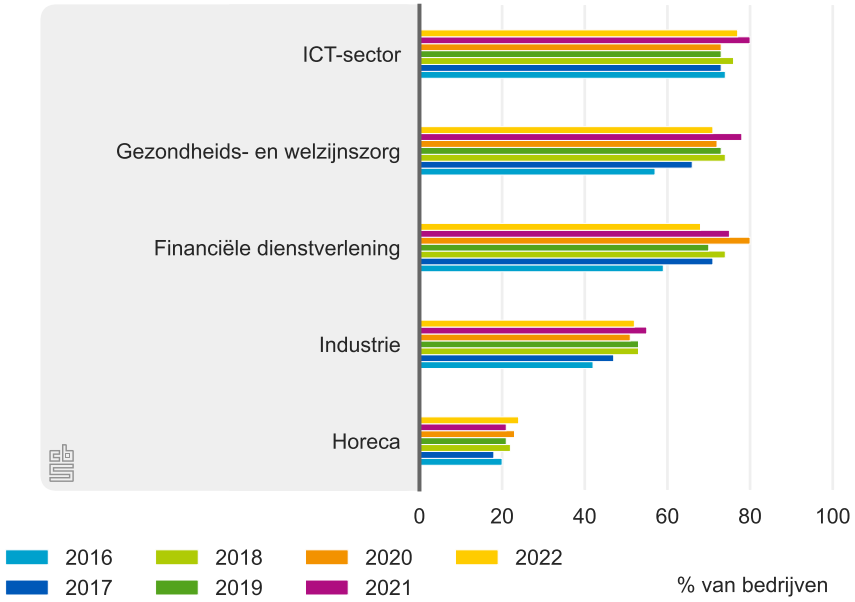
Bron: CBS (2023b)

2.1.4 Percentage van bedrijven die minimaal vijf van de tien gevraagde cybersecuritymaatregelen nemen per grootteklasse (a) en bedrijfstak (b).

(a) Grootteklasse



(b) Bedrijfstak



Bron: CBS (2023b)

Bijna de helft van de bedrijven met twee of meer werknemers nam in 2022 minstens vijf ICT-veiligheidsmaatregelen

Uit de verdeling van het aantal maatregelen is af te leiden welk deel van de bedrijven minimaal de helft van de gevraagde maatregelen neemt. Figuren 2.1.4(a) en 2.1.4(b) tonen per grootteklasse (a) en per bedrijfstak (b) het aandeel van bedrijven dat minstens vijf van de tien uitgevraagde ICT-veiligheidsmaatregelen neemt. Figuur 2.1.4(a) laat zien dat het aantal bedrijven dat vijf of meer maatregelen neemt tot 2021 is toegenomen. In 2022 is het aandeel van bedrijven met twee of meer werknemers dat minimaal vijf maatregelen neemt echter licht gedaald. Toch neemt in 2022 nog steeds 93 procent van de grote bedrijven (250 of meer werknemers) minimaal vijf van de tien maatregelen. Van de zzp'ers neemt 29 procent in 2022 vijf of meer van de gevraagde ICT-veiligheidsmaatregelen.

In figuur 2.1.4(b) is te zien dat in de bedrijfstakken 'ICT-sector', 'Financiële dienstverlening' en 'Gezondheids- en welzijnszorg' een relatief grote groep bedrijven meer dan vijf maatregelen treft (in 2022 ruim 70 procent), terwijl dit percentage voor de horeca een stuk lager ligt met ongeveer 25 procent. We kunnen echter zien dat, vergeleken met 2016, het aandeel bedrijven dat een groot aantal ICT-veiligheidsmaatregelen neemt, in alle bedrijfstakken is toegenomen. In 2022 neemt de toename van het percentage bedrijven dat minstens vijf maatregelen treft ten opzichte van 2021 wel iets af, behalve bij de horeca.

Uitvoering ICT-veiligheidswerkzaamheden

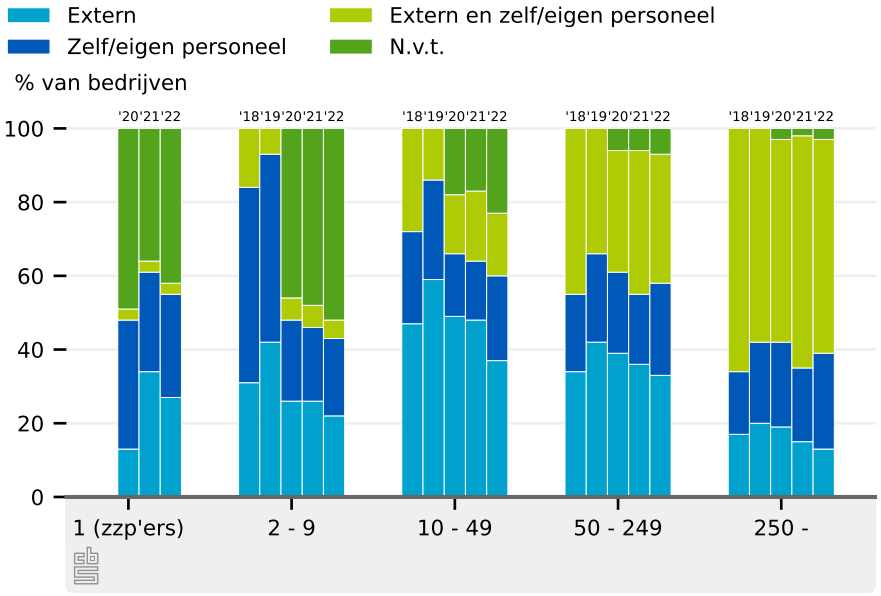
In figuren 2.1.5(a) en 2.1.5(b) wordt de organisatie van de ICT-veiligheidswerkzaamheden onder de loep genomen. Per grootteklasse en bedrijfstak wordt gekeken wie de ICT-veiligheidswerkzaamheden binnen het bedrijf uitvoert: het eigen personeel, een extern bedrijf of een mix van beide. Vanaf het jaar 2020 worden deze resultaten ook voor zzp'ers weergegeven. In 2020 is de vraagstelling wel enigszins veranderd; vanaf dat moment is de optie 'niet van toepassing' namelijk toegevoegd. In de jaren daarvoor was deze optie er niet en moesten bedrijven aangeven of de ICT-veiligheidswerkzaamheden werden uitgevoerd of werden uitbesteed (of een mix daarvan). Deze verandering is waarschijnlijk de oorzaak van de verschuiving die zichtbaar is in de resultaten vanaf 2020, vooral onder de kleinere bedrijven.

Figuur 2.1.5(a) laat zien dat de ICT-veiligheidswerkzaamheden het vaakst volledig worden uitbesteed door kleine bedrijven (10 tot 50 werknemers). Bij grote bedrijven (250 of meer werknemers) worden de maatregelen juist het vaakst deels uitbesteed en deels door het eigen personeel uitgevoerd. Dit laatste is niet opmerkelijk omdat een groot bedrijf meer personeel beschikbaar heeft om standaardmaatregelen zelf uit te voeren en daarnaast over de middelen beschikt om complexere zaken uit te besteden. Bij zzp'ers en microbedrijven (2 tot 10 werkzame personen) komt de optie 'Niet van toepassing' het vaakst voor. Dit komt overeen met de constatering dat door kleinere bedrijven minder maatregelen worden genomen dan door grote bedrijven. In alle grootteklassen lijkt de optie 'Niet van toepassing' door de tijd heen wel toe te nemen. Ook lijkt het erop dat de ICT-veiligheidswerkzaamheden steeds vaker volledig door het eigen personeel worden uitgevoerd, vooral bij grotere bedrijven (10 of meer werknemers).

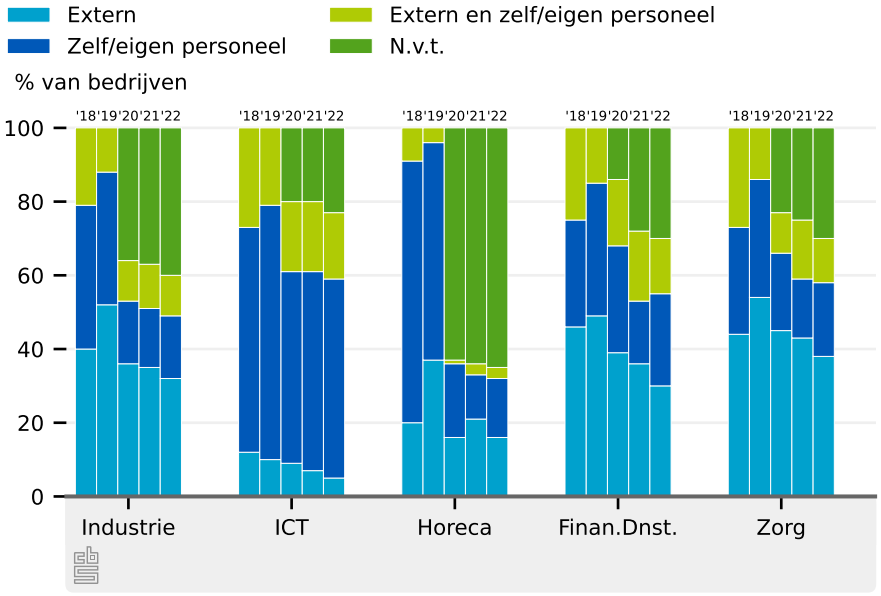
Figuur 2.1.5(b) laat tot slot zien dat bedrijven in de ICT-sector vaak in staat zijn om de ICT-veiligheidswerkzaamheden zelf uit te voeren; zo'n 54 procent doet dit volledig zelf. Ook

2.1.5 Uitvoering ICT-veiligheidswerkzaamheden per grootteklasse (a) en bedrijfstak (b)

(a) Grootteklasse



(b) Bedrijfstak



Bron: CBS (2019a, 2020b, 2021e, 2022a, 2023b)

dit is niet opmerkelijk omdat het te verwachten is dat bij deze bedrijven voldoende expertise voorhanden is om de ICT-beveiliging zelf uit te voeren. In de bedrijfstakken 'Zorg' en 'Industrie' worden de ICT-beveiligingswerkzaamheden bij zo'n 40 procent van de bedrijven volledig uitbesteed. De Horeca heeft het meest gebruik gemaakt van de nieuwe categorie 'Niet van toepassing': ruim twee derde van de horecabedrijven zegt dat ICT-beveiligingswerkzaamheden niet van toepassing. Dit hangt waarschijnlijk samen met het feit dat de Horeca relatief weinig ICT-maatregelen neemt, zodat ICT-veiligheidswerkzaamheden vaker niet aan de orde zijn.

2.2 Websites

Deze paragraaf beschrijft de maatregelen die bedrijven nemen om de beveiliging en betrouwbaarheid van hun websites te verhogen. Het gebruik van veilige en moderne internetstandaarden speelt hierbij een belangrijke rol.

Aandeel .nl-domeinnamen met DNSSEC-beveiliging stijgt

DNSSEC is een beveiligingssysteem voor het Domain Name System (DNS), oftewel het internet-telefoonboek dat zorgt voor de vertaling van domeinnamen naar IP-adressen. DNSSEC breidt DNS uit met een extra beveiliging. Met alleen DNS is de vertaling van een domeinnaam namelijk niet beveiligd. Hierdoor kan een kwaadwillende het internetverkeer van een gebruiker omleiden naar een vals IP-adres en vervolgens vertrouwelijke gegevens of zelfs geld ontfutselen. Met DNSSEC wordt bij de vertaling van domeinnaam naar IP-adres een digitale handtekening toegevoegd die een internetgebruiker automatisch kan laten controleren. Hierdoor wordt het omleiden naar een vals IP-adres voorkomen. DNSSEC is daarmee een belangrijk wapen in de strijd tegen *phishing* en *pharming*.[4)] De domeinregistratie en het bijhouden van het gebruik van DNSSEC in Nederland wordt uitgevoerd door de Stichting Internet Domeinregistratie Nederland (SIDN).

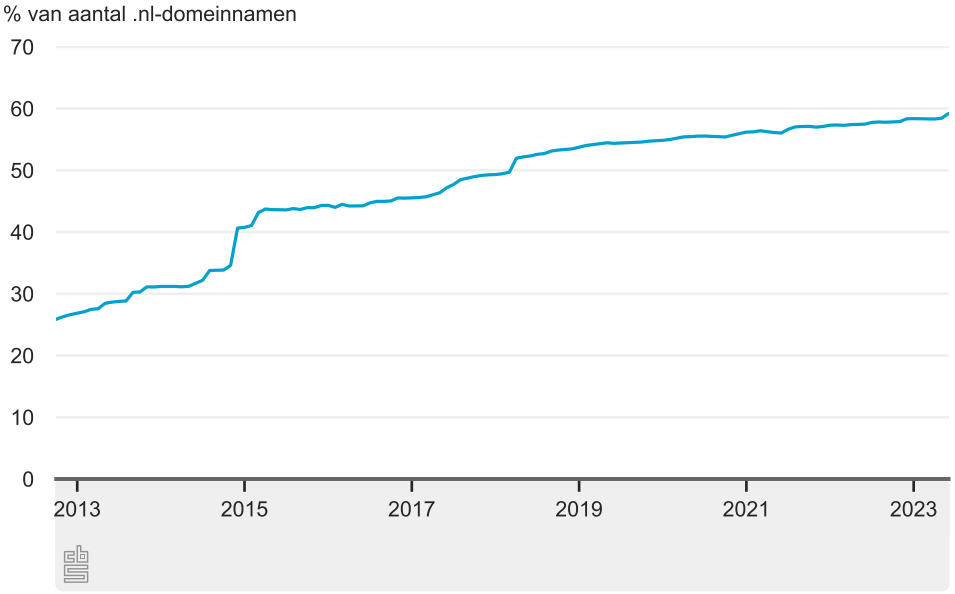
Figuur 2.2.1 toont dat het percentage met DNSSEC-beveiligde *.nl*-websites in de periode 2014 — 2024 is toegenomen tot bijna 62 procent. In de eerste jaren was deze toename groter dan in de latere jaren. Toch is dit percentage in 2024 weer wat sneller gestegen te zien ten opzichte van het jaar daarvoor. Tussen 2023 en 2024 nam het percentage met DNSSEC-beveiligde *.nl*-websites namelijk toe met ongeveer 3 procent.

Gebruik van internetstandaarden bij websites van bedrijven in Nederland

In de CBS-publicatie 'Toepassing van Internetstandaarden voor websites van bedrijven' (CBS, 2024) wordt een representatieve steekproef van websites van bedrijven met de webtool Internet.nl van Platform Internetstandaarden gescand om de mate van standaardisatie van websites van bedrijven in Nederland te bepalen. Deze mate van

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

2.2.1 Percentage .nl-domeinnamen met DNSSEC.



Bron: SIDN (2024)

standaardisatie wordt uitgedrukt in een eindscore tussen de 0% en 100%, waarbij 100% betekent dat een website aan alle internetstandaarden volgens de norm van Platform internetstandaarden voldoet.[5)] Het toepassen van internetstandaarden, zoals het gebruik van een domein-handtekening of HTTPS bij een website, is belangrijk omdat het de veiligheid, betrouwbaarheid en toegankelijkheid van het internet verhoogt.

Standaardisatie van websites van bedrijven neemt gestaag toe

De gemiddelde Internet.nl-eindscore per bedrijfsgrootte is per jaar voor alle bedrijfsgrootteklassen ongeveer gelijk en neemt per jaar gestaag toe (zie figuur 2.2.2). Zo is de gemiddelde Internet.nl-eindscore voor alle bedrijven met een website met twee of meer werknemers gestegen van 60,3 procent in 2020 naar 65,5 procent in april 2024. Dit laat zien dat bedrijven in Nederland steeds beter de juiste internetstandaarden voor hun website toepassen.

Ook de Internet.nl-eindscore per bedrijfstak is gestegen sinds 2020, zoals weergegeven in figuur 2.2.3. Met name de bedrijfstak ‘Financiële dienstverlening’ heeft het afgelopen jaar relatief veel aandacht besteed aan het implementeren van veiligheidsstandaarden voor hun website. Opvallend is wel 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. Ook enkele andere sectoren vertonen tussen april en december 2023 een daling in de eindscore. Deze dalingen komen met name door een daling van het aantal bedrijven dat slaagt voor de categorie IPv6, de moderne standaard voor het IP-adres. Zie voor meer informatie hierover de publicatie ‘Toepassing van Internetstandaarden voor websites van bedrijven’ (CBS, 2024).

5) Een score van 100 procent wil echter nog niet zeggen dat een online dienst per definitie veilig is; er zijn nog meer aspecten die een rol spelen. De Internet.nl-test is dus een test op het gebruik van de juiste internetstandaarden en geen veiligheidstest.

