Cybersecuritymonitor

2022

Cybersecuritymonitor

2022

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
2022–2023	2022 tot en met 2023
2022/2023	Het gemiddelde over de jaren 2022 tot en met 2023
2022/'23	Oogstjaar, boekjaar, schooljaar enz., beginnend in 2022 en eindigend in 2023
2020/'21–2022/'23	Oogstjaar, boekjaar, enz., 2020/'21 tot en met 2022/'23

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. Inleiding

Dit is het zesde jaar op rij dat het Centraal Bureau voor de Statistiek 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, 2021f).

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 gerelateerd 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) en 'ICT-gebruik bij bedrijven 2022' (CBS, 2022c,e,d,b,a).

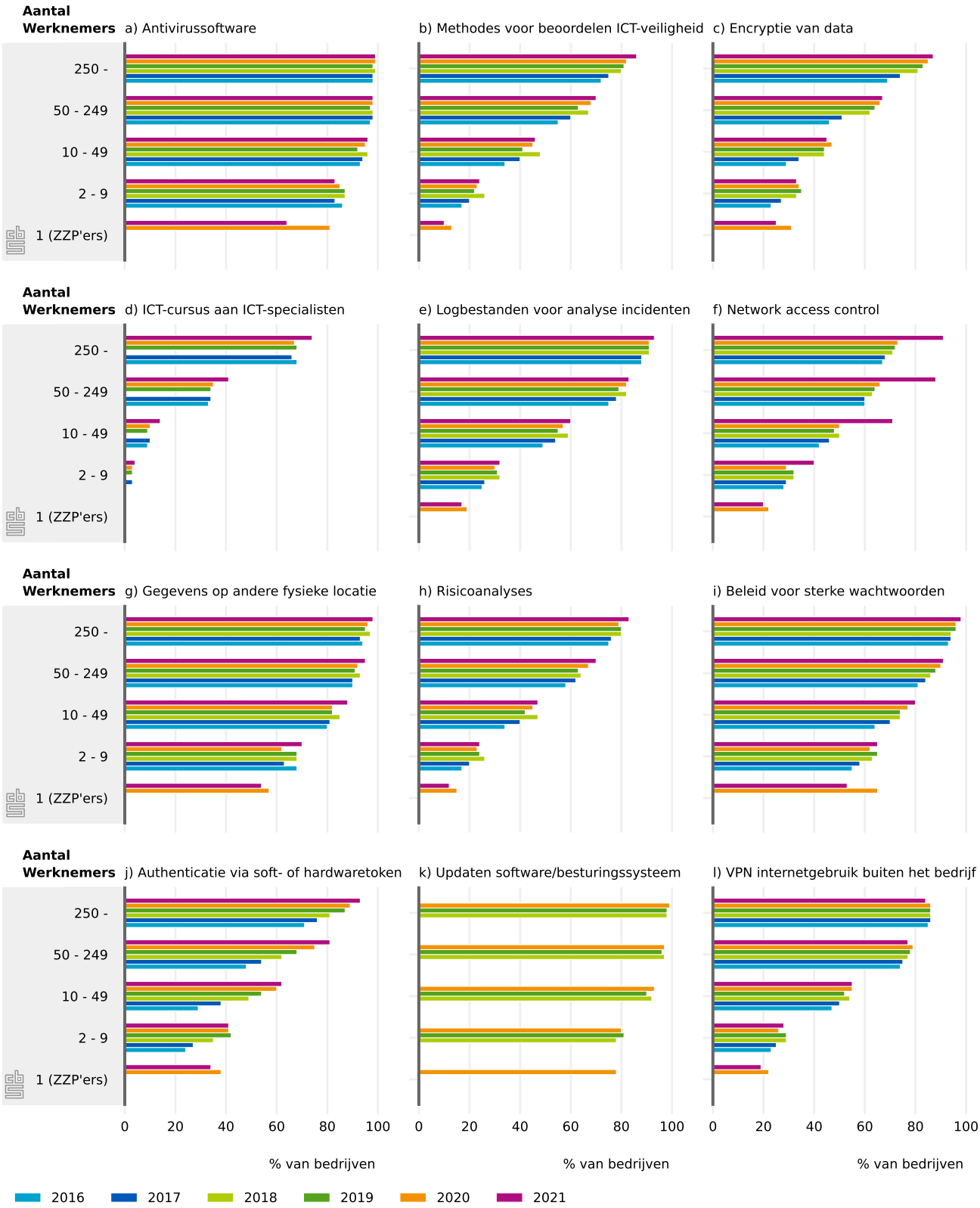
De jaarlijkse enquête 'ICT-gebruik bedrijven' (of kortweg: de ICT-enquête) wordt in samenwerking met de andere EU-landen uitgevoerd onder leiding van Eurostat. Een deel van de uitvoeringskosten van de ICT-enquête wordt door Eurostat gefinancierd. Het ministerie van Economische Zaken en Klimaat financiert 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 door bedrijven worden genomen om het bedrijf te beveiligen tegen aanvallen van buitenaf en de ICT-veiligheidsincidenten. De maatregelen worden in dit hoofdstuk beschreven, terwijl de incidenten in het volgende hoofdstuk aan bod komen.

De ICT-enquête wordt gehouden onder ongeveer 20 duizend aselect getrokken Nederlandse bedrijven uit verschillende grootteklassen en bedrijfstakken. De afgelopen twee 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 twee jaar in deze monitor meegenomen en vergeleken met die voor bedrijven met twee of meer werknemers te kunnen maken.

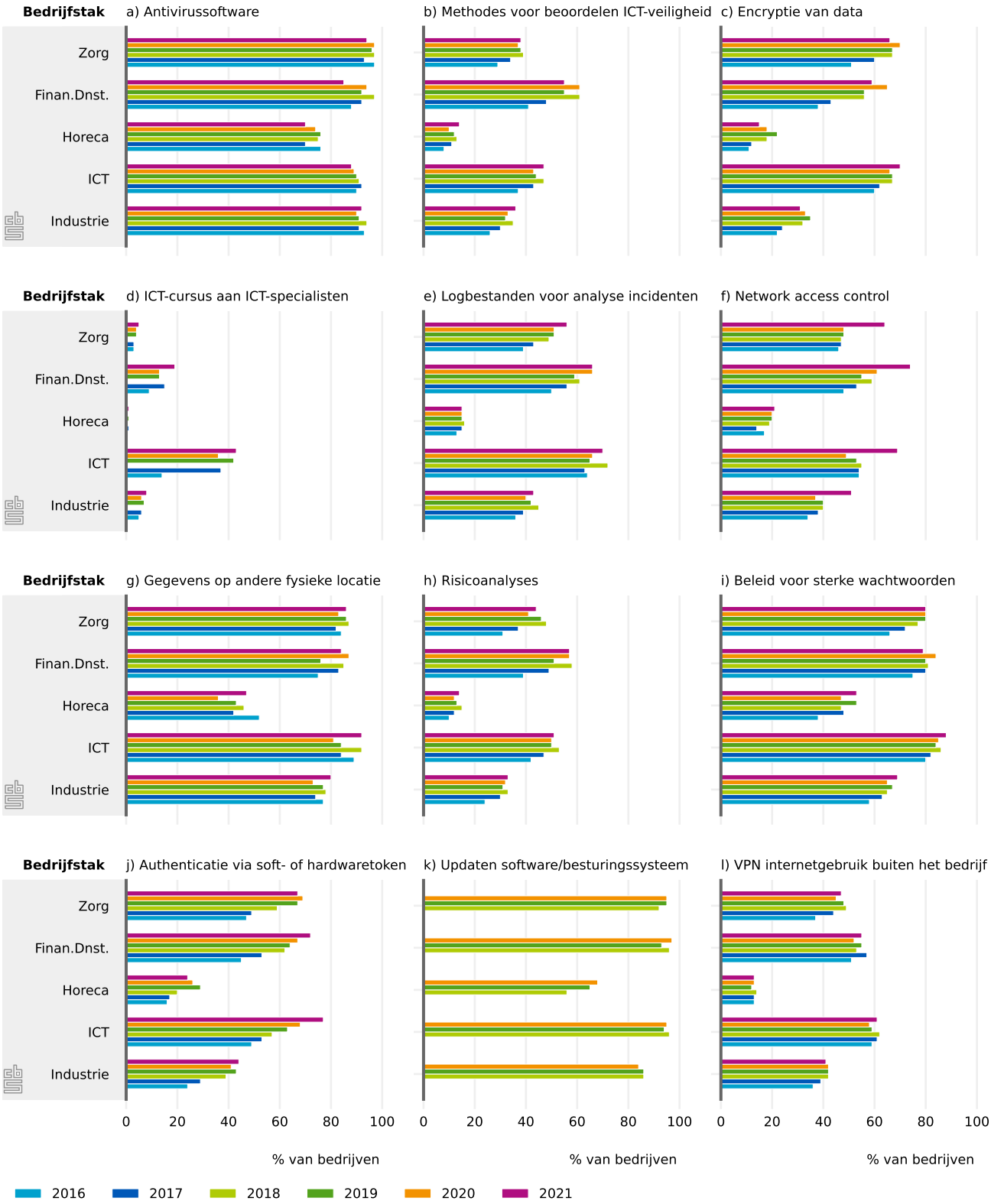
In de Appendix wordt in tabellen A.1.1 en A.1.2 een overzicht van respectievelijk alle grootteklassen en bedrijfstakken gegeven. In dit hoofdstuk worden de cijfers van vijf grootteklassen uitgelicht: ZZP'ers (1 werkzame persoon), bedrijven met 2 tot 10 werkzame personen, bedrijven met 10 tot 50 werkzame 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 doordat de resultaten van de genomen ICT-veiligheidsmaatregelen en opgelopen ICT-veiligheidsincidenten 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 dit rapport in bijlage A.2 en bijlage A.3 gevonden worden, of zijn online beschikbaar op Statline (CBS, 2022f).