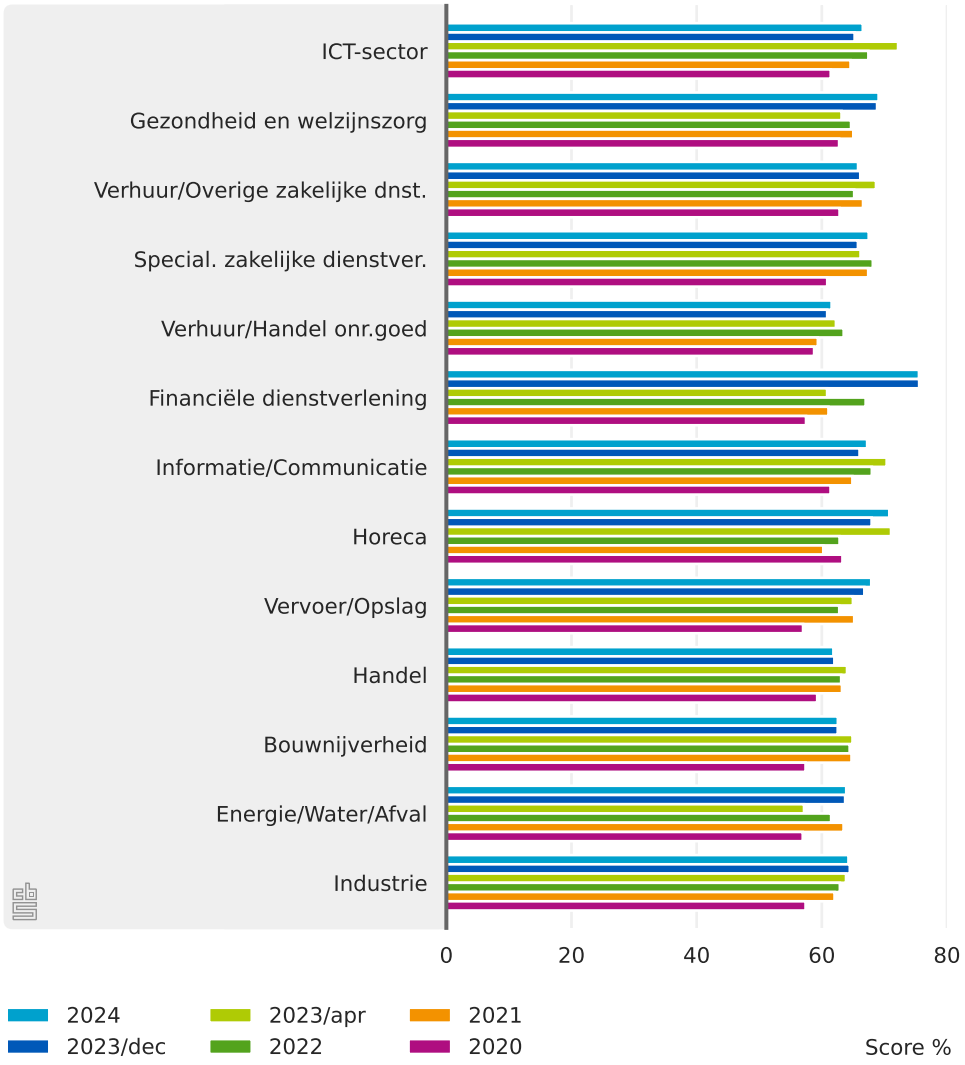
2.2.2 Gemiddelde Internet.nl-eindscore per bedrijfsgrootteklasse.

Kleinere bedrijven lopen voorop met IPv6, grote bedrijven met HSTS

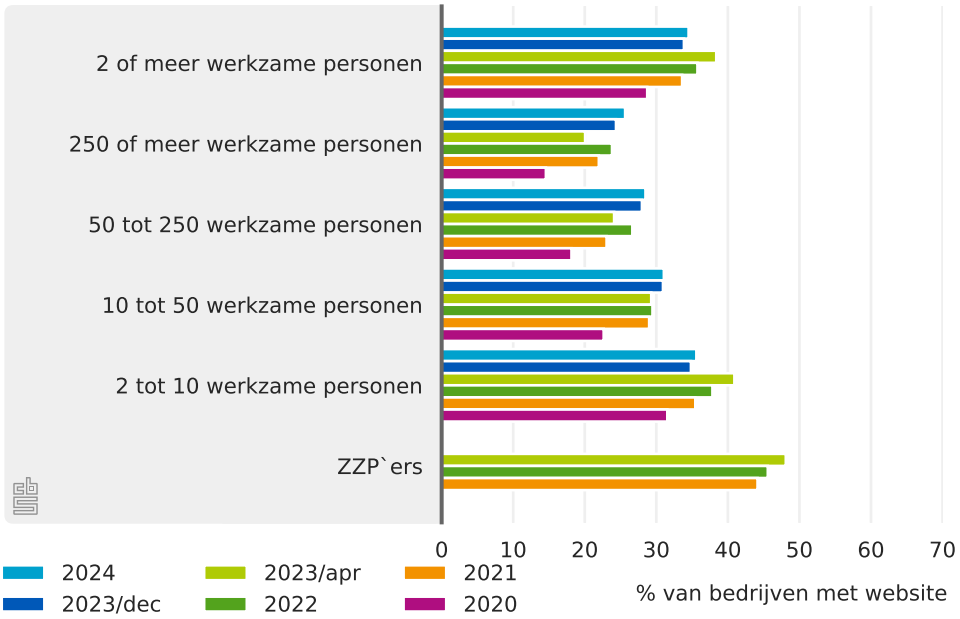
Alhoewel de eindscore vrij gelijkmatig over de verschillende bedrijfsgrootteklassen verdeeld is, vertonen de onderliggende subtesten waarop de eindscore gebaseerd is wel duidelijke verschillen afhankelijk van de bedrijfsgrootteklasse. Kleinere bedrijven hebben bijvoorbeeld vaker een website die bereikbaar is via een modern IPv6 internetadres (Figuur 2.2.4) (36 procent). IPv6 is de opvolger van IPv4, dat tegen zijn tijd aanloopt wat betreft het aantal beschikbare adressen dat dit internetprotocol aanbiedt. Ondersteunen van IPv6 is belangrijk om het internet ook in de toekomst toegankelijk te houden. Dat grote bedrijven nog niet zo hoog scoren (26 procent) komt waarschijnlijk omdat de website van grote bedrijven vaak op eigen, misschien al wat oudere servers draait. Ondersteunen van IPv6 vereist dus een behoorlijke investering terwijl het niet direct op korte termijn veel voordeel oplevert: het raakt niet aan de veiligheid van de website, alleen aan de toegankelijkheid in de toekomst.

Aan de andere kant is te zien dat grote bedrijven juist weer goed scoren op het ondersteunen van HSTS, oftewel *HTTPS Strict Transport Security* (Figuur 2.2.5). Websites met HSTS vereisen dat de webbrowser de website alleen via het beveiligde HTTPS kunnen benaderen en niet via het onveilige HTTP-protocol. Dat grote bedrijven hier weer hoger op scoren komt waarschijnlijk omdat deze instelling met de juiste kennis op netwerk niveau ingesteld kan worden en het direct de veiligheid van de website te goede komt. Bij IPv6 wordt gebruikgemaakt van de hardware van de webserver, terwijl ondersteuning van HSTS vereist dat op netwerkniveau een IT-specialist de juiste instellingen gekozen heeft. Uit eerder gepubliceerde cijfers op statline blijkt dat grote bedrijven vaker ICT-specialisten in dienst hebben (CBS, 2021d). Zie voor een volledig overzicht van alle internetstandaarden de publicatie Toepassing van Internetstandaarden voor websites van bedrijven (CBS, 2024).

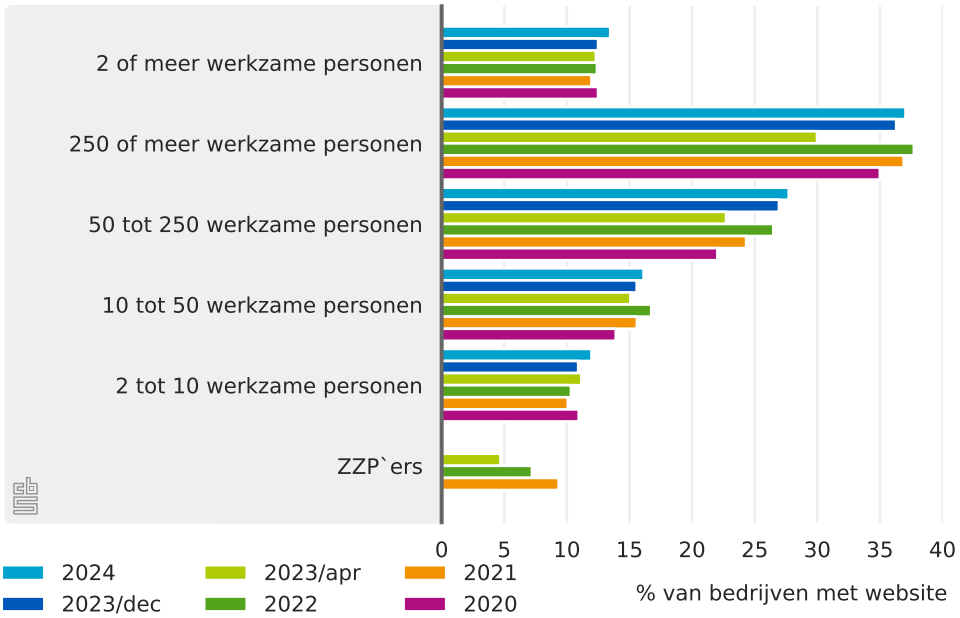
2.2.3 Gemiddelde Internet.nl-eindscore per bedrijfstak.



2.2.4 Percentage van bedrijven met een website bereikbaar via een modern internetadres (IPv6) per bedrijfsgrootteklasse.



2.2.5 Percentage van bedrijven met website die HSTS-policy aanbieden per bedrijfsgrootteklasse.



3. Cybersecurity-incidenten

In het voorgaande hoofdstuk werd gekeken naar de maatregelen die bedrijven en personen nemen om meer cyberweerbaar te worden. In dit hoofdstuk wordt ingegaan op de ICT-veiligheidsincidenten die plaatsvinden, ondanks de genomen maatregelen. Hierbij wordt onderscheid gemaakt tussen interne incidenten, die door onopzettelijk of eigen toedoen ontstaan, en incidenten ten gevolge van een aanval van buitenaf. Bij het laatste type incident wordt ook wel gesproken van 'cybercrime'. Cybercrime kan worden omschreven als 'alle delicten die gepleegd worden met behulp van ICT' (CBS, 2017f). Het gaat hierbij dus over strafbare feiten gepleegd door cybercriminelen, zoals online fraude, DDoS-aanvallen en inbraak in computers.

3.1 Bedrijven

Type ICT-veiligheidsincidenten

In de ICT-enquête onderscheiden we twee soorten ICT-veiligheidsincidenten: incidenten door eigen toedoen en incidenten als gevolg van een aanval van buitenaf. Voor beide soorten incidenten onderscheiden we drie varianten: uitval van een ICT-systeem, datavernietiging (vernietiging of verminking van elektronische gegevens) en dataonthulling (onthulling van vertrouwelijke elektronische gegevens). Hiermee komen we op zes typen ICT-veiligheidsincidenten in totaal.

Overzicht ICT-veiligheidsincidenten

De drie ICT-veiligheidsincidenten met een *interne oorzaak* zijn:

1. *Uitval van ICT-systeem* als gevolg van een ICT-gerelateerd veiligheidsincident, zoals een hardware- of softwarestoring.
2. *Datavernietiging of dataverminking* als gevolg van een ICT-gerelateerd veiligheidsincident, zoals een hardware- of softwarestoring.
3. *Dataonthulling* door onopzettelijk toedoen van eigen personeel.

De drie ICT-veiligheidsincidenten door een *aanval van buitenaf* zijn:

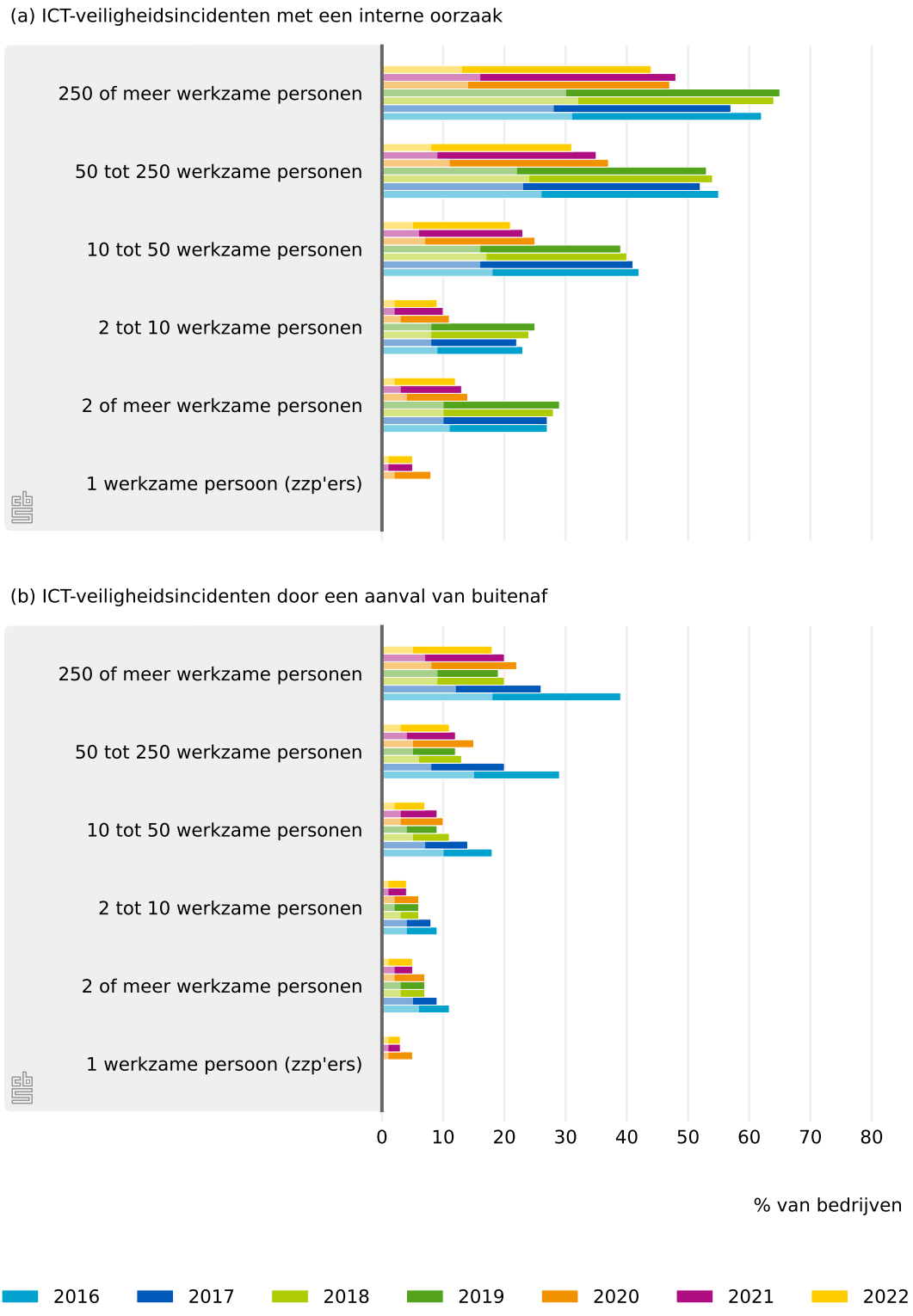
1. *Uitval van ICT-systeem* ten gevolge van een aanval van buitenaf, zoals een DDoS- of ransomwareaanval waarbij ICT-systemen niet meer gebruikt kunnen worden.
2. *Datavernietiging of dataverminking* ten gevolge van een infectie met kwaadaardige software of door ongeoorloofde elektronische toegang.
3. *Dataonthulling* door cyberinbraak, *phishing* of *pharming*. [a)]

[a)] Zie voetnoot [4)] in hoofdstuk 2 voor een toelichting van *phishing* en *pharming*.

Cybersecurityincidenten per bedrijfsgrootteklasse

In de ICT-enquête wordt aan een representatieve steekproef van bedrijven gevraagd hoe vaak ze te maken hebben gehad met elk van de eerder genoemde ICT-veiligheidsincidenten. Ook

3.1.1 ICT-veiligheidsincidenten met een interne oorzaak (a) of door een aanval van buitenaf (b) per grootteklasse.



Bron: CBS (2017e, 2018e, 2019a, 2020b, 2021e, 2022a, 2023b)

wordt gevraagd of er kosten werden gemaakt ten gevolge van de ICT-veiligheidsincidenten. Deze vragen zijn inmiddels zeven opeenvolgende jaren voorgelegd. In het volgende deel worden de resultaten eerst per bedrijfsgrootteklasse besproken. Daarna wordt gekeken naar de ontwikkeling van ICT-veiligheidsincidenten per bedrijfstak.

Grote bedrijven hebben vaker incidenten dan kleine bedrijven

In figuren 3.1.1(a) en 3.1.1(b) wordt per bedrijfsgrootteklasse het percentage van bedrijven getoond dat minstens één ICT-veiligheidsincident heeft gehad als gevolg van een interne oorzaak (a) of een aanval van buitenaf (b). Voor beide figuren worden dus de hiervoor genoemde type incidenten (uitval ICT-systeem, datavernietiging en dataonthulling) samengenomen. Het lichtgekleurde deel van de staafdiagrammen geeft het percentage bedrijven dat aangeeft dat er kosten met het ICT-incident gemoeid waren.

Grote bedrijven hebben over de jaren heen consistent meer incidenten dan kleine bedrijven. Dit geldt voor zowel interne incidenten als incidenten door een aanval van buitenaf. Voor dit patroon kunnen meerdere oorzaken zijn. Bij interne incidenten, zoals uitval van ICT-systemen door hardware of software storingen, kan meespelen dat grote bedrijven vaker een grotere en complexere ICT-infrastructuur hebben. Een groter aantal computers of meer hardware binnen een bedrijf gaat immers gepaard met een grotere kans dat er schade aan één van de systemen optreedt. Bij incidenten door een aanval van buitenaf is het daarnaast aannemelijk dat grote bedrijven interessanter zijn voor cybercriminelen. Bij grote bedrijven valt immers meer te halen en daar is de (publiciteits)schade groter. Tot slot kan meespelen dat grote bedrijven vaak meer ICT-specialisten in dienst hebben. Hierdoor kan de kans op detectie van ICT-veiligheidsincidenten groter zijn.

Aantal bedrijven met ICT-veiligheidsincidenten neemt af

In figuren 3.1.1(a) en 3.1.1(b) is te zien dat het totale aantal ICT-veiligheidsincidenten met zowel een interne oorzaak (a) als door een aanval van buitenaf (b) is afgenomen. Deze daling is zichtbaar voor bedrijven in alle bedrijfsgrootteklassen. In 2016 had bijvoorbeeld nog bijna 40 procent van de grootste bedrijven een ICT-veiligheidsincident door een aanval van buitenaf, terwijl dit in 2022 nog maar 18 procent was.

De daling van het aantal incidenten met een interne oorzaak is dit niet consistent, maar schommelt over de tijd. Voor de grootste bedrijven zien we bijvoorbeeld een toename voor de jaren 2017 – 2019, gevolgd door een afname voor de jaren 2020 – 2022. Dit kan te maken hebben met het feit dat interne incidenten niet per se te voorkomen zijn; een hardwareonderdeel kan nu eenmaal kapotgaan. De afname in 2020 is mogelijk deels te verklaren doordat de uitleg van de categorie ‘dataonthulling door eigen personeel’ is gewijzigd. Vanaf 2020 is hier namelijk uitdrukkelijk bij vermeld dat het gaat om *onopzettelijke* dataonthulling door eigen personeel, en niet om *opzettelijk* toedoen. Omdat het bij opzettelijke incidenten gaat om cybercrime, zijn dit eigenlijk incidenten die veroorzaakt worden door een aanval van buitenaf. Dit kan hebben geleid tot een afname van het aantal gerespondeerde incidenten door een interne oorzaak.

Een derde van de ICT-veiligheidsincidenten gaat gepaard met kosten

Ten slotte laten figuren 3.1.1(a) en 3.1.1(b) ook zien dat lang niet alle ICT-veiligheidsincidenten ook gepaard gaan met kosten. Dit geldt voor ICT-veiligheidsincidenten met zowel een interne oorzaak als door een aanval van buitenaf. In 2016–2019 had ongeveer de helft van de bedrijven met ten minste één ICT-veiligheidsincident ook daadwerkelijk kosten aan het incident. In 2020–2022 was dit nog maar het geval bij ongeveer een derde van de bedrijven.

Sinds 2020 wordt aan bedrijven ook gevraagd hoe hoog de kosten waren als percentage van de omzet. Deze resultaten worden later in dit hoofdstuk besproken.

Cybersecurityincidenten per bedrijfstak

Figuren 3.1.2(a) en 3.1.2(b) tonen het aandeel van bedrijven zien met ten minste één ICT-veiligheidsincident met een interne oorzaak (a) of door een aanval van buitenaf (b) per bedrijfstak voor bedrijven met twee of meer werknemers. Het lichtgekleurde deel van de staafdiagrammen geeft het percentage weer dat aangeeft dat er ook kosten aan de ICT-veiligheidsincidenten verbonden waren.

Figuur 3.1.2(a) laat zien dat ook per bedrijfstak het aandeel bedrijven met ten minste één ICT-veiligheidsincident met een interne oorzaak in de periode 2019 – 2022 behoorlijk is afgenomen. Deze trend kan mogelijk deels worden verklaard door de eerdergenoemde aanpassing in de vraagstelling. In de bedrijfstakken 'Gezondheids- en welzijnszorg' en 'Financiële dienstverlening' had een kleine 20 procent van de bedrijven in 2022 ten minste één intern ICT-veiligheidsincident. Ongeveer een vijfde van deze bedrijven gaf aan dat deze incidenten ook gepaard gingen met kosten. In de bedrijfstakken 'Industrie' en 'ICT' had respectievelijk 13 en 15 procent van de bedrijven een intern ICT-veiligheidsincident. In de bedrijfstak 'Horeca' traden de ICT-veiligheidsincidenten het minst vaak op: in 2022 had ongeveer 9 procent van de horecabedrijven ten minste één ICT-veiligheidsincident met een interne oorzaak. Op zich is dit niet vreemd, omdat de mate van digitalisering in de horeca lager is vergeleken met andere bedrijfstakken (CBS, 2021d). Hierdoor is de kans op uitval door een hardware- of softwarestoring ook kleiner.

Figuur 3.1.2(b) toont tot slot dat het aandeel van bedrijven dat ten minste één ICT-veiligheidsincident door een aanval van buitenaf meldt vanaf 2019 is afgenomen. Hoewel er van jaar op jaar soms een kleine stijging te zien is, is er over het algemeen sprake van een dalende trend. Dit geldt voor zowel het totale aantal ICT-veiligheidsincidenten als het aandeel dat gepaard ging met kosten.

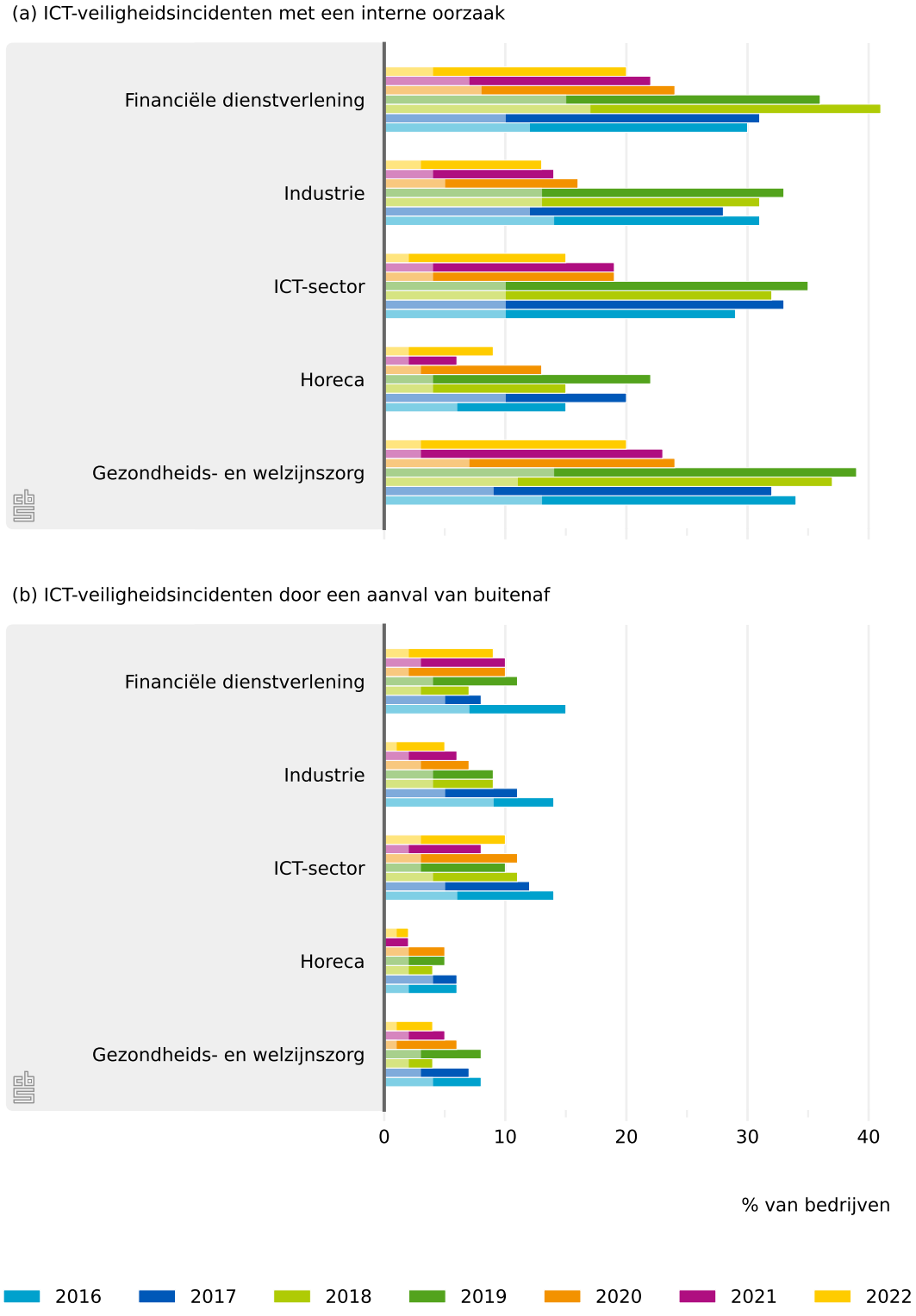
Cybersecurityincidenten per type incident

In dit deel bekijken we de bijdragen van de drie afzonderlijke type ICT-veiligheidsincidenten: uitval van ICT-systemen, datavernietiging en dataonthulling.

Cybersecurityincidenten per type incident per bedrijfsgrootteklasse

Figuur 3.1.3 toont per bedrijfsgrootteklasse het percentage van bedrijven dat ten minste één uitval van een ICT-systeem, datavernietiging, of dataonthulling had als gevolg van een interne oorzaak (a1, b1, c1) of een aanval van buitenaf (a2, b2, c2).

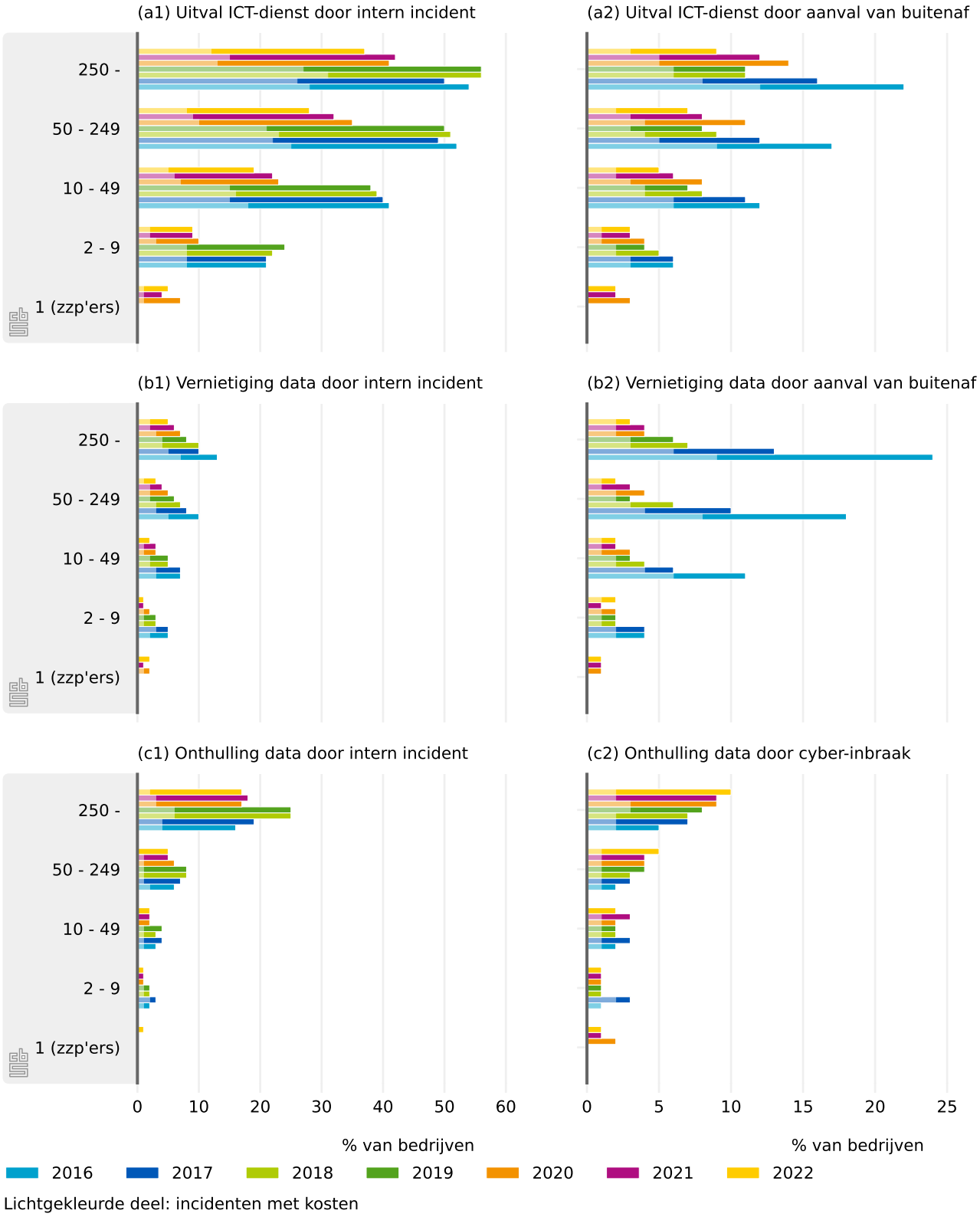
3.1.2 ICT-veiligheidsincidenten met een interne oorzaak (a) of door een aanval van buitenaf (b) per bedrijfstak voor bedrijven met 2 of meer werknemers.



Lichtgekleurde deel: incidenten met kosten

Bron: CBS (2017e, 2018e, 2019a, 2020b, 2021e, 2022a, 2023b)

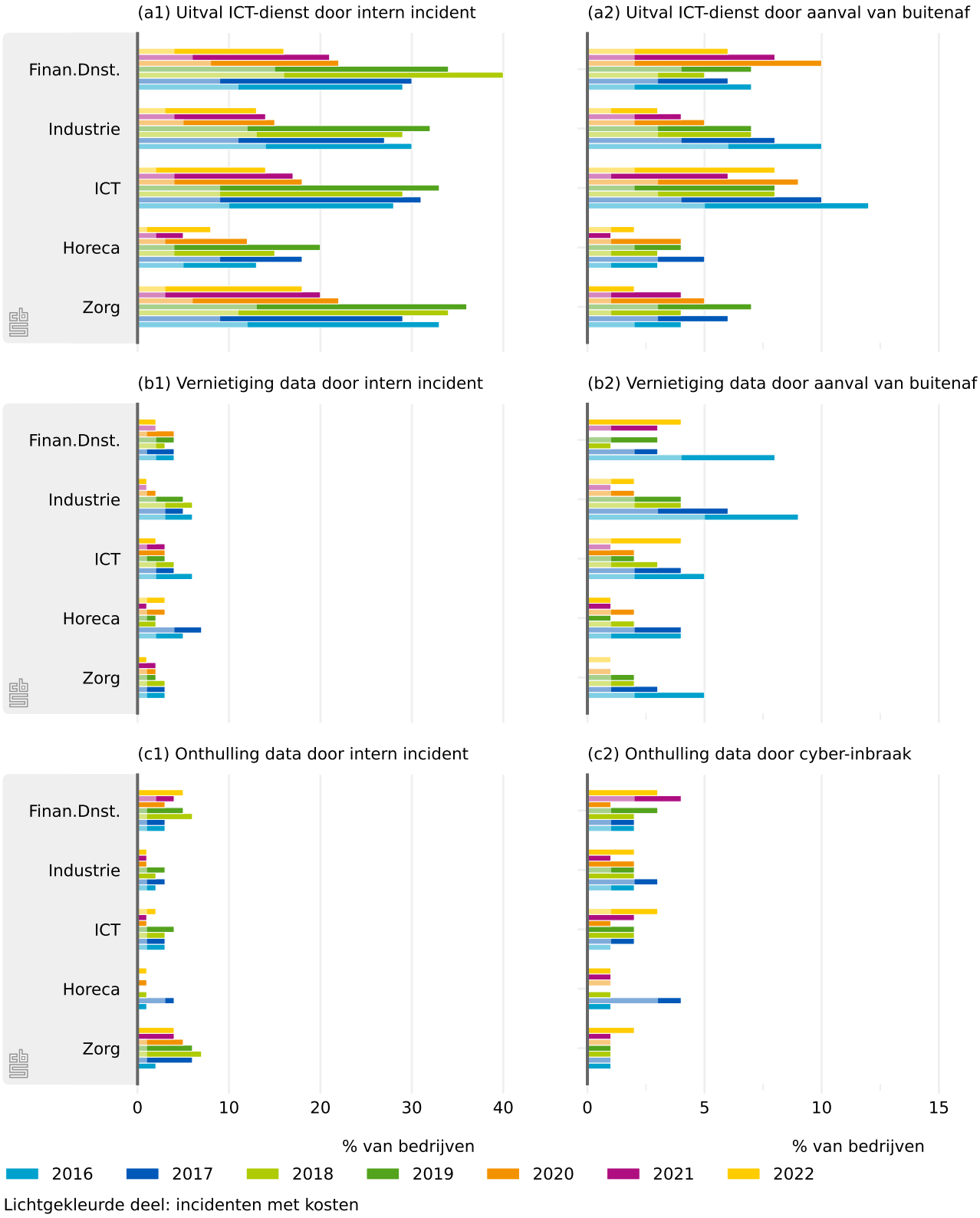
3.1.3 ICT-veiligheidsincidenten per categorie per grootteklasse.