2.1.1 Genomen ICT-veiligheidsmaatregelen per bedrijfsgrootteklasse over de periode 2016-2021.



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

2.1.2 Genomen ICT-veiligheidsmaatregelen per bedrijfstak met 2 of meer werkzame personen over de periode 2016-2021.



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

Maatregelen ter verbetering van de cyberweerbaarheid

Aan de bedrijven die aan de ICT-enquête hebben deelgenomen, zijn verschillende vragen voorgelegd die iets zeggen over hun cyberweerbaarheid. 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.

Eerst wordt bekeken 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 2016–2021 verschillende cybersecuritymaatregelen toegepast, 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, 2022f). Uiteraard kan met deze twaalf maatregelen nooit een compleet beeld van het ICT-beveiligingsniveau van bedrijven gegeven worden, maar er ontstaat wel een globale indruk, omdat elke extra maatregel die een bedrijf neemt een extra bijdrage levert aan de cyberweerbaarheid van het bedrijf.

Grote bedrijven nemen meer maatregelen tegen cyberdreigingen

In het algemeen kan gezegd worden dat het ICT-beveiligingsniveau van een bedrijf hoger is naarmate er meer maatregelen tegelijkertijd genomen worden. In figuur 2.1.1 is voor de jaren 2016–2021 te zien dat iedere maatregel vaker door grote dan door kleine bedrijven genomen wordt. Voor sommige maatregelen is dit patroon sterker dan voor andere.

Voor bijvoorbeeld een gangbare maatregel als het gebruik van antivirussoftware (figuur 2.1.1(a)) zijn de verschillen tussen grote en kleine bedrijven niet zo groot: meer dan 80 procent van alle bedrijven gebruikt antivirussoftware, ongeacht de grootteklasse. Bij een moeilijker toe te passen maatregel als het gebruik van een Virtual Private Netwerk (VPN) (figuur 2.1.1(l)) zijn wel grotere verschillen tussen kleine en grote bedrijven te zien. Minder dan 30 procent van de bedrijven met 2 tot 10 werknemers maakt gebruik van VPN tegen 84 procent van de bedrijven met 250 of meer werknemers in 2021. Dat grotere bedrijven meer maatregelen treffen is niet vreemd. Grotere bedrijven hebben immers vaker een grotere en meer complexe ICT-infrastructuur die daarom een breder spectrum aan beveiligingsmaatregelen vereist.

Figuur 2.1.1 toont ook het percentage ZZP'ers dat in 2020 en 2021 de maatregelen nam. Er kan geconstateerd 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— 10 werknemers. Dit is consistent met de constatering dat kleine bedrijven minder ICT-veiligheidsmaatregelen nemen dan grote bedrijven.

Toename authenticatie met soft- of hardwaretoken

Het gebruik van een soft- of hardwaretoken voor het inloggen bij een bedrijf is vanaf 2016 flink toegenomen. Deze zogenaamde twee-staps authentificatie[2)] vergroot de veiligheid omdat naast een wachtwoord een extra code ingevoerd moet worden die per inlogsessie

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 2021 uit de ICT-enquête van 2022 (CBS, 2022c).

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

verandert. Deze code wordt verkregen via een specifiek apparaatje of via een App op de smartphone zoals *Authy*, *Google Authenticator* of *RSA SecureID*. Op deze manier is inloggen een stuk veiliger, want zelfs als een wachtwoord onderschept wordt, biedt de vereiste extra code bescherming tegen inloggen door ongeautoriseerde gebruikers.

Onder grote bedrijven is het gebruik van soft- of hardwaretokens toegenomen van 71 procent in 2016 tot 93 procent in 2021 (figuur 2.1.1(j)). Voor alle grootteklassen is te zien dat deze manier van inloggen steeds vaker gebruikt wordt. Vooral de middelgrote bedrijven met 10 tot 50 werknemers maken een inhaalslag met een dekking die gestegen is van 29 procent in 2016 naar 62 procent in 2021. Onder kleine bedrijven (2 tot 10 werknemers) zien we een ontwikkeling van 23 procent in 2016 naar 41 procent in 2021 voor het gebruik van hardwaretokens, wat bijna een verdubbeling is. Overigens bieden steeds meer websites de mogelijkheid om twee-staps authentificatie te gebruiken. Het is daarom aannemelijk dat deze manier van inloggen in de toekomst nog meer zal toenemen.

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). Te zien is dat bedrijven die meer met ICT bezig zijn (ICT-sector) of bedrijven die een groot belang hebben bij het beveiligen van hun data (Gezondheidszorg) beter scoren dan andere sectoren waar cybersecurity iets minder belangrijke lijkt, zoals de horeca. Wel moet in het achterhoofd gehouden worden dat de horeca een relatief grote groep kleine bedrijven heeft, die over het algemeen minder geneigd zijn tot het nemen van cybersecuritymaatregelen. Daarnaast zijn horecabedrijven minder sterk aangewezen op het gebruik van ICT-systemen voor de uit te voeren werkzaamheden. Het ligt daarmee voor de hand dat er ook minder ICT-beveiligingsmaatregelen genomen worden.

Aantal genomen ICT-veiligheidsmaatregelen

Eerder bleek dat grote bedrijven vaker verschillende ICT-maatregelen nemen dan kleine bedrijven. Dit wordt weergegeven in figuren 2.1.3(a) en 2.1.3(b), waarbij we per bedrijfsgrootte en bedrijfstak het percentage bedrijven laten zien dat een zeker aantal maatregelen neemt. Kleine bedrijven scoren hoger op een kleiner aantal maatregelen, terwijl grote bedrijven juist vaker meerdere maatregelen tegelijk nemen (figuur2.1.3(a)). Van de bedrijven met 250 of meer werknemers neemt zelfs bijna de helft van de bedrijven alle tien de uitgevraagde maatregelen. [3)] In figuur 2.1.3(b) is te zien dat ICT-bedrijven over het algemeen de meeste maatregelen nemen, terwijl in de horeca vaker minder maatregelen genomen worden.

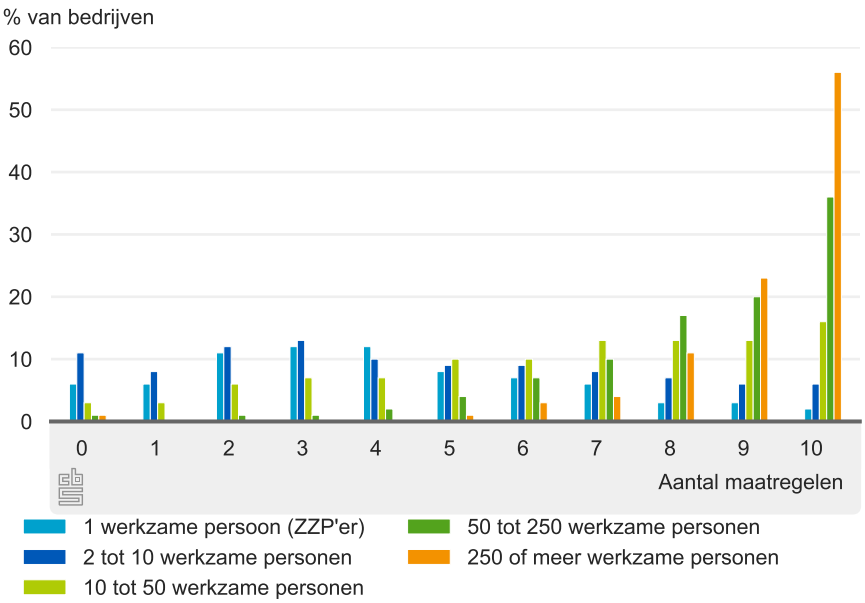
Ruim de helft van de bedrijven met twee of meer werknemers nam in 2021 minstens vijf ICT-veiligheidsmaatregelen

Uit de verdelingen van het aantal maatregelen is af te leiden welk deel van de bedrijven minimaal de helft van de gevraagde maatregelen neemt. Dit wordt in figuur 2.1.4(a) en figuur 2.1.4(b) respectievelijk per grootteklasse en bedrijfstak getoond voor de jaren 2016 tot en met 2021. In figuur 2.1.4(a) is nu goed te zien dat het aantal bedrijven dat vijf of meer maatregelen neemt tot 2018 toegenomen is. In 2021 is het aantal bedrijven met twee of