Lichtgekleurde deel: incidenten met kosten

Bron: CBS (2017e, 2018e, 2019a, 2020b, 2021e, 2022a, 2023b)

3.1.4 ICT-veiligheidsincidenten per categorie per bedrijfstak.



Lichtgekleurde deel: incidenten met kosten

Bron: CBS (2017e, 2018e, 2019a, 2020b, 2021e, 2022a, 2023b)

Tot nu toe zagen we dat het aandeel van bedrijven met een ICT-veiligheidsincident als gevolg van een interne oorzaak toeneemt met de bedrijfsgrootteklasse. Figuur 3.1.3(a1) laat nu zien dat deze toename voornamelijk is toe te schrijven aan de uitval van een ICT-systeem door een hardware- of softwarestoring. Van de bedrijven met 2 tot 10 werkzame personen had bijvoorbeeld 9 procent in 2022 ten minste één uitval door een storing, terwijl dit voor bedrijven met meer dan 250 werkzame personen 37 procent was. De overige twee incidenten, zoals getoond in de figuren 3.1.3(b1, c1), kwamen ook vaker voor bij grote bedrijven. Maar omdat deze incidenten minder vaak voorkwamen, droegen ze minder bij aan het totaal van interne incidenten.

Ook in de onderliggende categorieën van incidenten is de daling van het aantal bedrijven met ten minste één intern ICT-veiligheidsincident grotendeels zichtbaar. De ontwikkeling over de tijd per incident is echter minder eenduidig. Bijvoorbeeld, tot aan 2019 was er een toename te zien in dataonthulling als gevolg van interne incidenten bij grote bedrijven met 250 of meer werknemers, zoals weergegeven in figuur 3.1.3(c1), terwijl er vanaf 2020 weer een afname te zien is. Een vergelijkbaar patroon is waarneembaar voor de uitval van ICT-systemen, zoals weergegeven in figuur 3.1.3(a1). Deze trends wijken dus af van de ontwikkeling van het totale aantal interne incidenten.

Figuren 3.1.3(a2, b2, c2) laten verder zien dat alle typen incidenten als gevolg van een aanval van buitenaf vaker voorkomen bij grote bedrijven dan bij kleine bedrijven. Dit komt ook overeen met het eerder beschreven patroon voor het totaal van incidenten door een aanval van buitenaf. Tot slot zagen we eerder dat er sprake was van een afname van het aandeel bedrijven met ten minste één ICT-veiligheidsincident door een aanval van buitenaf. In figuren 3.1.3(a2, b2, c2) is nu te zien dat deze afname vooral toe te schrijven is aan de afname van het aandeel bedrijven met een uitval van een ICT-systeem en datavernietiging door een aanval van buitenaf. Het aandeel bedrijven dat een dataonthulling als gevolg van een cyberinbraak meldt, is juist toegenomen over de afgelopen jaren. De ontwikkelingen variëren dus sterk naar het type incident.

Cybersecurityincidenten per type incident per bedrijfstak

Figuur 3.1.4 laat per bedrijfstak het percentage van bedrijven zien dat ten minste één uitval van een ICT-systeem, datavernietiging, of dataonthulling had als gevolg van een interne oorzaak (a1, b1, c1) of een aanval van buitenaf (a2, b2, c2). Net zoals bij de afname van ICT-veiligheidsincidenten per bedrijfsgrootteklasse, zien we voor bijna alle bedrijfstakken een afname van het percentage bedrijven dat een ICT-veiligheidsincident met een interne oorzaak en door een aanval van buitenaf meldt. Opvallend genoeg geldt dit in 2022 ten opzichte van 2016 niet voor de bedrijfstakken ‘Financiële diensten’ en ‘Zorg’; we zien bij dataonthulling door een intern incident een toename, zoals getoond in figuur 3.1.4(c1). Ook zien we bij bijna alle bedrijfstakken dat het aandeel bedrijven dat een dataonthulling als gevolg van een cyberinbraak meldt, is toegenomen.

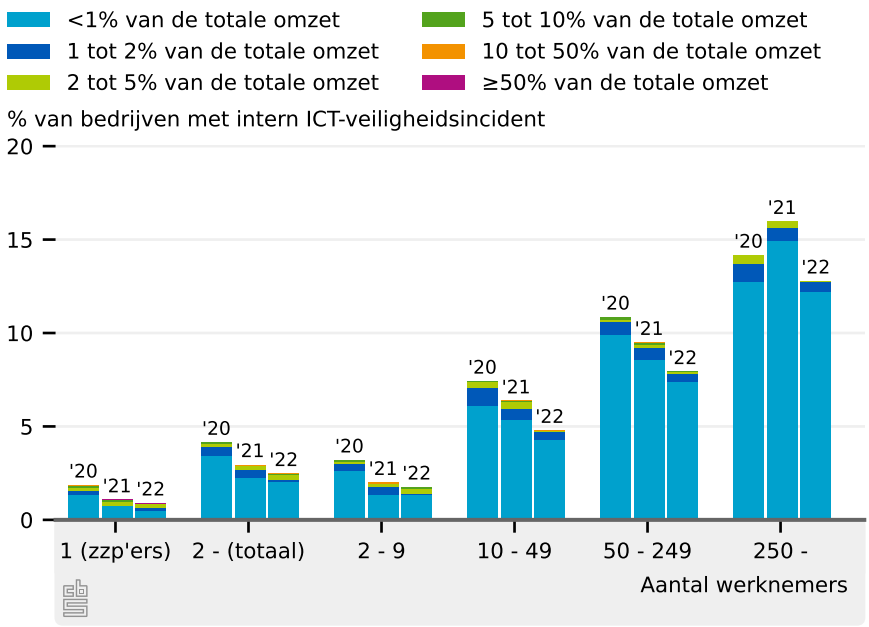
Kostenverdeling van de ICT-veiligheidsincidenten

Kostenverdeling van ICT-veiligheidsincidenten met interne oorzaak

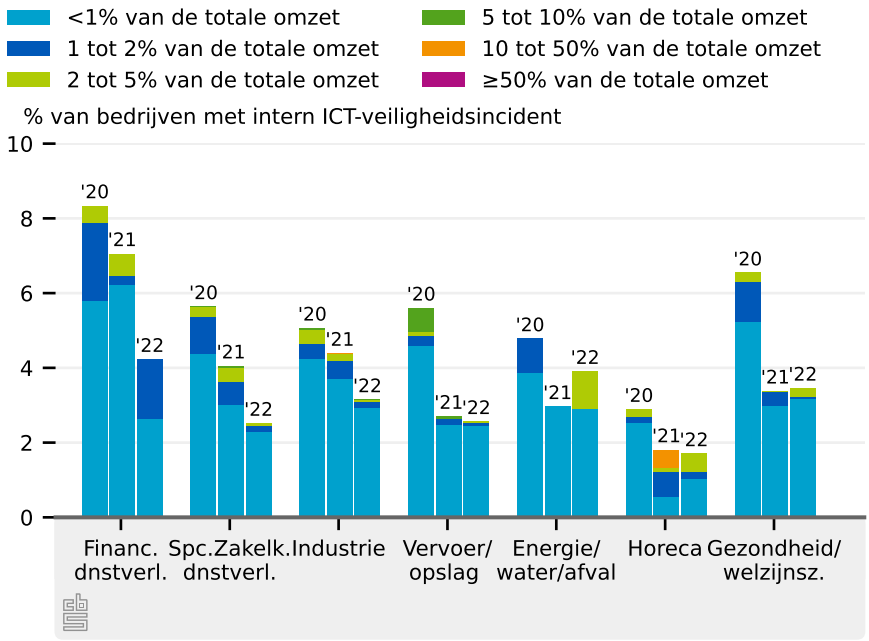
Figuren 3.1.5(a) en 3.1.5(b) laten per bedrijfsgrootteklasse (a) en bedrijfstak (b) de hoogte van de kosten van de interne ICT-veiligheidsincidenten zien als percentage van de omzet. De

3.1.5 Percentage van bedrijven per grootteklasse (a) en bedrijfstak met 2 of meer werknemers (b) die kosten hadden na een intern ICT-veiligheidsincident, uitgesplitst naar de hoogte van de kosten als percentage van de omzet.

(a) Grootteklasse



(b) Bedrijfstak



Bron: CBS (2021e, 2022a, 2023b)

hoogte van de samengestelde staafjes geeft het percentage weer van de bedrijven die kosten hadden aan een intern ICT-veiligheidsincident. De staafjes komen dus overeen met de hoogte van de lichtgekleurde delen van de staafjes in de figuren 3.1.1(b) en 3.1.2(b). Met kleur is aangegeven hoe hoog de kosten waren als percentage van de totale omzet van het bedrijf. De percentages zijn opgedeeld in zes categorieën: 'Minder dan 1%', '1 tot 2%', '2 tot 5%', '5 tot 10%', '10 tot 50%', of '50% of meer'.

Uit figuur 3.1.5(a) blijkt dat in 2022 in de meeste gevallen de kosten minder dan 1 procent van de bedrijfsomzet bedroegen. Bij een klein deel van de bedrijven waren de kosten meer dan 1 procent van de omzet. In 2022 meldde bijvoorbeeld 0,1 procent van de kleine bedrijven (2 tot 10 werknemers) met ten minste één ICT-veiligheidsincident dat de kosten tussen 5 tot 10 procent van de totale omzet waren. Bij deze bedrijven moeten de incidenten dus een behoorlijk grote impact hebben gehad.

Figuur 3.1.5(b) laat daarnaast zien dat het aandeel bedrijven met kosten aan een intern ICT-veiligheidsincident in de bedrijfstak 'Financiële dienstverlening' flink is gedaald. Toch waren er in deze bedrijfstak alsnog relatief veel bedrijven waarbij de kosten hoger waren dan één procent van de bedrijfsomzet. In de bedrijfstak 'Energie/water/afval' steeg het aandeel bedrijven met kosten aan een intern ICT-veiligheidsincident juist behoorlijk, met name waar de kosten tussen de 2 en 5 procent van de totale omzet waren. In de horeca bleef het aandeel met kosten in 2022 ongeveer gelijk, maar daalde de hoogte van de kosten als percentage van de bedrijfsomzet.

Kostenverdeling van ICT-veiligheidsincidenten door aanval van buitenaf

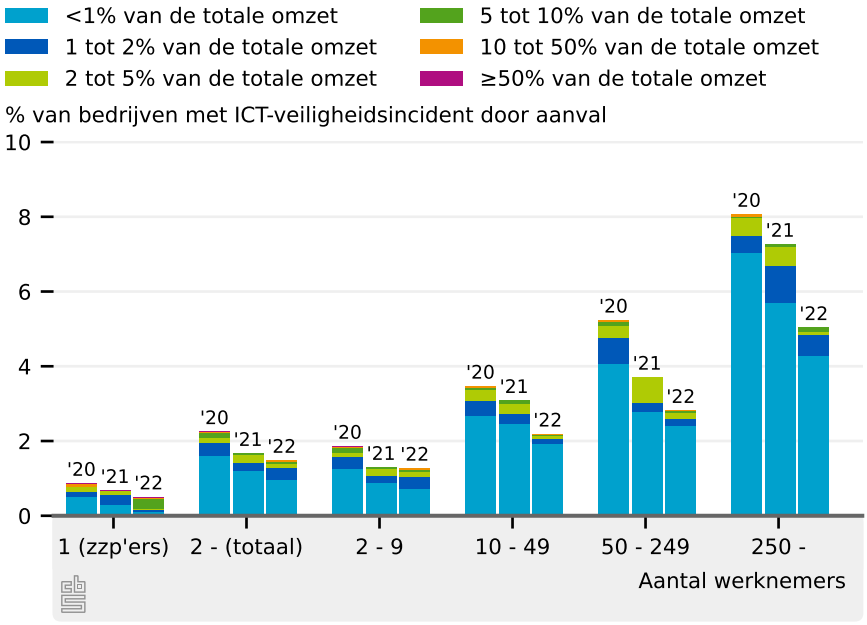
Figuren 3.1.6(a) en 3.1.6(b) laten per bedrijfsgrootteklasse (a) en bedrijfstak (b) de hoogte zien van de kosten van de ICT-veiligheidsincidenten als gevolg van een aanval van buitenaf als percentage van de omzet. De hoogte van de samengestelde staafjes geeft het percentage weer van de bedrijven die kosten hadden aan een ICT-veiligheidsincident van buitenaf. De staafjes komen dus overeen met de hoogte van de lichtgekleurde delen van de staafjes in de figuren 3.1.1(a) en 3.1.2(a). Met kleur is weer aangegeven hoe hoog de kosten waren als percentage van de totale omzet van het bedrijf.

Ook in deze figuren is te zien dat het aandeel bedrijven met kosten aan een ICT-veiligheidsincident door een aanval van buitenaf in 2022 is afgenomen. In de meeste gevallen bedroegen de kosten minder dan 1 procent van de omzet van het bedrijf. Bij een klein deel van de bedrijven waren de kosten meer dan 1 procent van de omzet. Figuur 3.1.6(b) laat echter zien dat, in tegenstelling tot het voorgaande jaar, er in 2022 wel bedrijven waren waarbij de hoogte van de kosten tussen de 10 en 50 procent van de bedrijfsomzet was. Dit was relatief vaak het geval in de bedrijfstak 'Energie/water/afval'. In deze bedrijfstak moeten de ICT-veiligheidsincidenten dus een behoorlijke impact hebben gehad.

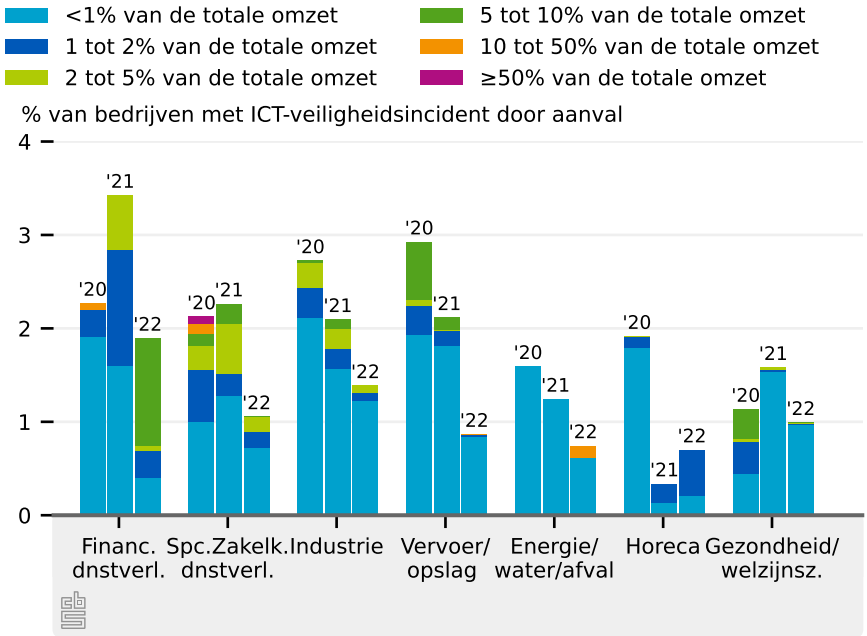
Het aandeel met kosten aan een incident door een aanval van buitenaf is het meest afgenomen in de bedrijfstak 'Financiële dienstverlening'. De hoogte van de kosten als percentage van de totale omzet is in deze bedrijfstak juist wel behoorlijk gestegen: bij een groot gedeelte van de bedrijven in deze bedrijfstak bedroegen de kosten maar liefst 5 tot 10 procent van de totale bedrijfsomzet.

3.1.6 Percentage van bedrijven per grootteklasse (a) en bedrijfstak met 2 of meer werknemers (b) die kosten hadden na een ICT-veiligheidsincident door een aanval van buiten, uitgesplitst naar de hoogte van de kosten als percentage van de omzet.

(a) Grootteklasse



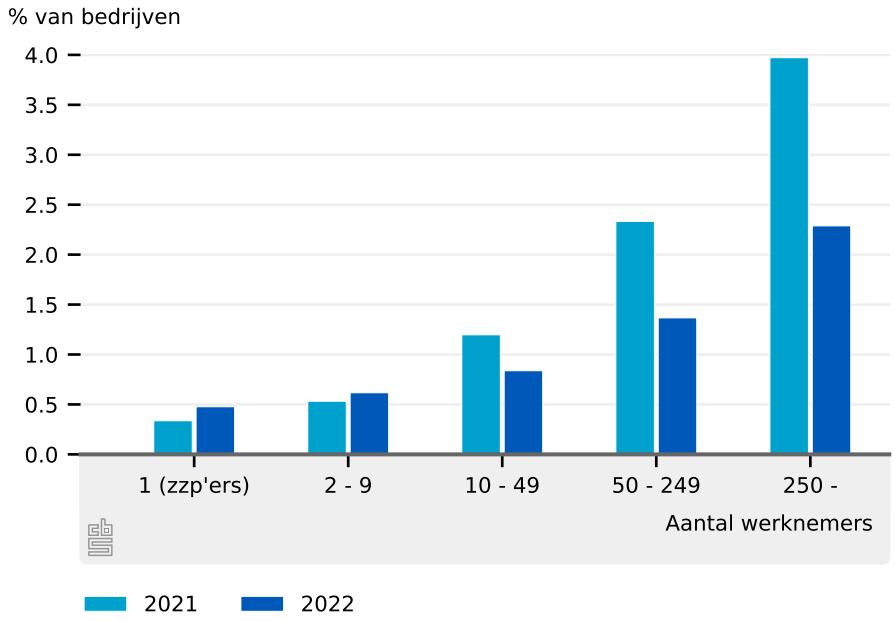
(b) Bedrijfstak



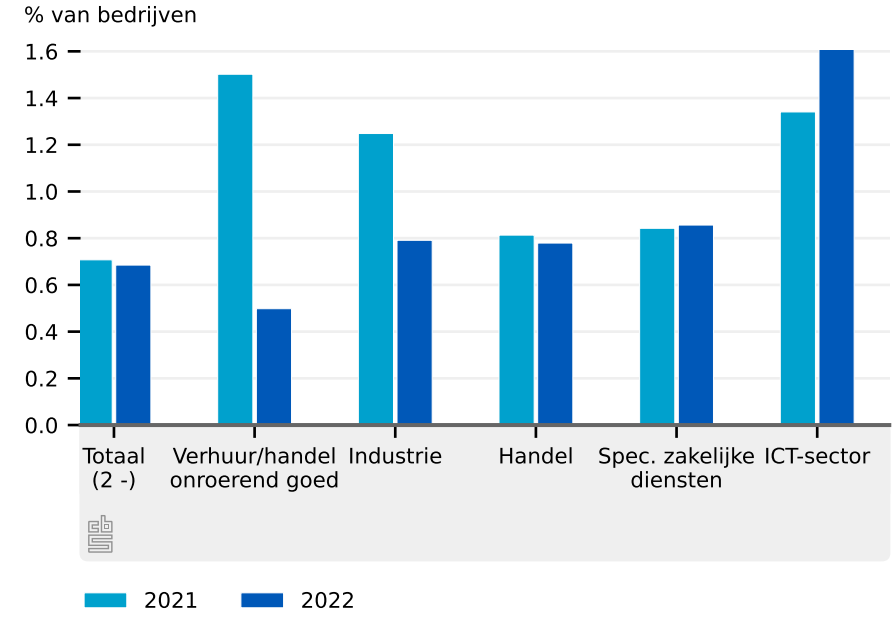
Bron: CBS (2021e, 2022a, 2023b)

3.1.7 Percentage van bedrijven die een ransomwareaanval gehad hebben per bedrijfsgrootteklasse.

(a) Grootteklasse



(b) Bedrijfstak



Bron: CBS (2022a)

3.1.8 Aantal ransomwareaanvallen in 2022 per grootteklasse en het percentage per groep.

Bedrijfsgrootte	Ransomwareaanval gehad	
	Aantal	Percentage
1 werkzame persoon (zzp'er)	6 000	0,5
Totaal (2 of meer werkzame personen)	2 310	0,7
2 tot 10 werkzame personen	1 700	0,6
10 tot 50 werkzame personen	410	0,8
50 tot 250 werkzame personen	140	1,4
250 of meer werkzame personen	60	2,3

Ransomwareaanvallen

Sinds 2021 wordt er in de ICT-enquête ook specifiek gevraagd naar ransomwareaanvallen (CBS, 2022a, 2023b). Bij een ransomwareaanval worden de ICT-systemen van een bedrijf of particulier door middel van malware geblokkeerd, om zo het slachtoffer te chanteren om losgeld ('ransom') te betalen om de systemen weer vrij te geven. Ransomware wordt door de Nationaal Coördinator Terrorismebestrijding en Veiligheid als een belangrijk risico voor de nationale veiligheid gezien (NCTV, 2023). Het is daarom belangrijk om te monitoren hoe vaak dit voorkomt bij bedrijven in Nederland.

Aantal ransomwareaanvallen

In 2022 vonden er in totaal 8 310 ransomwareaanvallen plaats bij bedrijven (zie Tabel 3.1.8). Hiervan kwamen er 6 000 voor bij zzp'ers en 2 310 bij bedrijven met twee of meer werkzame personen. Tabel 3.1.8 geeft naast de absolute getallen ook het percentage van bedrijven per grootteklasse weer dat meldt een ransomwareaanval gehad te hebben. Hieruit blijkt dat procentueel gezien grote bedrijven meer last hebben van ransomwareaanvallen dan kleine bedrijven.

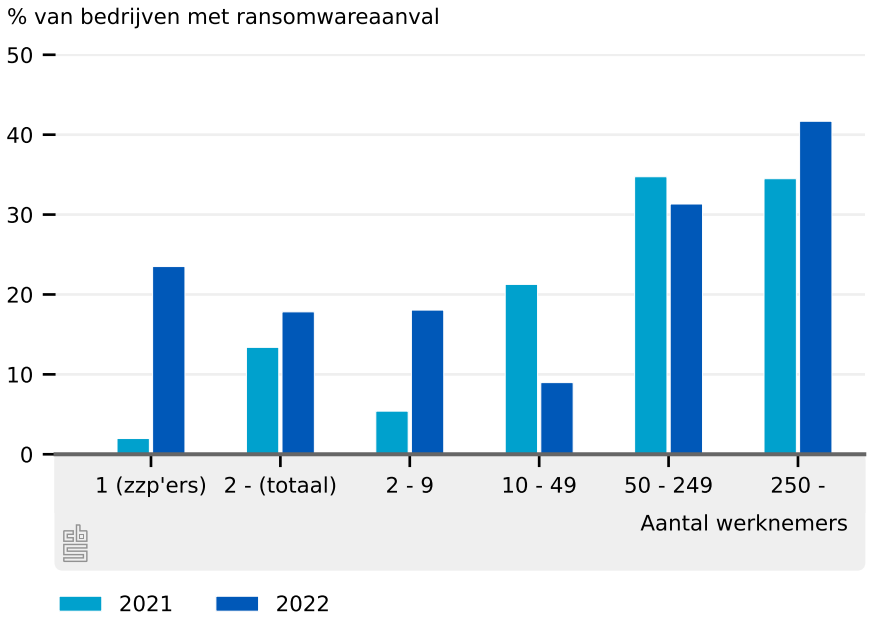
Figuren 3.1.7(a) en 3.1.7b(b) tonen respectievelijk de percentages van bedrijven met een ransomwareaanval per grootteklasse en bedrijfstak voor bedrijven met twee of meer werknemers. Uit figuur 3.1.7(a) blijkt dat zzp'ers en microbedrijven (2 tot 10 werknemers) in 2022 iets vaker te maken kregen met een ransomwareaanval dan in 2021. Bij grotere bedrijven met 10 of meer werknemers is er juist een afname te zien van het ransomwareaanvallen tussen 2021 en 2022. Figuur 3.1.7(b) laat daarnaast zien dat bedrijven in de ICT-sector het vaakst werden getroffen door een ransomwareaanval. Ransomwareaanvallen kwamen hier iets vaker voor dan in 2021. In de bedrijfstakken 'Verhuur/handel onroerend goed' en 'Industrie' daalde het aandeel bedrijven met een ransomwareaanval juist aanzienlijk ten opzichte van een jaar eerder. Een overzicht van alle cijfers is terug te vinden op Statline (CBS, 2023b).

Hulpvraag bij politie en cybersecuritybedrijven

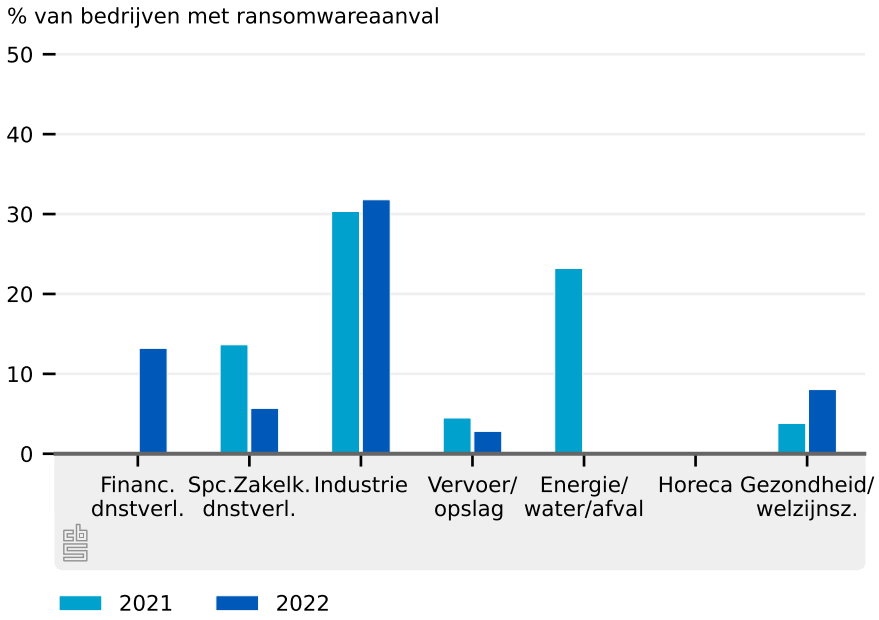
Figuren 3.1.9 en 3.1.10 tonen het percentage van de bedrijven die een ransomwareaanval hadden en als gevolg daarvan hulp hebben gevraagd van respectievelijk de politie of een

3.1.9 Percentage van bedrijven met ransomwareaanval die de hulp hebben in geschakeld van de politie per grootteklasse (a) en bedrijfstak met 2 of meer werknemers (b).

(a) Grootteklasse



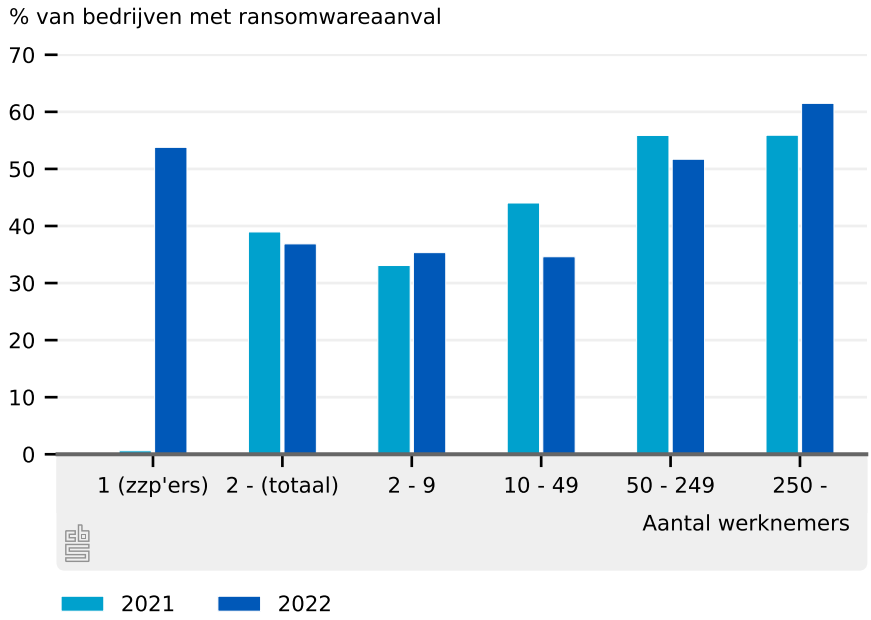
(b) Bedrijfstak



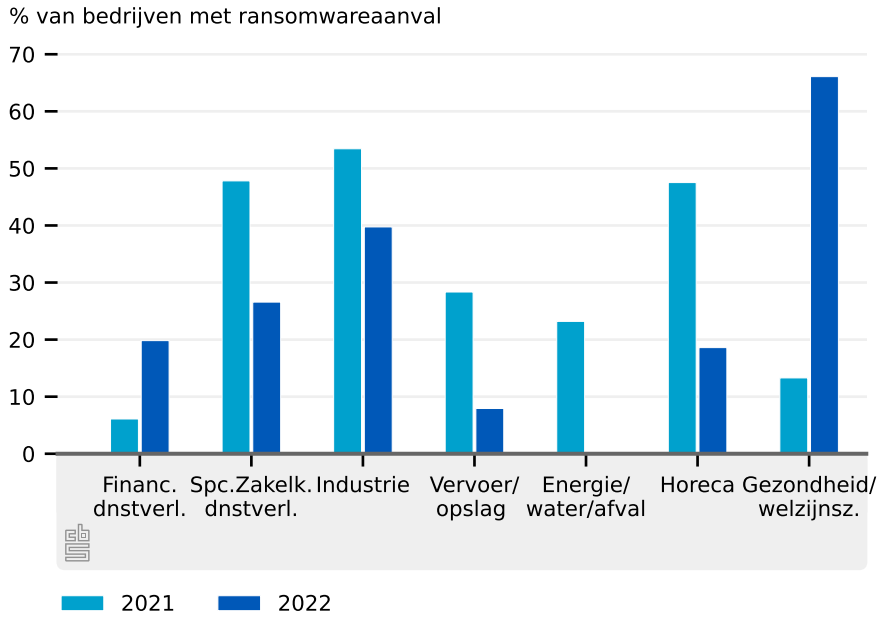
Bron: CBS (2022a, 2023b)

3.1.10 Percentage van bedrijven met ransomwareaanval die de hulp hebben in geschakeld van een cybersecuritybedrijf per grootteklasse (a) en bedrijfstak met 2 of meer werknemers (b).

(a) Grootteklasse



(b) Bedrijfstak



Bron: CBS (2022a, 2023b)

cybersecuritybedrijf. Van alle bedrijven met twee of meer werknemers die een ransomwareaanval gehad hebben schakelde 37 procent in 2022 de hulp in van een cybersecuritybedrijf. Een kleiner aandeel stapte naar de politie (18 procent). Het is hierbij uiteraard mogelijk dat een bedrijf hulp inschakelde van zowel de politie als een cybersecuritybedrijf. Opvallend is wel dat kleinere bedrijven minder vaak de hulp inschakelden van de politie en/of een cybersecuritybedrijf dan grotere bedrijven. Van de microbedrijven (2 tot 10 werkzame personen) stapte bijvoorbeeld 18 procent naar de politie, tegenover 42 procent van de grote bedrijven (250 of meer werkzame personen). Figuur 3.1.9(b) laat tot slot zien dat er ook verschillen waren tussen bedrijfstakken. In de bedrijfstak 'Gezondheids- en welzijnszorg' werd bijvoorbeeld veel vaker de hulp ingeschakeld van een cybersecuritybedrijf (66 procent) dan de politie (8 procent), terwijl in de bedrijfstak 'Industrie' respectievelijk 40 en 31 procent van de bedrijven naar een cybersecuritybedrijf of de politie stapte.

Grote bedrijven vaker verzekerd tegen ICT-veiligheidsincidenten

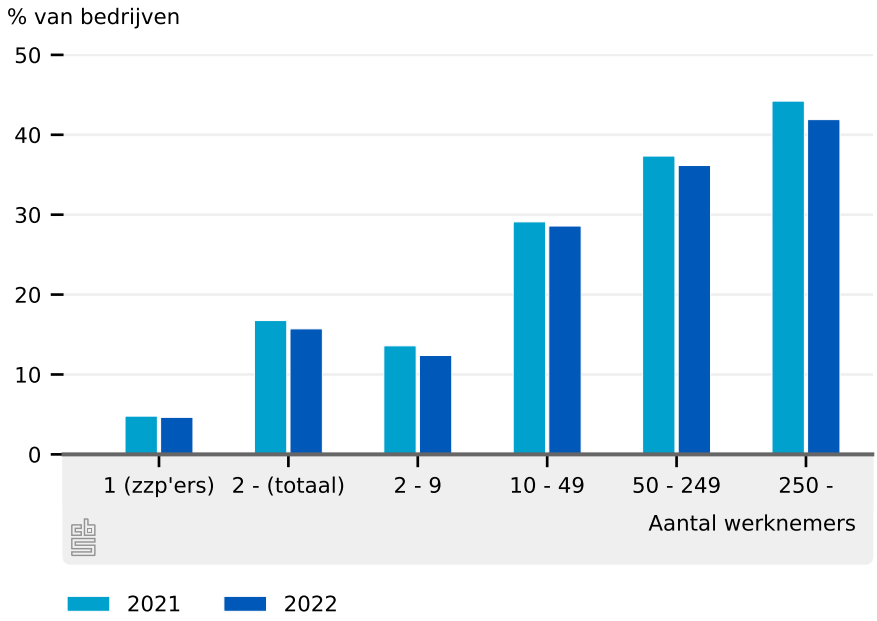
Figuren 3.1.11(a) en 3.1.11(b) laten tot slot zien hoeveel bedrijven per grootteklasse (a) en bedrijfstak (b) een verzekering tegen ICT-veiligheidsincidenten afgesloten hebben. Van alle bedrijven met twee of meer werknemers was 16 procent in 2022 verzekerd tegen ICT-veiligheidsincidenten. Grotere bedrijven waren vaker verzekerd dan kleinere bedrijven. Van de zzp'ers was bijvoorbeeld slechts 5 procent verzekerd, terwijl van de bedrijven met 250 of meer werknemers zo'n 42 procent verzekerd was. Uit figuur 3.1.11(b) blijkt dat de hoogste percentages van verzekerde bedrijven te vinden zijn bij de financiële sector, de gezondheidszorg en de energiesector.