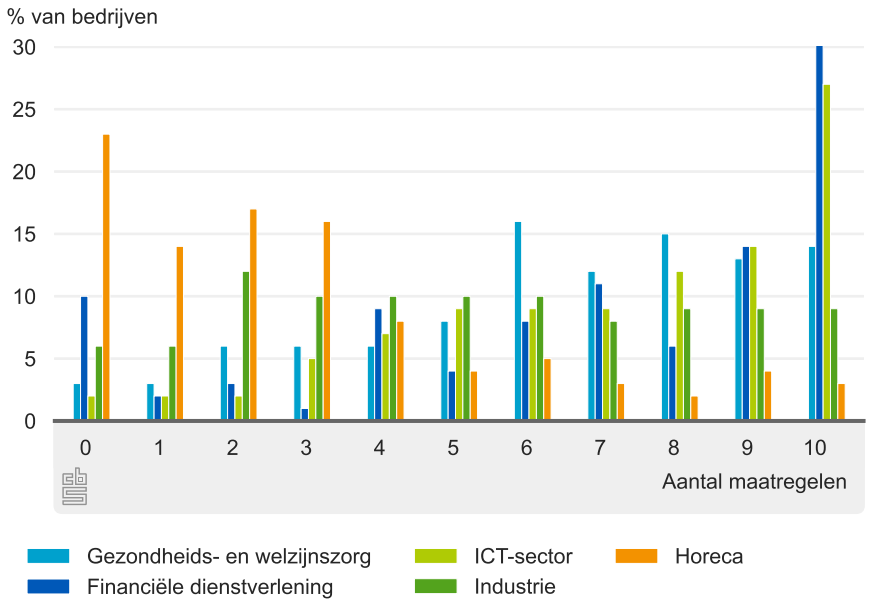
[3)] Van de twaalf maatregelen die in figuur 2.1.1 en figuur 2.1.2 getoond worden, nemen we er maar tien mee in figuur 2.1.3a en figuur 2.1.3b waar we het totaal aantal maatregelen tonen dat bedrijven nemen. Dit omdat de maatregelen 'ICT-cursus aan specialisten' (d) en 'Updaten software' (k) niet over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

2.1.3 Verdeling van het aantal cybersecuritymaatregelen per grootteklasse (a) en bedrijfstak (b), 2021.

(a) grootteklasse



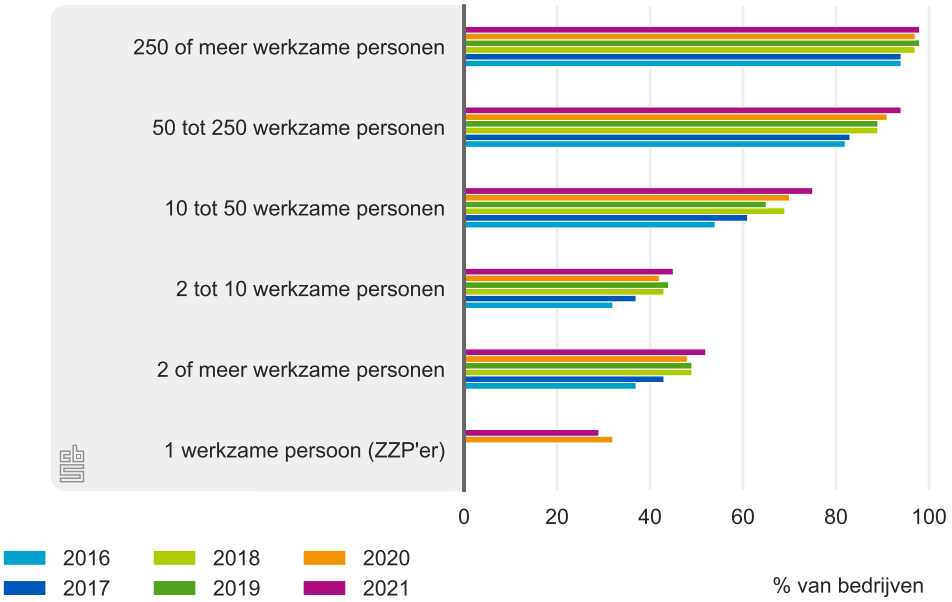
(b) Bedrijfstak



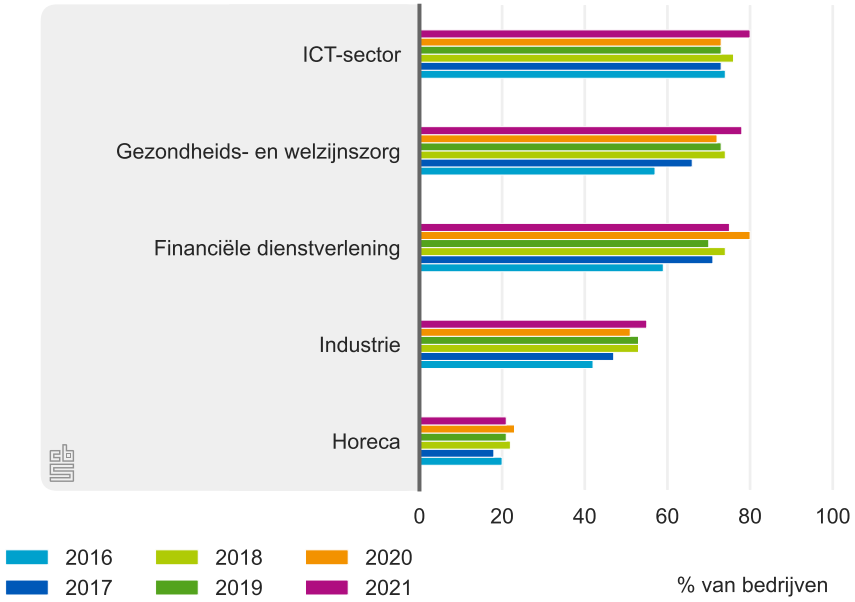
Bron: CBS (2022a)

2.1.4 Percentage van bedrijven die in 2021 minimaal vijf van de tien gevraagde cybersecuritymaatregelen namen per grootteklasse (a) en bedrijfstak (b).

(a) grootteklasse



(b) Bedrijfstak



Bron: CBS (2022a)

meer werknemers dat minimaal vijf maatregelen neemt na een jaar van stagnatie weer toegenomen tot 52 procent. Hoe groter de bedrijven, hoe meer maatregelen genomen worden. Grote bedrijven met 250 werknemers of meer nemen bijna allemaal minimaal vijf van de tien maatregelen. Tenslotte is te zien dat ongeveer één derde van de ZZP'ers vijf of meer van de gevraagde ICT-veiligheidsmaatregelen neemt.

Figuur 2.1.4(b) toont het aandeel bedrijven met twee of meer werknemers dat vijf of meer ICT-veiligheidsmaatregelen heeft getroffen, per bedrijfstak. Het is te zien dat in de ICT-sector, bij Financiële dienstverlening en in de Gezondheid een relatief grote groep bedrijven meer dan vijf maatregelen treft (in 2021 bijna 80 procent), terwijl dit voor de Horeca een stuk lager ligt met ongeveer 20 procent. Wel kunnen we zien dat ook per bedrijfstak de afgelopen zes jaar het aandeel bedrijven dat een groot aantal ICT-veiligheidsmaatregelen tegelijkertijd neemt, is toegenomen. In 2021 neemt het percentage bedrijven dat minstens vijf maatregelen neemt na twee jaar van stagnatie weer toe.

Uitvoering ICT-veiligheidswerkzaamheden

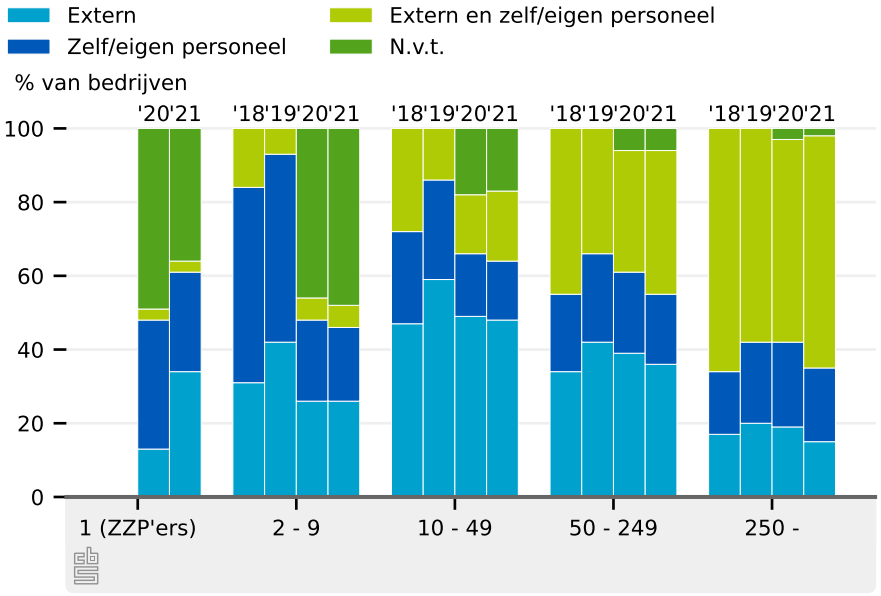
De organisatie van de ICT-beveiliging wordt in figuur 2.1.5(a) en figuur 2.1.5(b) onder de loep genomen. Er wordt per grootteklasse en bedrijfstak gekeken wie de ICT-veiligheidswerkzaamheden binnen het bedrijf uitvoert: het eigen personeel, een extern bedrijf of een mix van beide. Vanaf het jaar 2020 worden deze resultaten ook voor ZZP'ers weergegeven. De vraagstelling is in 2020 iets veranderd. Vanaf dat jaar is het mogelijk de optie 'niet van toepassing' te gebruiken. In de jaren daarvoor was deze mogelijkheid er niet en moesten bedrijven aangeven of de ICT-veiligheidswerkzaamheden werden uitgevoerd of werden uitbesteed (of een mix daarvan). De verandering is waarschijnlijk de oorzaak van de verschuiving die zichtbaar is in de resultaten vanaf 2020, vooral onder de kleine bedrijven. Daarom wordt vooral gekeken naar de ontwikkeling voor bedrijven die ICT-veiligheidswerkzaamheden geheel uitbesteden (categorie 'Extern'). Deze groep lijkt redelijk constant gebleven te zijn over de overgelopen drie jaren. ZZP'ers besteden de ICT-veiligheidswerkzaamheden het minst vaak volledig uit. Het aandeel bedrijven dat deze vraag als 'niet van toepassing' aanduidt, is het grootst.