DDoS-aanvallen

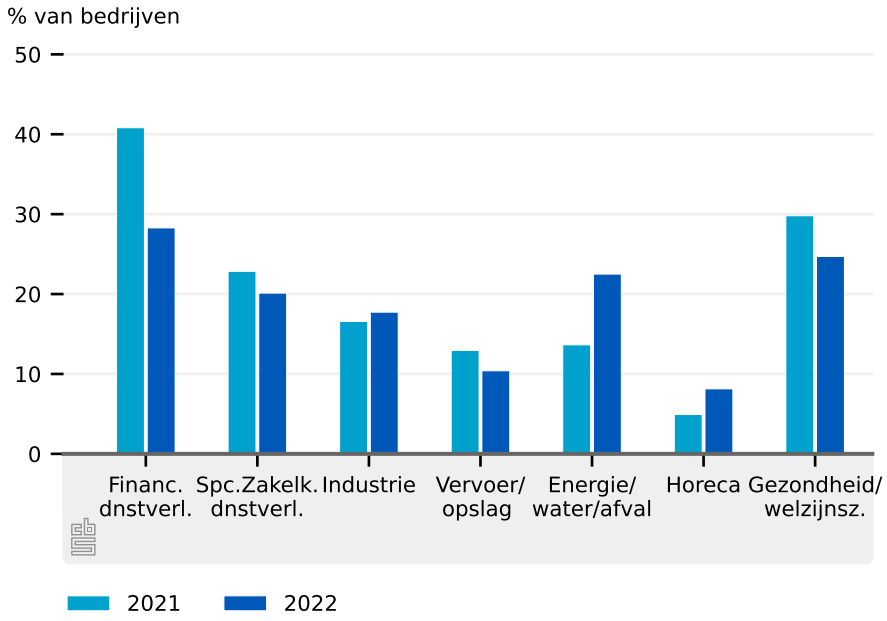
Bij de Nationale anti-DDoS-Wasstraat (NaWas) werden in 2023 2 148 DDoS-aanvallen (Distributed Denial of Service aanvallen) geteld. Het gaat hier om aanvallen waarbij een aanvallende partij een server tijdelijk of langdurig onbeschikbaar probeert te maken door deze vanaf meerdere kanten te overspoelen met aanvragen. Dit zijn er meer dan in 2022 toen er 2 001 werden geteld, maar minder dan 2021 waarin het er 2 830 waren (NBIP, 2023a). Bij de NaWas zijn rond de 100 deelnemers aangesloten, waaronder voornamelijk internetproviders. Figuur 3.1.12(a) geeft het aantal DDoS-aanvallen zoals per kwartaal door de NaWas gemeten is; figuur 3.1.12(b) geeft het aantal intensieve DDoS-aanvallen met een duur van langer dan 4 uur. De aanvallen richten zich vooral op nationale veiligheidsdiensten, ziekenhuizen, de gezondheidszorg en andere kritieke infrastructuur. De meeste aanvallen vonden plaats in het eerste kwartaal (676) terwijl het aantal aanvallen in de andere kwartalen onder de 600 bleef en in het tweede kwartaal waren er slechts 408 aanvallen. Daarentegen vonden in het tweede en derde kwartaal wel de heftigste aanvallen plaats. Respectievelijk 36 en 39 aanvallen duurden in het tweede en derde kwartaal langer dan 4 uur. In zowel het eerste en vierde kwartaal waren dit er minder dan 30. Ook vond in het tweede kwartaal de krachtigste aanval plaats met een capaciteit van 381 Gbps, even groot als de heftigste aanval in het jaar 2022.

3.1.11 Percentage van bedrijven die een verzekering voor ICT-veiligheidsincidenten hebben per grootteklasse (a) en bedrijfstak met 2 of meer werknemers (b).

(a) Grootteklasse



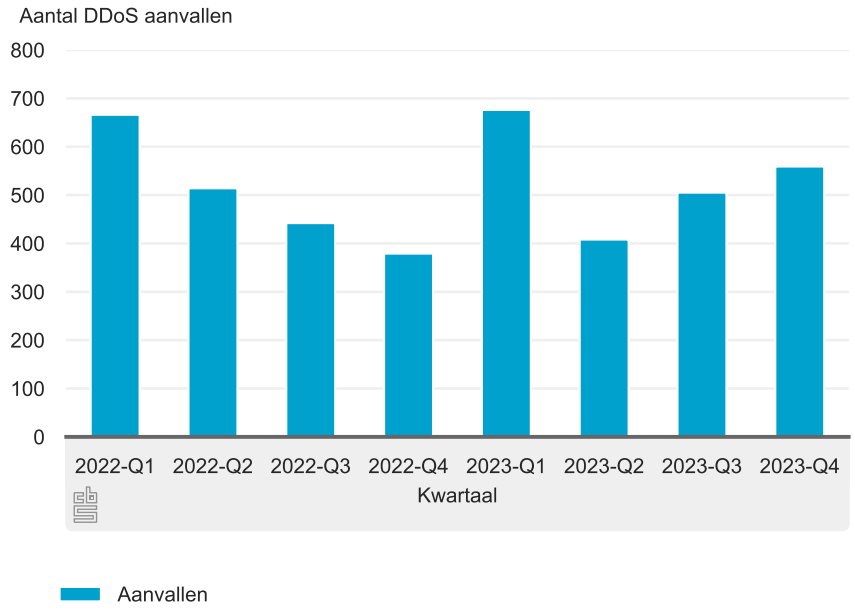
(b) Bedrijfstak



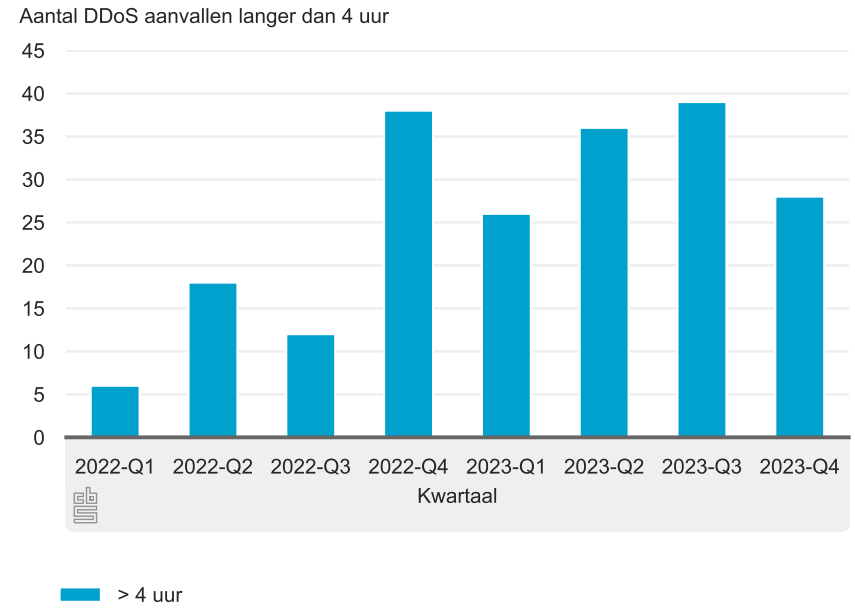
Bron: CBS (2022a)

3.1.12 Aantal DDoS-aanvallen per kwartaal[1)]

(a) Aantal aanvallen



(b) Aantal aanvallen langer dan 4 uur



Bron: NBIP (2023b)

[1)] Van de bij NaWas aangesloten organisaties.

4. Cybercrime

In dit hoofdstuk worden enkele cijfers beschreven over online criminaliteit. Ook wordt ingegaan op de sancties en/of straffen die worden opgelegd voor het plegen van een specifieke vorm van cybercrime, namelijk computervredebreuk.

Cybercrime

Cybercrime zijn alle delicten die gepleegd worden met behulp van ICT. Cybercrime omvat criminaliteit die gericht is op een ICT-systeem of de informatie die door ICT wordt verwerkt. Cybercrime omvat ook de al langer bestaande criminaliteit die door ICT een nieuwe impuls heeft gekregen, zoals oplichting en verspreiding van kinderporno via internet. Deze definitie is een samenvoeging van de enge definitie van cybercrime die het Nationaal Cyber Security Centrum en de politie hanteren, en de categorie 'gedigitaliseerde criminaliteit' die de politie ook onderscheidt.

Om goed aan te sluiten bij actuele ontwikkelingen op het gebied van online criminaliteit zijn de vragen over online criminaliteit in de Veiligheidsmonitor in 2021 grondig herzien. Ook de onderzoeksopzet is gewijzigd. Hierdoor zijn de uitkomsten van 2021 niet meer vergelijkbaar met die van voorgaande edities.

4.1 Online criminaliteit

Onder online criminaliteit worden delicten en incidenten geschaard die via internet, e-mail of app plaatsvinden. Het betreft strafbare feiten in de sfeer van oplichting en fraude (aan- en verkoopfraude, fraude betalingsverkeer, ID-fraude, phishing), computervredebreuk (hacken) en om incidenten in de interpersoonlijke sfeer die niet altijd strafbaar zijn zoals bedreigingen, pesten, stalken en shame sexting[1)]).

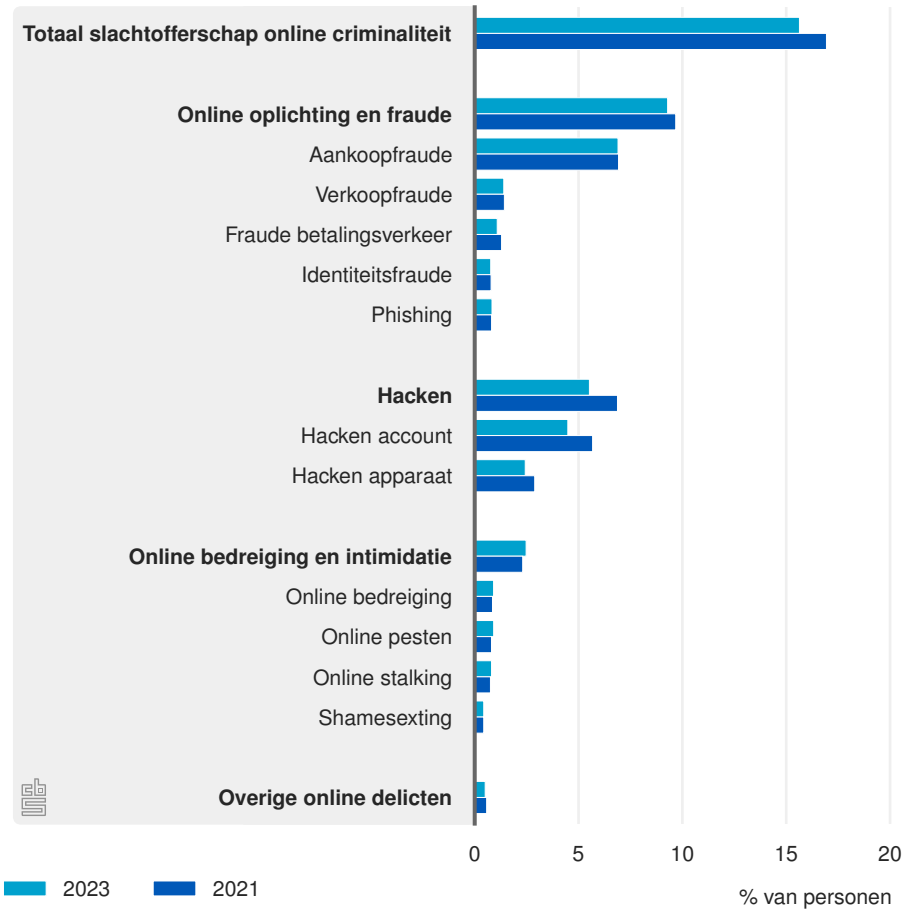
Slachtofferschap online criminaliteit afgenomen

Het slachtofferschap van online criminaliteit is sinds 2021 met 8 procent afgenomen, van 16,9 procent van alle personen ouder 15 jaar naar 15,6 procent (figuur 4.1.1). Van de onderscheiden vormen van online criminaliteit nam het slachtofferschap van hacken het sterkst af, en dan met name het hacken van een account. Het percentage slachtoffers van online oplichting en fraude en van online bedreiging en intimidatie is de afgelopen 2 jaar vrij stabiel gebleven.

In 2023 was 16 procent van de bevolking van 15 jaar en ouder, slachtoffer van een of meer online delicten of incidenten. Jongeren waren vaker slachtoffer dan ouderen. In 2023 is 18 procent van de 15- tot 25-jarigen slachtoffer geweest van online criminaliteit, van de 65-plussers 11 procent. Vooral met online bedreiging en intimidatie hebben jongeren vaker te maken dan ouderen. Ook van hacken zijn ze vaker slachtoffer. Van aankoopfraude en fraude in het betalingsverkeer werden 25- tot 65-jarigen juist het vaakst slachtoffer. Phishing treft de 65-plussers het vaakst. Van alle slachtoffers van online criminaliteit deed 17 procent aangifte bij de politie. De cijfers per leeftijdscategorie worden niet in de figuur gegeven, maar zijn op

1) Het ongevraagd doorsturen van seksueel getinte beelden met als doel de afgebeelde persoon aan de schandpaal te nagelen.

4.1.1 Slachtofferschap online criminaliteit voor alle personen van 15 en ouder[1)]



1) De cijfers zijn gebaseerd op de Veiligheidsmonitor nieuwe stijl

Statline terug te vinden (CBS, 2023a). Meer cijfers over online criminaliteit zijn te vinden in de Veiligheidsmonitor 2023 (CBS, 2023i) van het CBS.

4.2 Opgelegde sancties voor computervredebreuk

Het Openbaar Ministerie (OM) en de rechter kunnen sancties opleggen aan verdachten van computervredebreuk. In een deel van de gevallen deelt het OM zonder tussenkomst van de rechter een strafbeschikking uit, biedt een transactie aan of besluit tot het seponeren van de zaak onder bepaalde voorwaarden (voorwaardelijk beleidssepot). Veelal bestaan strafbeschikkingen of transacties uit een taakstraf, een geldboete of schadevergoeding. Een deel van de zaken stuurt het OM door naar de rechter die op zijn beurt een straf of maatregel kan opleggen.

Aandeel computervredebreukzaken afgehandeld met een OM-sanctie gedaald

Het totaal aantal keren dat het OM een beslissing nam bij computervredebreukzaken nam toe van 419 in de periode 2011–2016 tot 707 in 2017–2022. Dat betekent een toename van bijna 70 procent. In de periode 2017–2022 werden 128 van de in totaal 707 (18 procent) door het OM genomen beslissingen inzake computervredebreuk afgehandeld door het OM met een transactie, strafbeschikking of voorwaardelijk beleidssepot (tabel 4.2.1). Deze zaken zijn dus afgehandeld met een strafoplegging zonder tussenkomst van een rechter. Dit aandeel is sterk afgenomen ten opzichte van de periode 2011–2016, toen nog een derde van het totaal aantal beslissingen met een strafoplegging door het OM werd afgehandeld. Een deel van de zaken stuurt het OM door naar de rechter waarna de rechter bij schuldigverklaring een straf of maatregel op kan leggen. In 2017–2022 werden 150 zaken doorgestuurd naar de rechter. Dat is een toename van 40 procent in vergelijking met de periode 2011–2016.

In de periode 2017–2022 werden 125 computervredebreukzaken afgedaan door de rechter. Bijna 40 procent meer dan in de periode 2011–2016. Bij 99 (bijna 80 procent) van de computervredebreukzaken die door de rechter zijn afgedaan in 2017–2022 deelde de rechter een straf uit tegenover 72 procent van de zaken in de periode 2011–2016. De meeste overige door de rechter afgedane zaken leiden tot vrijspraak dan wel een schuldigverklaring zonder straf.

Rechter legt vaker gevangenis- en taakstraf op, maar minder boetes

Voor de zaken die bij de rechter tot een straf leiden betreft dit relatief vaak een taakstraf. Bij 80 procent van de zaken waarbij door de rechter een straf werd opgelegd in 2017–2022 betrof dit een taakstraf. Dat is meer dan in 2011–2016 toen nog 57 procent werd afgedaan met een taakstraf. Het aandeel door de rechter opgelegde boetes is gedaald van 37 procent in 2011–2016 naar 7 procent in 2017–2022. Het aandeel opgelegde gevangenisstraffen is daarentegen verdubbeld. Bij 40 procent van de schuldigverklaringen in de periode 2017–2022 tegenover 20 procent in 2011–2016, waarbij door de rechter een straf werd opgelegd betrof dit een gevangenisstraf.