Bij grote bedrijven komt het vaker voor dat het eigen personeel in ieder geval een deel van de ICT-veiligheidsmaatregelen uitvoert. Bovendien komt 'Niet van toepassing' bij grote bedrijven nauwelijks voor. Dit is niet opmerkelijk omdat een groot bedrijf meer personeel beschikbaar heeft om standaard maatregelen zelf uit te voeren en daarnaast over de middelen beschikt om complexere zaken uit te besteden.

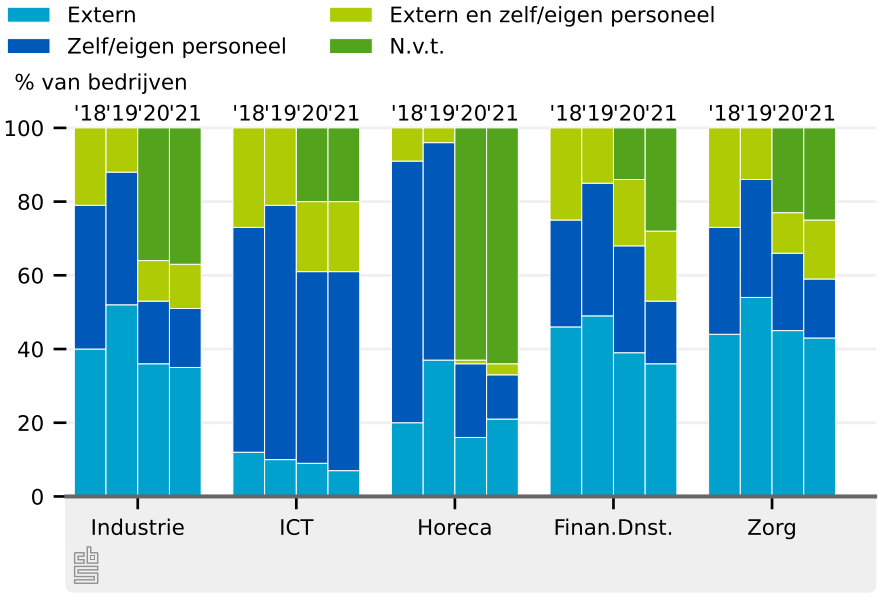
Als we in figuur 2.1.5(b) naar de uitvoering van ICT-veiligheidswerkzaamheden per bedrijfstak kijken, kunnen we zien dat ICT-bedrijven in de meeste gevallen prima in staat zijn alle ICT-beveiliging zelf te doen; zo'n 70 procent van de ICT-bedrijven doet de ICT-beveiliging volledig zelf. Ook dit is niet opmerkelijk omdat je kan verwachten dat bij bedrijven in de ICT-sector voldoende expertise voorhanden is om de ICT-beveiliging zelf te doen. In de Zorg en in de Industrie worden de ICT-beveiligingswerkzaamheden in de helft van de gevallen uitbesteed. De Horeca heeft het meest gebruik gemaakt van de nieuwe categorie 'Niet van toepassing': bijna 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.

2.1.5 Uitvoering ICT-veiligheidswerkzaamheden voor de periode 2018-2021 per grootteklasse (a) en bedrijfstak(b)

(a) grootteklasse



(b) Bedrijfstak



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

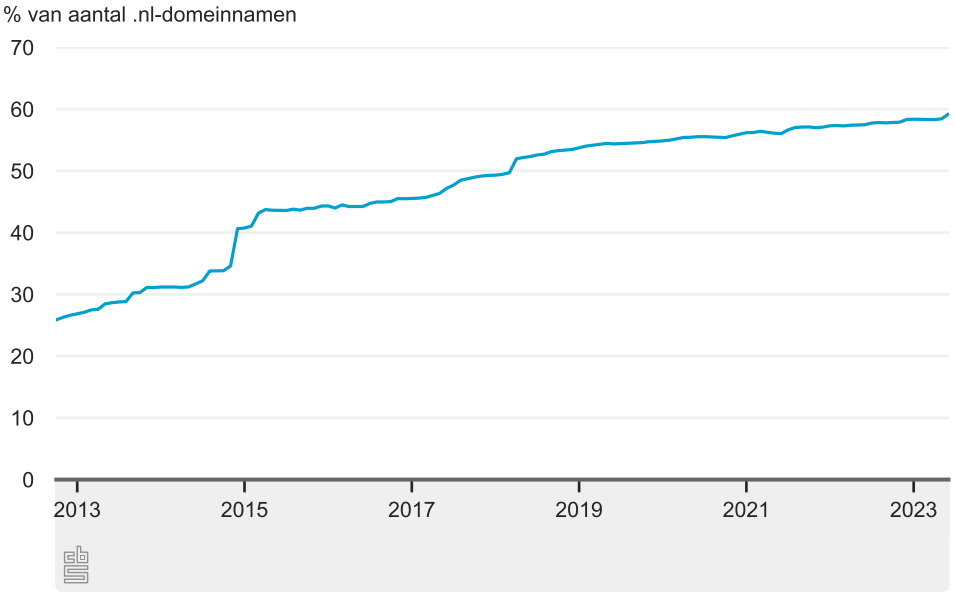
2.2 Websites

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 DNS (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).

2.2.1 Percentage .nl-domeinnamen met DNSSEC



Bron: SIDN (2023)

Tenslotte toont figuur 2.2.1) dat tussen eind april 2012 en eind juni 2023 is het percentage met DNSSEC-beveiligde *.nl*-websites continu toegenomen tot 59 procent. In de eerste jaren van deze periode was deze toename wel sneller dan in de latere jaren.

4) Bij *pharming* probeert een cybercrimineel gegevens van gebruikers te verkrijgen door ze naar een nep-versie 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.

Gebruik van internetstandaarden bij websites van bedrijven in Nederland

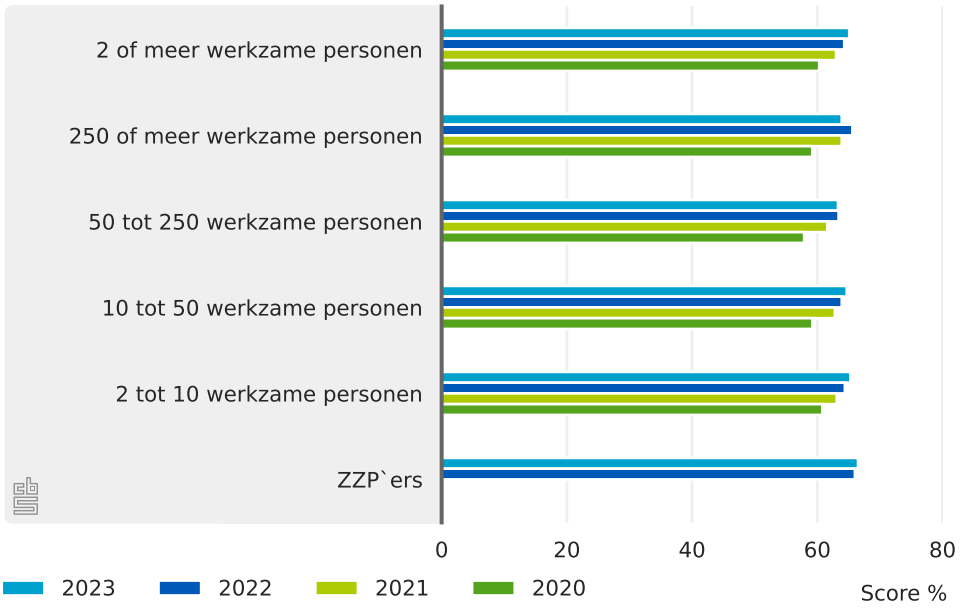
In de publicatie **?** wordt een representatieve steekproef van websites van bedrijven met de webtool Internet.nl van Platform Internetstandaarden gescand om de mate van standaardisatie van websites van bedrijven in Nederland te bepalen. De mate van standaardisatie van websites wordt met de webtool Internet.nl van Platform Internetstandaarden de mate van standaardisatie 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 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 even hoog en neemt per jaar gestaag toe (Figuur 2.2.2). De gemiddelde Internet.nl-eindscore voor alle bedrijven met website met 2 of meer werknemers is gestegen van 60,3% in 2020 naar 65,8% in 2023. Dit toont aan dat bedrijven in Nederland steeds beter de juiste internetstandaarden voor hun website toepassen.

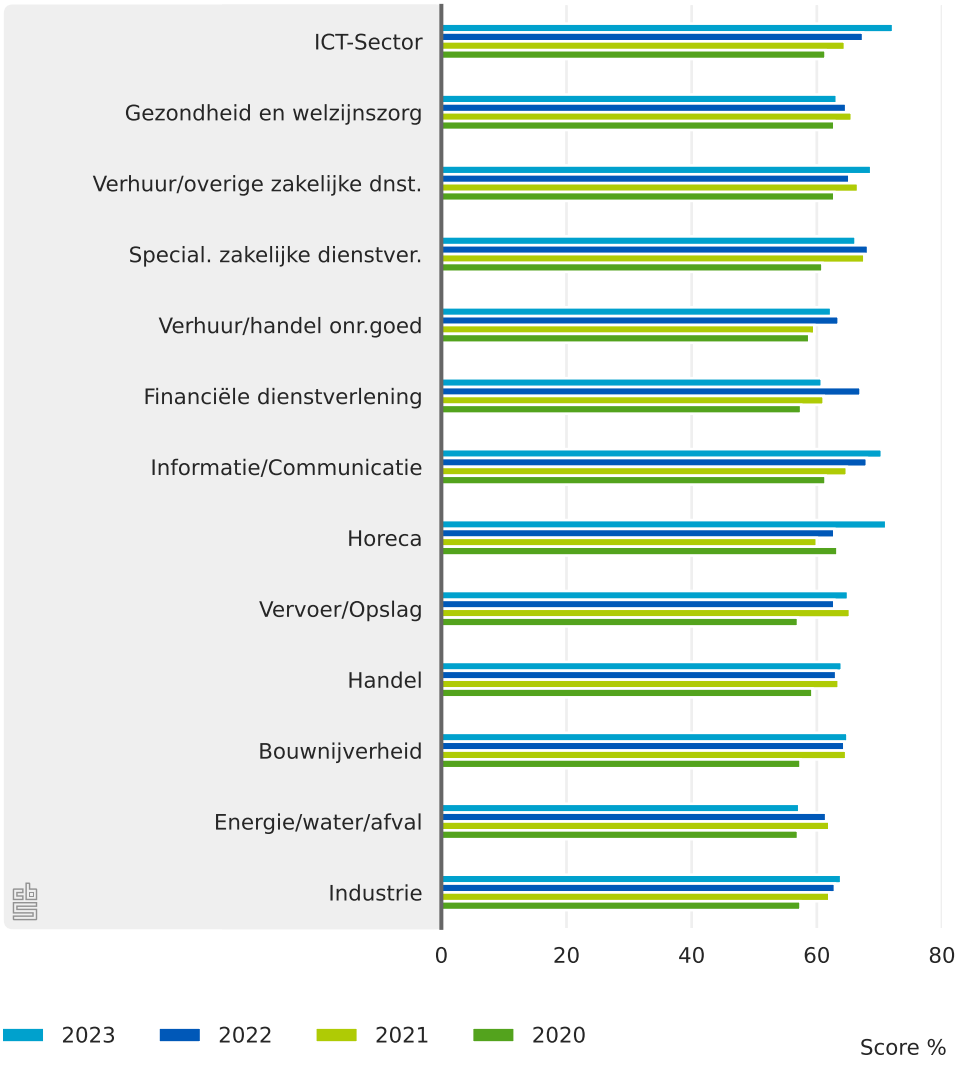
De Internet.nl eindscore per bedrijfstak vertoont ook een stijging over de periode tussen 2020 en 2023 (Figuur 2.2.3). Met name in de ICT-sector is relatief een grote stijging te zien, met een gemiddelde Internet.nl-eindscore van 61,4% in 2020 naar score van 72,2% in 2023. Ook de Horeca en Industrie vertonen een opvallende toename over deze periode.

2.2.2 Gemiddelde Internet.nl-eindscore per bedrijfsgrootteklasse.



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.

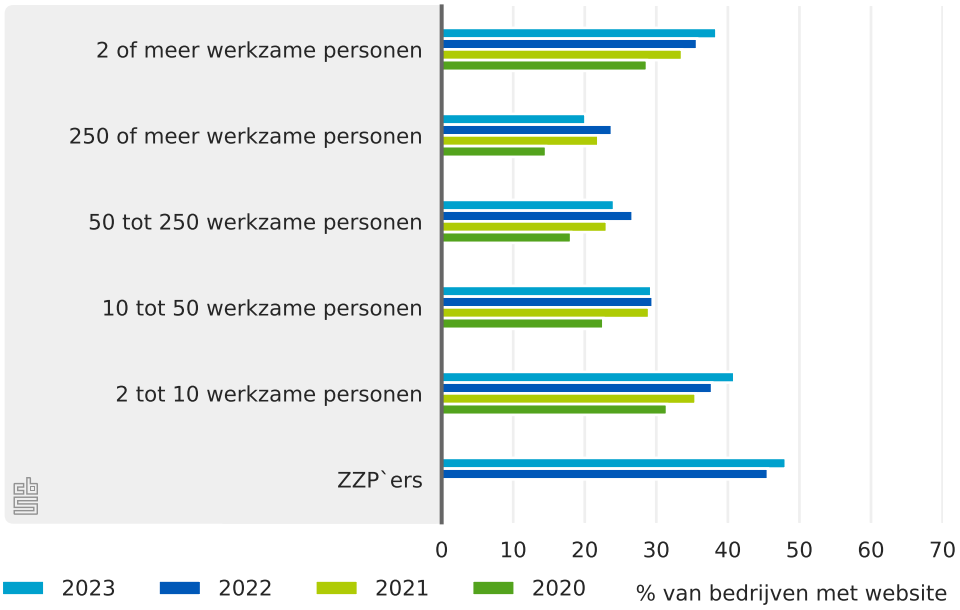
2.2.3 Gemiddelde Internet.nl-eindscore per bedrijfstak.



Kleine 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. Kleine bedrijven hebben bijvoorbeeld vaker een website die bereikbaar via een modern internetadres IPv6 (Figuur 2.2.4). 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 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. Kleine bedrijven *hosten* hun website vaak op externe service providers die vaak wel vaak hun servers met de meest moderne protocollen ingericht hebben.

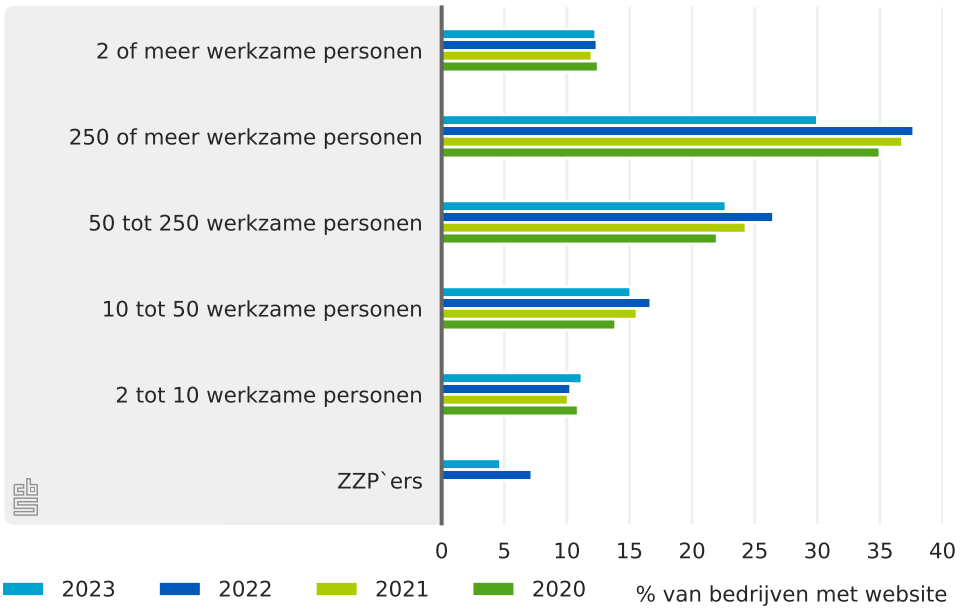
2.2.4 Percentage van bedrijven met een website bereikbaar via een modern internetadres (IPv6) per bedrijfsgrootteklasse.



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 goed op score 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 maak je gebruik van de hardware van de webserver, terwijl ondersteuning van HSTS vereist dat op netwerkniveau een IT-specialist de juiste instellingen gekozen heeft.

Zie voor een volledig overzicht van alle internetstandaarden de publicatie Toepassing van Internetstandaarden voor websites van bedrijven (**?**).

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 gewone 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). We praten dus over strafbare feiten gepleegd door cybercriminelen. Denk hierbij bijvoorbeeld aan aan 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.