4.2.1 Aantal computervredebreuk zaken afgehandeld door de rechter of het OM

	2011–2016	2017–2022 [1)]
Totaal door OM genomen beslissingen	419	707
– strafoplegging OM[2)]	138	128
– door OM doorgestuurd naar de rechter (dagvaarding en oproep na verzet)	107	150
Straf opgelegd door rechter	65	99

Bron: CBS

[1)] De aantallen ingeschreven rechtbankstrafzaken, totaal beslissingen door OM en onvoorwaardelijke sepots zijn in 2019 (in elk geval deels) gestegen als gevolg van een wijziging in het vastleggen van sepots. Tot 2019 legde de officier van justitie een groot deel van de sepotbeslissingen vast in BOSZ, een politiesysteem. Vanaf 1 januari 2019 worden alle sepotbeslissingen geregistreerd in het GPS-systeem van het OM. Daarom tellen deze zaken nu mee bij zowel de instroom als de uitstroom (technische sepots, vallende onder de categorie onvoorwaardelijke sepots).

[2)] Door het OM afgedaan met transactie, strafbeschikking of voorwaardelijk beleidssepot.

4.2.2 Door de rechter opgelegde straffen en maatregelen voor computervredebreuk per strafzaak[1)].

	% van aantal strafzaken	
	2011–2016	2017–2022
Taakstraf	56,9	79,8
Maatregelen[2)]	26,2	30,3
Gevangenisstraf	21,5	40,4
Geldboete	36,9	7,1
Onbekende straffen	15,4	5,1
Bijkomende straffen	6,2	11,1

Bron: CBS

[1)] Één strafzaak kan meerder straffen toegekend krijgen (bijvoorbeeld taakstraf en geldboete), dus het totaal hoeft niet tot 100 procent op te tellen.

[2)] Betaling aan de staat, onttrekking aan het verkeer.

Bijlagen

Bijlage A

Tabellen

A.1 Definities

A.1.1 Overzicht van de bedrijfsgroottes

Code	Grootteklasse	Aanduiding in tekst
Totaal	2 of meer werkzame personen	Totaal
1	1 werkzame persoon	Zzp'er
2–9	2 tot 10 werkzame personen	Microbedrijf
10–49	10 tot 50 werkzame personen	Klein bedrijf
50–249	50 tot 250 werkzame personen	Middelgroot bedrijf
250+	250 of meer werkzame personen	Groot bedrijf

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 Maatregelen

A.2.1 1) Gebruikte ICT-maatregelen voor alle grootteklassen als percentage van het aantal bedrijven, 2016 -2022

Maatregel	Bedrijfsgrootte	2016	2017	2018	2019	2020	2021	2022
Antivirussoftware	Totaal	87	85	89	89	87	85	83
	1 werkzame persoon (zzp'ers)	.	.	.	.	81	64	66
	2 tot 10 werkzame personen	86	83	87	87	85	83	81
	10 tot 50 werkzame personen	93	94	96	92	95	96	89
	50 tot 250 werkzame personen	97	98	98	97	98	98	95
	250 of meer werkzame personen	98	98	99	98	99	99	95
	2 tot 250 werkzame personen	87	85	89	89	87	85	83
Authenticatie via soft- of hardwaretoken	Totaal	26	30	39	46	45	46	50
	1 werkzame persoon (zzp'ers)	.	.	.	.	38	34	44
	2 tot 10 werkzame personen	24	27	35	42	41	41	45
	10 tot 50 werkzame personen	29	38	49	54	60	62	66
	50 tot 250 werkzame personen	48	54	62	68	75	81	84
	250 of meer werkzame personen	71	76	81	87	89	93	91
	2 tot 250 werkzame personen	25	30	39	45	45	45	49
Beleid voor sterke wachtwoorden	Totaal	57	61	65	68	66	68	66
	1 werkzame persoon (zzp'ers)	.	.	.	.	65	53	58
	2 tot 10 werkzame personen	55	58	63	65	62	65	64
	10 tot 50 werkzame personen	64	70	74	74	77	80	77
	50 tot 250 werkzame personen	81	84	86	88	90	91	89
	250 of meer werkzame personen	93	94	94	96	96	98	93
	2 tot 250 werkzame personen	57	61	65	68	65	68	66
Encryptie van data	Totaal	25	29	37	38	37	36	33
	1 werkzame persoon (zzp'ers)	.	.	.	.	31	25	26
	2 tot 10 werkzame personen	23	27	33	35	34	33	29
	10 tot 50 werkzame personen	29	34	44	44	47	45	45
	50 tot 250 werkzame personen	46	51	62	64	66	67	65
	250 of meer werkzame personen	69	74	81	83	85	87	85
	2 tot 250 werkzame personen	25	29	36	38	37	35	32
Gegevens op andere fysieke locatie	Totaal	71	67	72	71	66	74	66
	1 werkzame persoon (zzp'ers)	.	.	.	.	57	54	52
	2 tot 10 werkzame personen	68	63	68	68	62	70	63
	10 tot 50 werkzame personen	80	81	85	82	82	88	80
	50 tot 250 werkzame personen	90	90	93	91	92	95	91
	250 of meer werkzame personen	94	93	97	95	96	98	93
	2 tot 250 werkzame personen	70	66	72	71	66	73	66
Logbestanden voor analyse incidenten	Totaal	31	33	39	37	36	38	32
	1 werkzame persoon (zzp'ers)	.	.	.	.	19	17	15
	2 tot 10 werkzame personen	25	26	32	31	30	32	26
	10 tot 50 werkzame personen	49	54	59	55	57	60	53
	50 tot 250 werkzame personen	75	78	82	79	82	83	79
	250 of meer werkzame personen	88	88	91	91	91	93	88
	2 tot 250 werkzame personen	30	33	38	37	36	38	32

Vervolg op volgende pagina…

A.2.1 2) Gebruikte ICT-maatregelen voor alle grootteklassen als percentage van het aantal bedrijven, 2016 - 2022

Maatregel	Bedrijfsgrootte	2016	2017	2018	2019	2020	2021	2022
Methodes voor beoordelen ICT-veiligheid	Totaal	22	25	31	28	28	29	25
	1 werkzame persoon (zzp'ers)	.	.	.	.	13	10	9
	2 tot 10 werkzame personen	17	20	26	22	23	24	20
	10 tot 50 werkzame personen	34	40	48	41	45	46	42
	50 tot 250 werkzame personen	55	60	67	63	68	70	69
	250 of meer werkzame personen	72	75	80	81	82	86	84
	2 tot 250 werkzame personen	21	24	31	27	27	29	24
Network access control	Totaal	31	33	37	37	34	46	42
	1 werkzame persoon (zzp'ers)	.	.	.	.	22	20	21
	2 tot 10 werkzame personen	28	29	32	32	29	40	36
	10 tot 50 werkzame personen	42	46	50	48	50	71	66
	50 tot 250 werkzame personen	60	60	63	64	66	88	86
	250 of meer werkzame personen	67	68	71	72	73	91	87
	2 tot 250 werkzame personen	31	33	36	36	34	46	42
Risicoanalyses	Totaal	22	25	31	29	28	29	27
	1 werkzame persoon (zzp'ers)	.	.	.	.	15	12	12
	2 tot 10 werkzame personen	17	20	26	24	23	24	21
	10 tot 50 werkzame personen	34	40	47	42	45	47	44
	50 tot 250 werkzame personen	58	62	64	63	67	70	69
	250 of meer werkzame personen	75	76	80	80	79	83	82
	2 tot 250 werkzame personen	21	24	31	28	28	29	26
VPN internetgebruik buiten het bedrijf	Totaal	29	32	35	35	32	33	31
	1 werkzame persoon (zzp'ers)	.	.	.	.	22	19	19
	2 tot 10 werkzame personen	23	25	29	29	26	28	25
	10 tot 50 werkzame personen	47	50	54	52	55	55	49
	50 tot 250 werkzame personen	74	75	77	78	79	77	75
	250 of meer werkzame personen	85	86	86	86	86	84	81
	2 tot 250 werkzame personen	28	31	35	35	32	33	30

A.2.2 1) Gebruikte ICT-maatregelen voor alle bedrijfstakken als percentage van het aantal bedrijven met 2 of meer werknemers, 2016-2022

Maatregel	Bedrijfstak	2016	2017	2018	2019	2020	2021	2022
Antivirussoftware	Totaal	87	85	89	89	87	85	83
	Industrie	93	91	94	91	90	92	87
	Energie	91	80	92	88	81	91	92
	Bouwnijverheid	85	85	85	89	89	84	85
	Handel	88	85	91	89	85	85	83
	Vervoer	84	83	87	87	84	85	84
	Horeca	76	70	75	76	74	70	74
	Informatie en communicatie	87	89	89	90	86	86	80
	Financiële dienstverlening	88	92	97	92	94	85	81
	Verhuur en handel onroerend goed	80	77	84	82	80	83	80
	Specialistische zakelijke diensten	90	91	93	92	91	90	85
	Verhuur en overige zakelijke diensten	84	85	88	90	89	87	82
	Gezondheidszorg	97	93	97	96	97	94	89
	ICT-sector	90	92	91	90	89	88	82
Authenticatie via soft- of hardwaretoken	Totaal	26	30	39	46	45	46	50
	Industrie	24	29	39	43	41	44	51
	Energie	34	34	43	46	45	49	62
	Bouwnijverheid	16	25	31	33	37	33	38
	Handel	21	26	36	43	42	41	44
	Vervoer	21	25	33	45	39	38	42
	Horeca	16	17	20	29	26	24	30
	Informatie en communicatie	47	50	55	60	66	73	72
	Financiële dienstverlening	45	53	62	64	67	72	68
	Verhuur en handel onroerend goed	28	30	34	39	47	50	53
	Specialistische zakelijke diensten	31	35	47	52	52	57	64
	Verhuur en overige zakelijke diensten	20	30	39	48	43	47	46
	Gezondheidszorg	47	49	59	67	69	67	72
	ICT-sector	49	53	57	63	68	77	79
Beleid voor sterke wachtwoorden	Totaal	57	61	65	68	66	68	66
	Industrie	58	63	65	67	65	69	68
	Energie	67	57	68	71	61	70	77
	Bouwnijverheid	50	54	54	64	60	58	61
	Handel	57	58	66	67	64	68	66
	Vervoer	56	55	62	65	61	65	60
	Horeca	38	48	47	53	47	53	52
	Informatie en communicatie	77	78	85	82	84	83	77
	Financiële dienstverlening	75	80	81	80	84	79	76
	Verhuur en handel onroerend goed	51	52	67	59	59	68	64
	Specialistische zakelijke diensten	67	70	71	73	72	75	72
	Verhuur en overige zakelijke diensten	56	61	67	67	68	67	64
	Gezondheidszorg	66	72	77	80	80	80	79
	ICT-sector	80	82	86	84	85	88	81

Vervolg op volgende pagina…

A.2.2 2) Gebruikte ICT-maatregelen voor alle bedrijfstakken als percentage van het aantal bedrijven met 2 of meer werknemers, 2016-2022

Maatregel	Bedrijfstak	2016	2017	2018	2019	2020	2021	2022
Encryptie van data	Totaal	25	29	37	38	37	36	33
	Industrie	22	24	32	35	33	31	32
	Energie	29	27	37	38	44	33	42
	Bouwnijverheid	15	20	27	23	26	22	18
	Handel	20	23	32	33	32	32	26
	Vervoer	17	20	26	30	26	29	25
	Horeca	11	12	18	22	18	15	17
	Informatie en communicatie	58	59	66	65	65	64	62
	Financiële dienstverlening	38	43	56	56	65	59	48
	Verhuur en handel onroerend goed	26	16	26	37	37	36	29
	Specialistische zakelijke diensten	31	36	44	46	44	44	43
	Verhuur en overige zakelijke diensten	22	29	34	39	37	34	29
	Gezondheidszorg	51	60	67	67	70	66	62
	ICT-sector	60	62	67	67	66	70	67
Gegevens op andere fysieke locatie	Totaal	71	67	72	71	66	74	66
	Industrie	77	74	78	77	73	80	71
	Energie	78	72	74	70	63	75	82
	Bouwnijverheid	64	62	66	66	65	66	63
	Handel	67	62	71	72	63	72	65
	Vervoer	61	62	63	65	63	67	58
	Horeca	52	42	46	43	36	47	42
	Informatie en communicatie	87	82	89	84	82	90	78
	Financiële dienstverlening	75	83	85	76	87	84	75
	Verhuur en handel onroerend goed	69	63	69	64	65	70	63
	Specialistische zakelijke diensten	83	80	85	80	78	88	78
	Verhuur en overige zakelijke diensten	70	65	69	70	66	71	65
	Gezondheidszorg	84	82	87	86	83	86	77
	ICT-sector	89	84	92	84	81	92	82
Logbestanden voor analyse incidenten	Totaal	31	33	39	37	36	38	32
	Industrie	36	39	45	42	40	43	36
	Energie	48	42	54	51	41	48	50
	Bouwnijverheid	20	22	30	29	26	27	22
	Handel	29	31	37	35	34	36	33
	Vervoer	25	29	35	31	33	31	25
	Horeca	13	15	16	15	15	15	10
	Informatie en communicatie	60	58	67	63	63	62	58
	Financiële dienstverlening	50	56	61	59	66	66	52
	Verhuur en handel onroerend goed	31	25	28	33	31	43	29
	Specialistische zakelijke diensten	39	41	48	44	44	47	41
	Verhuur en overige zakelijke diensten	29	33	36	34	34	33	27
	Gezondheidszorg	39	43	49	51	51	56	47
	ICT-sector	64	63	72	65	66	70	66

Vervolg op volgende pagina…

A.2.2 3) Gebruikte ICT-maatregelen voor alle bedrijfstakken als percentage van het aantal bedrijven met 2 of meer werknemers, 2016-2022

Maatregel	Bedrijfstak	2016	2017	2018	2019	2020	2021	2022
Methodes voor beoordelen ICT-veiligheid	Totaal	22	25	31	28	28	29	25
	Industrie	26	30	35	32	33	36	30
	Energie	35	35	46	35	35	41	47
	Bouwnijverheid	16	20	30	22	21	22	19
	Handel	19	22	30	27	27	28	23
	Vervoer	18	19	27	23	27	26	18
	Horeca	8	11	13	12	10	14	13
	Informatie en communicatie	35	43	46	43	39	41	39
	Financiële dienstverlening	41	48	61	55	61	55	44
	Verhuur en handel onroerend goed	25	23	31	28	32	30	24
	Specialistische zakelijke diensten	28	29	37	30	34	34	30
	Verhuur en overige zakelijke diensten	21	26	30	27	27	28	22
	Gezondheidszorg	29	34	39	38	37	38	34
	ICT-sector	37	43	47	44	43	47	45
Network access control	Totaal	31	33	37	37	34	46	42
	Industrie	34	38	40	40	37	51	48
	Energie	37	38	42	51	41	60	64
	Bouwnijverheid	20	27	34	31	23	37	31
	Handel	29	32	36	37	33	43	41
	Vervoer	23	30	30	30	31	36	26
	Horeca	17	14	19	20	20	21	23
	Informatie en communicatie	51	50	53	51	47	64	60
	Financiële dienstverlening	48	53	59	55	61	74	58
	Verhuur en handel onroerend goed	36	26	28	33	34	47	43
	Specialistische zakelijke diensten	38	37	42	41	38	61	54
	Verhuur en overige zakelijke diensten	28	33	35	34	34	44	37
	Gezondheidszorg	46	47	47	48	48	64	59
	ICT-sector	54	54	55	53	49	69	68
Risicoanalyses	Totaal	22	25	31	29	28	29	27
	Industrie	24	30	33	31	32	33	30
	Energie	33	34	34	37	33	40	45
	Bouwnijverheid	16	20	25	21	17	19	16
	Handel	20	20	27	26	26	27	25
	Vervoer	19	22	28	24	27	28	21
	Horeca	10	12	15	13	12	14	13
	Informatie en communicatie	39	47	50	48	47	45	44
	Financiële dienstverlening	39	49	58	51	57	57	50
	Verhuur en handel onroerend goed	22	22	25	24	27	31	24
	Specialistische zakelijke diensten	25	30	37	31	33	34	31
	Verhuur en overige zakelijke diensten	19	25	30	28	29	27	25
	Gezondheidszorg	31	37	48	46	41	44	44
	ICT-sector	42	47	53	50	50	51	50

Vervolg op volgende pagina…

A.2.2 4) Gebruikte ICT-maatregelen voor alle bedrijfstakken als percentage van het aantal bedrijven met 2 of meer werknemers, 2016-2022

Maatregel	Bedrijfstak	2016	2017	2018	2019	2020	2021	2022
VPN internetgebruik buiten het bedrijf	Totaal	29	32	35	35	32	33	31
	Industrie	36	39	42	42	42	41	40
	Energie	42	45	51	50	43	40	51
	Bouwnijverheid	20	21	29	26	23	26	23
	Handel	26	28	34	34	30	31	29
	Vervoer	23	26	27	26	27	28	22
	Horeca	13	13	14	12	13	13	13
	Informatie en communicatie	54	56	58	55	52	54	47
	Financiële dienstverlening	51	57	53	55	52	55	46
	Verhuur en handel onroerend goed	34	28	31	31	34	35	32
	Specialistische zakelijke diensten	36	38	42	44	39	42	40
	Verhuur en overige zakelijke diensten	25	32	32	31	29	31	26
	Gezondheidszorg	37	44	49	48	45	47	41
	ICT-sector	59	61	62	59	58	61	55

A.2.3 Percentage van bedrijven die minimaal vijf van de tien gevraagde cybersecuritymaatregelen nemen per grootteklasse.