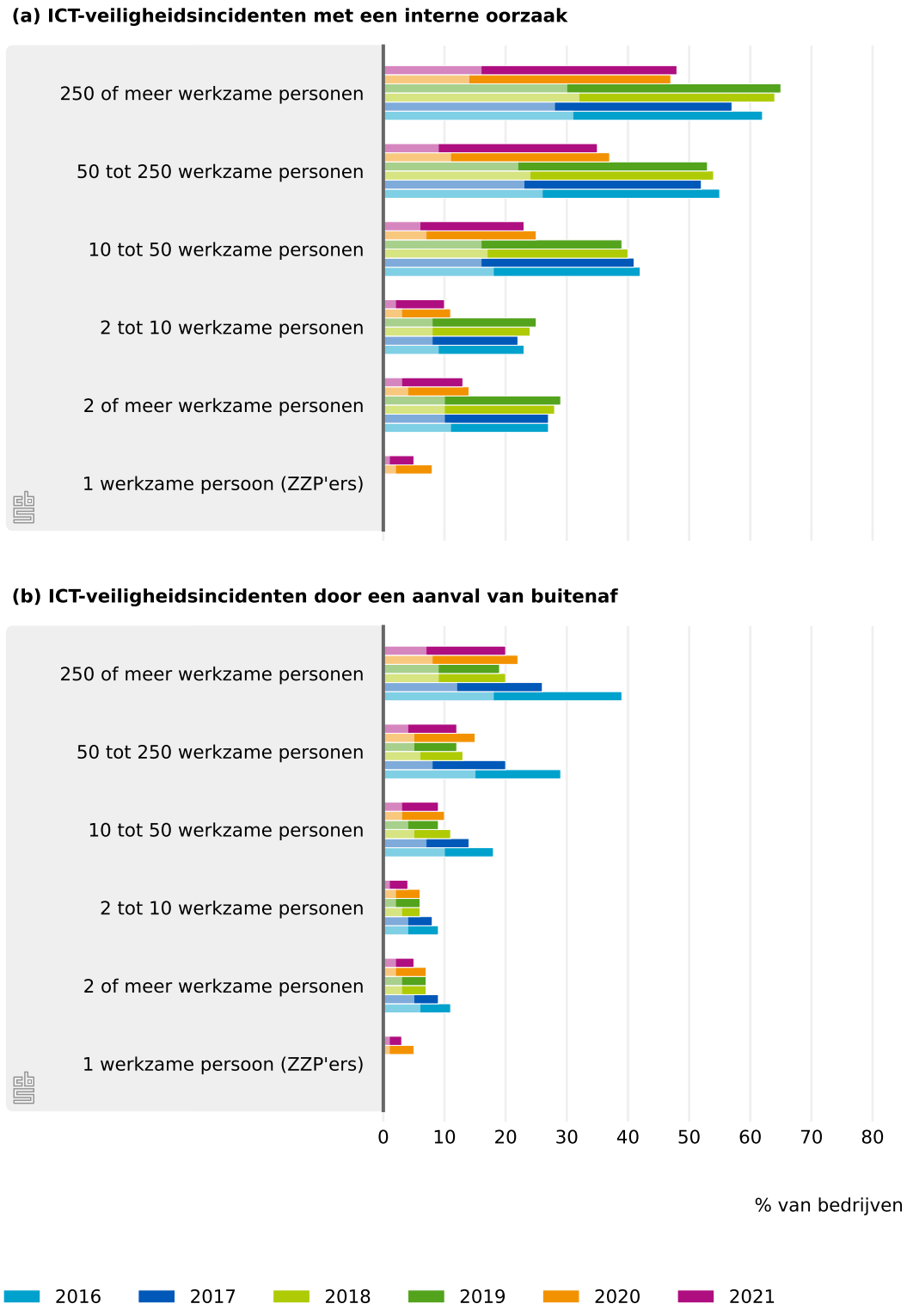
De drie ICT-veiligheidsincidenten door een *aanval van buitenaf* zijn:

1. *Uitval van ICT-systeem* ten gevolge van een aanval van buitenaf, zoals een DDoS of Ransomware-aanval 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

4. *phishing* en *pharming*.

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



Lichtgekleurde deel: incidenten met kosten

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

Cybersecurityincidenten per grootteklasse

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 wordt gevraagd of er kosten werden gemaakt ten gevolge van de ICT-veiligheidsincidenten. Deze vragen zijn inmiddels zes opeenvolgende jaren voorgelegd. We kijken nu eerst naar de In het volgende deel worden eerst de resultaten per grootteklasse 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 voor de periode 2016–2021 per grootteklasse het percentage van bedrijven getoond dat minstens één ICT-veiligheidsincident heeft gehad als gevolg van respectievelijk een interne oorzaak of een aanval van buitenaf. 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. Dit patroon kan meerdere oorzaken hebben. Bij de interne incidenten, zoals uitval van ICT-systemen door hardware of software storingen, speelt mee dat grote bedrijven vaker een grote, meer complexe ICT-infrastructuur hebben. Een groter aantal computers of meer hardware binnen het bedrijf gaat gepaard met een grotere kans op schade aan één van de systemen. Wat betreft de incidenten door een aanval van buitenaf lijkt het aannemelijk dat grote bedrijven een grotere interesse hebben van cybercriminelen omdat er meer te halen valt of de (publiciteits) schade groter is. Wat verder een rol kan spelen, is dat grote bedrijven vaak meer ICT-specialisten in dienst hebben, waardoor de kans op detectie van ICT-veiligheidsincidenten waarschijnlijk groter is.

Aantal bedrijven met ICT-veiligheidsincidenten neemt af

Figuren 3.1.1(a) en 3.1.1(b) laten een afname zien van het totaal aantal ICT-veiligheidsincidenten met zowel een interne oorzaak als door een aanval van buitenaf. Deze daling was zichtbaar onder bedrijven in alle grootteklassen. Voor de incidenten met een interne oorzaak is dit niet overal duidelijk, zeker niet voor de grootste bedrijven: bij deze groep zien we een toename over de jaren 2017–2019, gevolgd door weer een afname voor de jaren 2020–2021. Dit zou te maken kunnen hebben met het feit dat interne incidenten niet per se te voorkomen zijn: een kapot hardware onderdeel is iets wat nu eenmaal kan ontstaan.

Ook valt voor een deel deze daling te verklaren door de iets nauwere formulering van de categorie ‘dataonthulling door eigen personeel’. Vanaf 2020 is daar duidelijk bij vermeld dat het uitdrukkelijk gaat om *onopzettelijke* dataonthulling door eigen personeel, en niet om opzettelijk toedoen. In dat laatste geval valt het incident onder dataonthulling als gevolg van een aanval van buitenaf, omdat het hoort bij de categorie cybercrime. Door de duidelijkere omschrijving dat het gaat om onopzettelijke handelingen van eigen personeel, is het mogelijk dat dit heeft geleid tot een afname van incidenten in deze categorie

Voor de ICT-veiligheidsincidenten door een aanval van buitenaf is de afname voor alle grootteklassen over de periode 2016–2019 waar te nemen. In het jaar 2020 is juist weer een lichte toename van ICT-veiligheidsincidenten door een aanval van buiten te zien, wat in het laatste jaar 2021 weer iets daalt. Zo is te zien dat in 2016 bijna 40 procent van de grote bedrijven (250 of meer werknemers) met een ICT-veiligheidsincident door een aanval van

buitenaf te maken heeft gehad, terwijl dat in 2019 was afgenomen tot 19 procent. In 2020 steeg het aantal grote bedrijven dat een ICT-veiligheidsincident door een aanval van buitenaf meldde tot 22 procent, maar in 2021 daalde dit weer tot 20 procent.

De helft van de ICT-veiligheidsincidenten gaat gepaard met kosten

Wat figuren 3.1.1(a) en 3.1.1(b) ook laten zien is dat lang niet alle ICT-veiligheidsincidenten met kosten gepaard gaan. Ongeveer de helft van de bedrijven die ICT-veiligheidsincidenten hadden, ging dat gepaard met kosten. Voor 2020 en 2021 is het aandeel bedrijven met kosten zelfs nog wat gedaald vergeleken met het jaar daarvoor. In 2020 en 2021 gaat nog maar ongeveer een derde van de ICT-veiligheidsincidenten gepaard met kosten.

Ook als alleen naar de incidenten met kosten gekeken wordt, is te zien dat het aantal meldingen gehalveerd is: in 2016 gaf 19 procent van de grote bedrijven aan een ICT-veiligheidsincident met kosten gehad te hebben, terwijl dat in 2020 nog maar 9 procent was. In 2021 is dit nog wat verder afgenomen: bij 8 procent van de grote bedrijven vond een ICT-veiligheidsincident door een aanval van buitenaf plaats dat met kosten gepaard ging. Deze afname van het aantal ICT-veiligheidsincidenten door een aanval van buitenaf is waarneembaar voor alle grootteklassen. Toch zal verderop aangetoond worden dat deze afname wel iets genuanceerder bekeken moet worden, omdat het beeld is samengesteld uit drie verschillende soorten incidenten en de ontwikkelingen per type incident verschillen.

Het is dus vaak het geval dat er wel sprake was van een ICT-veiligheidsincident, maar dat dit niet direct heeft geleid tot kosten. Dit geldt voor zowel incidenten met een interne oorzaak als incidenten als gevolg van een aanval van buitenaf. Vanaf 2020 wordt aan bedrijven ook gevraagd hoe hoog de kosten waren als percentage van de omzet; deze resultaten worden later in dit hoofdstuk besproken.

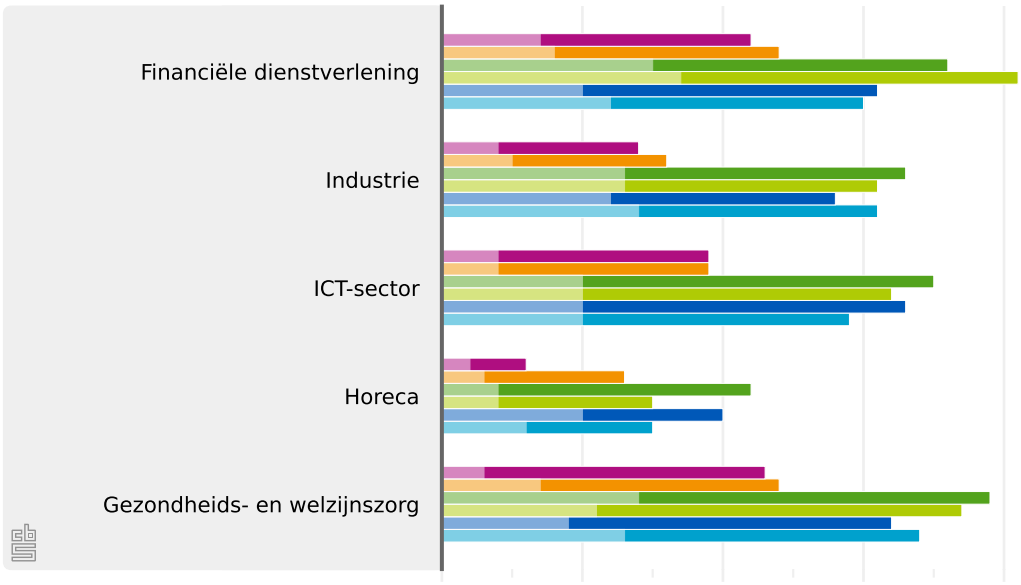
Cybersecurityincidenten per bedrijfstak

In figuren 3.1.2(a) en 3.1.2(b) wordt voor de periode 2016–2021 de aantallen ICT-veiligheidsincidenten met een interne oorzaak of door een aanval van buitenaf per bedrijfstak gespecificeerd voor bedrijven met twee of meer werknemers. Het lichtgekleurde deel van de staafdiagrammen geeft het percentage van bedrijven weer dat aangeeft dat er ook kosten aan de ICT-veiligheidsincidenten verbonden waren.

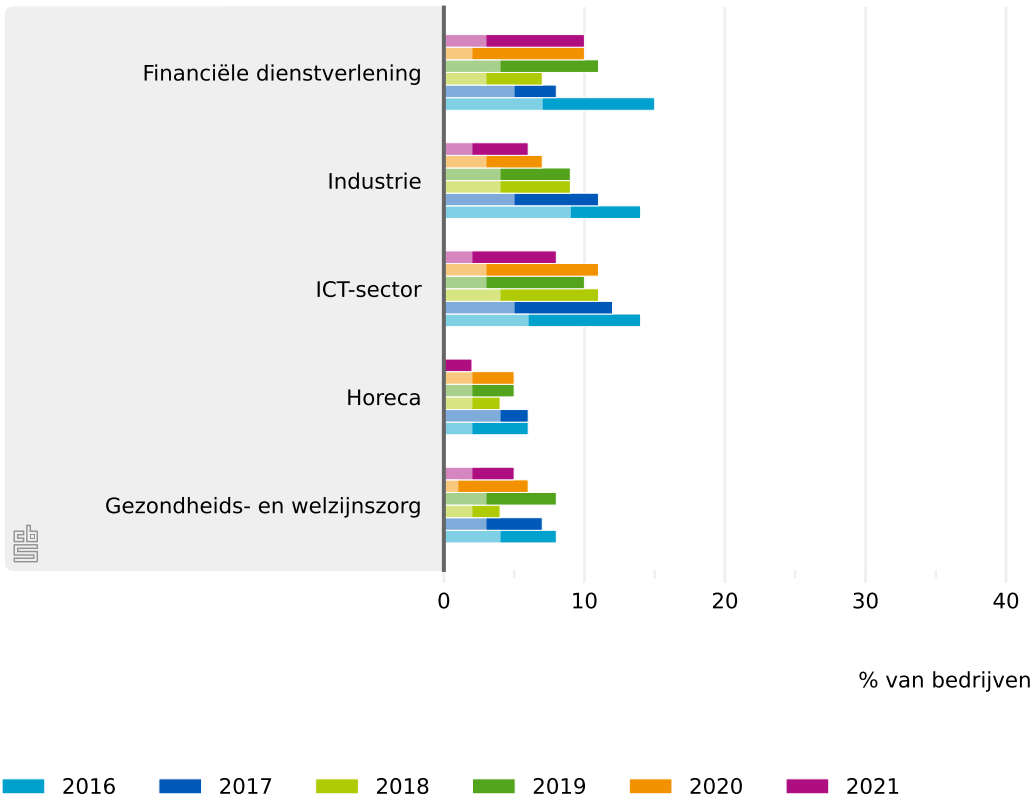
Het aandeel bedrijven met een intern ICT-veiligheidsincident is in 2020 en 2021 behoorlijk afgenomen ten opzicht van 2019. Ook hier wordt de trend mogelijk deels verklaard door kleine aanpassing in de vraagstelling. Voor de bedrijfstakken ‘Gezondheids- en welzijnszorg’ en ´Financiële dienstverlening’ is in figuur 3.1.2(a) te zien dat in 2020 en 2021 ruim 20 procent van de bedrijven een intern incident heeft gemeld, waarvan weer ongeveer de een derde kosten met zich meebracht. De Industrie en ICT-sector zitten juist iets onder die 20 procent interne ICT-veiligheidsincidenten, opnieuw met ongeveer een derde van die incidenten die ook met kosten gepaard gaan. Alleen de horeca had aanzienlijk minder interne incidenten: in 2020 had 13 procent van de horecabedrijven een ICT-veiligheidsincident met interne oorzaak, wat in 2021 nog verder afgenomen is naar 6 procent. De interne incidenten met kosten zijn daar wederom ongeveer een derde van. Op zich is dit niet vreemd omdat in de horeca waarschijnlijk minder met een computer gewerkt wordt, zodat de kans op uitval door een hardware- of softwarestoring ook kleiner is.

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.

(a) ICT-veiligheidsincidenten met een interne oorzaak



(b) ICT-veiligheidsincidenten door een aanval van buitenaf



Lichtgekleurde deel: incidenten met kosten

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

Opnieuw zien we bij de industrie dat het percentage van bedrijven dat een incident door een aanval van buitenaf meldt over de laatste zes jaar afgenomen is. Bij de ICT-bedrijven is er in 2020 een kleine toename te zien ten opzicht van 2019 van het aantal bedrijven dat een ICT-veiligheidsincidenten door een aanval van buiten meldt, maar in 2021 is neemt het percentage bedrijven dat een ICT-veiligheidsincident door een aanval van buiten meldt weer af. Ook het aandeel ICT-veiligheidsincidenten gepaard met kosten neemt af, ook relatief ten opzichte van het totaal aantal ICT-veiligheidsincidenten.

Voor incidenten door een aanval van buitenaf (figuur 3.1.2(b)), vinden we vooral lage percentages bedrijven die hier melding van maken: voor bedrijven uit de Financiële dienstverlening ging het in 2021 om 3 procent van de bedrijven; voor bedrijven uit de ICT-sector, de Industrie en de Gezondheids- en welzijnssector was het 2 procent van de bedrijven; en bedrijven uit de Horeca melden helemaal geen ICT-veiligheidsincidenten waaraan kosten verbonden waren.

Cybersecurityincidenten per type incident

In dit deel wordt nagegaan wat de bijdragen van de drie afzonderlijke type incidenten zijn: uitval, datavernietiging en dataonthulling.

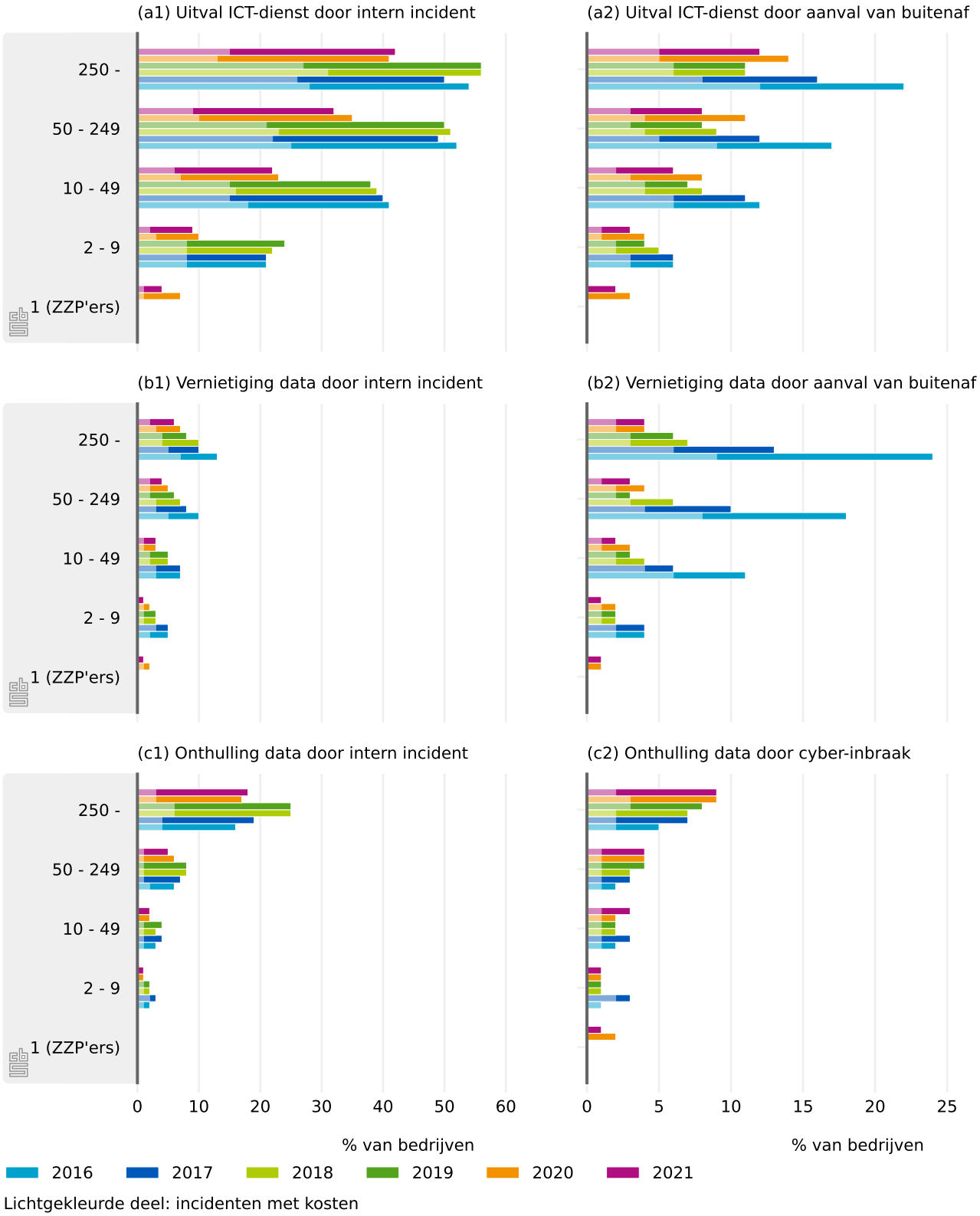
Cybersecurityincidenten per type incident per grootteklasse