Bedrijfsgrootte	2016	2017	2018	2019	2020	2021	2022
1 werkzame persoon (zzp'er)	.	.	.	.	32	29	29
2 of meer werkzame personen	37	43	49	49	48	52	47
2 tot 10 werkzame personen	32	37	43	44	42	45	41
10 tot 50 werkzame personen	54	61	69	65	70	75	71
50 tot 250 werkzame personen	82	83	89	89	91	94	90
250 of meer werkzame personen	94	94	97	98	97	98	93

A.2.4 Percentage van bedrijven die minimaal vijf van de tien gevraagde cybersecuritymaatregelen nemen per bedrijfstak.

Bedrijfstak	2016	2017	2018	2019	2020	2021	2022
Horeca	20	18	22	21	23	21	24
Bouwnijverheid	26	30	41	39	35	39	34
Vervoer en opslag	30	33	38	41	39	42	37
Verhuur en overige zakelijke diensten	34	40	48	49	46	48	44
Handel	34	38	46	48	44	49	45
Verhuur en handel van onroerend goed	41	39	42	43	48	56	49
Industrie	42	47	53	53	51	55	52
Specialistische zakelijke diensten	47	53	59	58	58	65	59
Financiële dienstverlening	59	71	74	70	80	75	68
Energie, water, afvalbeheer	51	47	55	59	52	59	68
Informatie en communicatie	68	67	75	73	70	75	70
Gezondheids- en welzijnszorg	57	66	74	73	72	78	71
ICT-sector	74	73	76	73	73	80	77

A.3 Incidenten

A.3.1 Incidenten met interne oorzaak en kosten per grootteklasse als percentage van het aantal bedrijven, 2016-2022[1]

		2016		2020		2021		2022	
		Incident gehad	ook met kosten	Incident gehad	ook met kosten	Incident gehad	ook met kosten	Incident gehad	ook met kosten
Interne incidenten	*Aantal werkzame personen*								
Uitval ICT-systeem door ICT-veiligheidsincident	Totaal	26	10	13	4	11	3	11	2
	1 werkzame persoon (zzp'ers)	.	.	7	1	4	1	5	1
	2 tot 10 werkzame personen	21	8	10	3	9	2	9	2
	10 tot 50 werkzame personen	41	18	23	7	22	6	19	5
	50 tot 250 werkzame personen	52	25	35	10	32	9	28	8
	250 of meer werkzame personen	54	28	41	13	42	15	37	12
	2 tot 250 werkzame personen	25	10	13	4	11	3	11	2
Vernietiging data door ICT-veiligheidsincident	Totaal	5	3	2	1	2	0	1	0
	1 werkzame persoon (zzp'ers)	.	.	2	1	1	0	2	0
	2 tot 10 werkzame personen	5	2	2	1	1	0	1	0
	10 tot 50 werkzame personen	7	3	3	1	3	1	2	0
	50 tot 250 werkzame personen	10	5	5	2	4	2	3	1
	250 of meer werkzame personen	13	7	7	3	6	2	5	2
	2 tot 250 werkzame personen	5	2	2	1	2	0	1	0
Onthulling door intern incident	Totaal	2	1	1	0	1	0	1	0
	1 werkzame persoon (zzp'ers)	.	.	0	0	0	0	1	0
	2 tot 10 werkzame personen	2	1	1	0	1	0	1	0
	10 tot 50 werkzame personen	3	1	2	0	2	0	2	0
	50 tot 250 werkzame personen	6	2	6	1	5	1	5	0
	250 of meer werkzame personen	16	4	17	3	18	3	17	2
	2 tot 250 werkzame personen	2	1	1	0	1	0	1	0

[1] Cijfers over 2017—2019 worden weggelaten. Alle cijfers zijn openbaar en te vinden via: CBS (2017e, 2018e, 2019a, 2020b, 2021e, 2022a, 2023b)

A.3.2 Incidenten door aanval van buitenaf en kosten per grootteklasse als percentage van het aantal bedrijven, 2016-2022[1]

		2016		2020		2021		2022	
		Incident gehad	ook met kosten	Incident gehad	ook met kosten	Incident gehad	ook met kosten	Incident gehad	ook met kosten
Incidenten door aanval	*Aantal werkzame personen*								
Uitval ICT-systeem door aanval van buitenaf	Totaal	8	4	5	2	4	1	3	1
	1 werkzame persoon (zzp'ers)	.	.	3	0	2	0	2	0
	2 tot 10 werkzame personen	6	3	4	1	3	1	3	1
	10 tot 50 werkzame personen	12	6	8	3	6	2	5	2
	50 tot 250 werkzame personen	17	9	11	4	8	3	7	2
	250 of meer werkzame personen	22	12	14	5	12	5	9	3
	2 tot 250 werkzame personen	7	4	5	2	4	1	3	1
Vernietiging data aanval van buitenaf	Totaal	6	3	2	1	1	1	2	1
	1 werkzame persoon (zzp'ers)	.	.	1	0	1	0	1	0
	2 tot 10 werkzame personen	4	2	2	1	1	0	2	1
	10 tot 50 werkzame personen	11	6	3	1	2	1	2	1
	50 tot 250 werkzame personen	18	8	4	2	3	1	2	1
	250 of meer werkzame personen	24	9	4	2	4	2	3	2
	2 tot 250 werkzame personen	6	3	2	1	1	1	2	1
Onthulling gegevens door ICT-inbraak	Totaal	2	1	2	1	2	0	2	0
	1 werkzame persoon (zzp'ers)	.	.	2	0	1	0	1	0
	2 tot 10 werkzame personen	1	1	1	0	1	0	1	0
	10 tot 50 werkzame personen	2	1	2	1	3	1	2	0
	50 tot 250 werkzame personen	2	1	4	1	4	1	5	1
	250 of meer werkzame personen	5	2	9	3	9	2	10	2
	2 tot 250 werkzame personen	2	1	1	1	2	0	2	0

[1] Cijfers over 2017—2019 worden weggelaten. Alle cijfers zijn openbaar en te vinden via : CBS (2017e, 2018e, 2019a, 2020b, 2021e, 2022a, 2023b)

A.3.3 Incidenten met interne oorzaak per bedrijfstak als percentage van het aantal bedrijven, 2016-2022[1]

		2016		2020		2021		2022	
		Incident gehad	ook met kosten	Incident gehad	ook met kosten	Incident gehad	ook met kosten	Incident gehad	ook met kosten
Interne incidenten	*Bedrijfstak*								
Uitval ICT-systeem door ICT-veiligheidsincident	Totaal	26	10	13	4	11	3	11	2
	Industrie	30	14	15	5	14	4	13	3
	Energie	29	12	16	4	14	3	18	4
	Bouwnijverheid	22	9	10	4	8	2	10	3
	Handel	26	11	10	3	10	3	10	2
	Vervoer	21	9	14	6	10	3	8	2
	Horeca	13	5	12	3	5	2	8	1
	Informatie en communicatie	28	10	18	5	16	3	13	2
	Financiële dienstverlening	29	11	22	8	21	6	16	4
	Verhuur en handel onroerend goed	29	11	8	3	8	1	11	3
	Specialistische zakelijke diensten	29	12	16	5	14	4	11	2
	Verhuur en overige zakelijke diensten	22	8	10	2	10	2	10	2
	Gezondheidszorg	33	12	22	6	20	3	18	3
	ICT-sector	28	10	18	4	17	4	14	2
Vernietiging data door ICT-veiligheidsincident	Totaal	5	3	2	1	2	0	1	0
	Industrie	6	3	2	1	1	1	1	0
	Energie	7	4	2	0	2	0	1	0
	Bouwnijverheid	5	2	1	1	1	0	1	0
	Handel	6	3	2	1	1	0	1	0
	Vervoer	4	2	3	2	2	0	0	0
	Horeca	5	2	3	1	1	0	3	1
	Informatie en communicatie	6	2	2	0	3	1	2	0
	Financiële dienstverlening	4	2	4	1	2	2	2	0
	Verhuur en handel onroerend goed	8	3	2	1	1	0	3	1
	Specialistische zakelijke diensten	5	3	3	1	2	1	2	0
	Verhuur en overige zakelijke diensten	4	2	1	0	1	0	1	0
	Gezondheidszorg	3	1	2	1	2	0	1	0
	ICT-sector	6	2	3	0	3	1	2	0
Onthulling door intern incident	Totaal	2	1	1	0	1	0	1	0
	Industrie	2	1	1	0	1	0	1	0
	Energie	5	3	3	1	3	0	2	0
	Bouwnijverheid	2	1	0	0	0	0	0	0
	Handel	2	1	1	0	1	0	1	0
	Vervoer	1	1	1	0	2	0	1	0
	Horeca	1	0	1	0	0	0	1	0
	Informatie en communicatie	3	1	1	0	1	0	2	0
	Financiële dienstverlening	3	1	3	0	4	2	5	0
	Verhuur en handel onroerend goed	2	1	1	0	2	1	2	0
	Specialistische zakelijke diensten	2	1	2	0	2	0	2	0
	Verhuur en overige zakelijke diensten	2	1	1	0	1	0	1	0
	Gezondheidszorg	2	0	5	1	4	0	4	0
	ICT-sector	3	1	1	0	1	0	2	1

[1] Cijfers over 2017—2019 worden weggelaten. Alle cijfers zijn openbaar en te vinden via: CBS (2017e, 2018e, 2019a, 2020b, 2021e, 2022a, 2023b).

A.3.4 Incidenten door aanval van buitenaf per bedrijfstak als percentage van het aantal bedrijven, 2016-2022[1]

		2016		2020		2021		2022	
		Incident gehad	ook met kosten	Incident gehad	ook met kosten	Incident gehad	ook met kosten	Incident gehad	ook met kosten
Incidenten door aanval	*Bedrijfstak*								
Vernietiging data aanval van buitenaf	Totaal	8	4	5	2	4	1	3	1
	Industrie	10	6	5	2	4	2	3	1
	Energie	8	3	8	1	2	1	3	1
	Bouwnijverheid	9	4	3	2	3	1	4	1
	Handel	8	4	5	2	4	2	4	1
	Vervoer	5	3	5	2	4	1	3	1
	Horeca	3	1	4	1	1	0	2	1
	Informatie en communicatie	12	4	9	3	6	1	7	1
	Financiële dienstverlening	7	2	10	2	8	2	6	2
	Verhuur en handel onroerend goed	6	3	6	0	1	0	3	1
	Specialistische zakelijke diensten	9	5	5	2	5	2	2	1
	Verhuur en overige zakelijke diensten	8	4	4	1	3	0	2	0
	Gezondheidszorg	4	2	5	1	4	1	2	0
	ICT-sector	12	5	9	3	6	1	8	2
Uitval ICT-systeem door aanval van buitenaf	Totaal	6	3	2	1	1	1	2	1
	Industrie	9	5	2	1	1	1	2	1
	Energie	9	5	1	0	2	0	0	0
	Bouwnijverheid	8	3	2	1	1	0	2	1
	Handel	6	3	2	1	1	0	2	1
	Vervoer	6	3	3	2	2	1	1	0
	Horeca	4	1	2	1	1	0	1	0
	Informatie en communicatie	4	2	1	0	1	1	3	1
	Financiële dienstverlening	8	4	0	0	3	1	4	0
	Verhuur en handel onroerend goed	6	2	2	1	1	0	3	2
	Specialistische zakelijke diensten	5	2	2	1	2	1	1	0
	Verhuur en overige zakelijke diensten	7	4	2	1	2	1	1	0
	Gezondheidszorg	5	2	1	1	0	0	1	1
	ICT-sector	5	2	2	0	1	1	4	1
Onthulling gegevens door ICT-inbraak	Totaal	2	1	2	1	2	0	2	0
	Industrie	2	1	2	0	1	0	2	0
	Energie	2	0	1	0	1	0	3	0
	Bouwnijverheid	2	0	1	1	1	0	2	1
	Handel	2	1	2	1	2	0	1	0
	Vervoer	2	1	2	0	1	0	2	0
	Horeca	1	0	1	1	1	0	1	0
	Informatie en communicatie	1	1	1	0	1	0	2	0
	Financiële dienstverlening	2	1	1	0	4	2	3	0
	Verhuur en handel onroerend goed	1	1	1	0	2	1	2	0
	Specialistische zakelijke diensten	2	1	2	1	2	1	1	0
	Verhuur en overige zakelijke diensten	2	1	2	0	2	0	3	0
	Gezondheidszorg	1	0	1	1	1	0	2	0
	ICT-sector	1	1	1	0	2	0	3	1

[1] Cijfers over 2017—2019 worden weggelaten. Alle cijfers zijn openbaar en te vinden via: CBS (2017e, 2018e, 2019a, 2020b, 2021e, 2022a, 2023b)

Bibliografie

CBS (2017a). ICT-gebruik bij bedrijven; bedrijfsgrootte.

CBS (2017b). ICT-gebruik bij bedrijven; bedrijfstak.

CBS (2017c). ICT-gebruik bij bedrijven; bedrijfstak en bedrijfsgrootte.

CBS (2017d). ICT-gebruik bij kleine bedrijven; bedrijfsgrootte.

CBS (2017e). ICT-gebruik bij kleine bedrijven; bedrijfstak en bedrijfsgrootte.

CBS (2017f). Cybersecuritymonitor 2017.

CBS (2018a). ICT-gebruik bij bedrijven; bedrijfsgrootte.

CBS (2018b). ICT-gebruik bij bedrijven; bedrijfstak.

CBS (2018c). ICT-gebruik bij bedrijven; bedrijfstak en bedrijfsgrootte.

CBS (2018d). ICT-gebruik bij kleine bedrijven; bedrijfsgrootte.

CBS (2018e). ICT-gebruik bij kleine bedrijven; bedrijfstak en bedrijfsgrootte.

CBS (2018f). Cybersecuritymonitor 2018.

CBS (2019a). ICT-gebruik bij kleine bedrijven; bedrijfstak en bedrijfsgrootte.

CBS (2019b). ICT-gebruik bij kleine bedrijven; bedrijfsgrootte.

CBS (2019c). ICT-gebruik bij bedrijven; bedrijfsgrootte.

CBS (2019d). ICT-gebruik bij bedrijven; bedrijfstak en bedrijfsgrootte.

CBS (2019e). ICT-gebruik bij bedrijven; bedrijfstak.

CBS (2019f). Cybersecuritymonitor 2019.

CBS (2020a). ICT-gebruik bij bedrijven; bedrijfstak.

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

CBS (2020c). ICT-gebruik bij kleine bedrijven; bedrijfsgrootte.

CBS (2020d). ICT-gebruik bij bedrijven; bedrijfsgrootte.

CBS (2020e). ICT-gebruik bij bedrijven; bedrijfstak en bedrijfsgrootte.

CBS (2020f). Cybersecuritymonitor 2020.

CBS (2021a). ICT-gebruik bij kleine bedrijven; bedrijfsgrootte.

CBS (2021b). ICT-gebruik bij bedrijven; bedrijfsgrootte.

CBS (2021c). ICT-gebruik bij bedrijven; bedrijfstak en bedrijfsgrootte.

CBS (2021d). ICT-gebruik bij bedrijven; bedrijfstak.

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

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

CBS (2022b). ICT-gebruik bij kleine bedrijven; bedrijfsgrootte.

CBS (2022c). ICT-gebruik bij bedrijven; bedrijfsgrootte.

CBS (2022d). ICT-gebruik bij bedrijven; bedrijfstak en bedrijfsgrootte.

CBS (2022e). ICT-gebruik bij bedrijven; bedrijfstak.

CBS (2022f). Cybersecuritymonitor 2021.

CBS (2023a). Statline Slachtofferschap online criminaliteit 2023; persoonskenmerken.

CBS (2023b). ICT-gebruik bij kleine bedrijven; bedrijfstak en bedrijfsgrootte, 2023.

CBS (2023c). ICT-gebruik bij kleine bedrijven; bedrijfsgrootte.

CBS (2023d). ICT-gebruik bij bedrijven; bedrijfsgrootte.

CBS (2023e). ICT-gebruik bij bedrijven; bedrijfstak en bedrijfsgrootte.

CBS (2023f). ICT-gebruik bij bedrijven; bedrijfstak.

CBS (2023g). CBS StatLine.

CBS (2023h). Cybersecuritymonitor 2022.

CBS (2023i). Veiligheidsmonitor 2023.

CBS (2024). Toepassing van Internetstandaarden voor websites van bedrijven.

NBIP (2023a). Cijfers DDoS-aanvallen in het eerste kwartaal 2024.

NBIP (2023b). Cijfers DDoS-aanvallen in het eerste kwartaal 2023.

NCTV (2023). Cybersecuritybeeld Nederland 2023.

SIDN (2024). SIDN Labs: .nl stats en data.

Uitgave 2024