In figuren 3.1.3(a1–c1) toont de linker kolom de interne ICT-veiligheidsincidenten voor respectievelijk uitval van ICT-systemen, datavernietiging en dataonthulling per grootteklasse. Figuren 3.1.3(a2–c2) geven de incidenten door een aanval van buitenaf voor dezelfde drie typen incidenten per grootteklasse.

Voor de interne incidenten zijn de eerder gevonden daling in het aandeel bedrijven met een intern ICT-incident ook terug te zien in de onderliggende specifiekere categoriëen van incidenten. Er was eerder al geconcludeerd dat het aandeel bedrijven met een interne incidenten toeneemt met de bedrijfsgrootte. Als we naar de drie typen interne incidenten kijken dan zien we dat deze toename voornamelijk toe te schrijven is aan de uitval van ICT-systemen door een hardware- of softwarestoring, zoals te zien is in figuur 3.1.3(a1): ongeveer 9 procent van de kleine bedrijven had in 2021 een uitval door een storing, terwijl dit voor grote bedrijven zo'n 42 procent was. Beide percentages zijn een stuk lager dan de in 2019 gemeten percentages (respectievelijk 24 en 56 procent).

Datavernietiging door een hardwarestoring komt bij minder dan 10 procent van de bedrijven voor; bovendien is de samenhang met de grootte van het bedrijf minder sterk aanwezig. Wel is te zien dat ook dataonthulling vaker bij grote dan bij kleine bedrijven voorkomt, maar omdat het aantal bedrijven met dergelijke incidenten gering is, draagt deze categorie een stuk minder bij aan het totaal van interne incidenten. De ontwikkeling over de tijd is voor de interne incidenten minder eenduidig en varieert naar categorie. Voor dataonthulling door een intern incident, getoond in figuur 3.1.3(c1), is tot voor 2020 een *toename* over de tijd te zien voor de grote bedrijven van 250 of meer werknemers, terwijl vanaf 2020 weer afneemt. Dit is

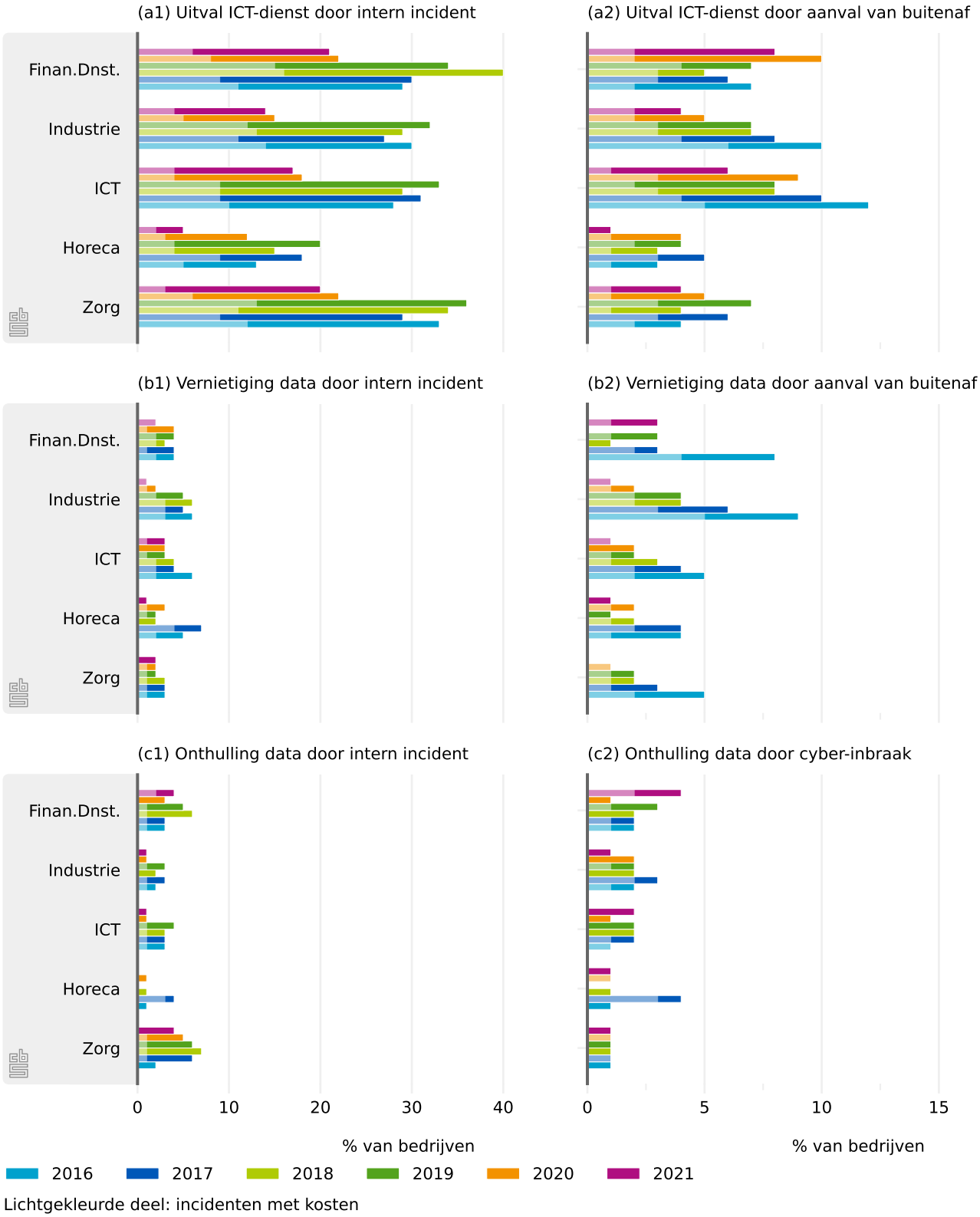
3.1.3 ICT-veiligheidsincidenten per categorie per grootteklasse.



Lichtgekleurde deel: incidenten met kosten

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

3.1.4 ICT-veiligheidsincidenten per categorie per bedrijfstak.



Lichtgekleurde deel: incidenten met kosten

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

anders dan de ontwikkeling voor het totaal aan interne incidenten. De ontwikkelingen variëren dus sterk naar type incident.

Figuur 3.1.3(a2–c2) laat zien dat alle typen incidenten als gevolg van een aanval van buitenaf vaker voorkomen bij grote bedrijven. Dit komt overeen met het eerder beschreven patroon voor het totaal van incidenten door een aanval van buitenaf. Dit is alleen toe te schrijven aan de afname van uitval van ICT-systemen en vernietiging van data door een aanval van buitenaf. Het aantal bedrijven dat dataonthulling als gevolg van een cyberinbraak meldt, is echter weer toegenomen over de afgelopen vier jaar, vooral als er naar de grote bedrijven gekeken wordt. Er kan dus geconcludeerd worden dat alleen kijkend naar de cijfers voor dataonthulling, we een toename van het aantal incidenten zien. Dit neemt echter niet weg dat als we de incidenten van datavernietiging en uitval van ICT-systemen meenemen, het aantal incidenten over de jaren afgenomen is.

Cybersecurityincidenten per type incident per bedrijfstak

Figuren 3.1.4(a1–c1) toont de linker kolom de interne ICT-veiligheidsincidenten voor respectievelijk uitval van ICT-systemen, datavernietiging en dataonthulling per bedrijfstak. Figuren 3.1.4(a2–c2) geven de incidenten door een aanval van buitenaf voor dezelfde drie typen ICT-veiligheidsincidenten per bedrijfstak. Net als we bij afname van ICT-veiligheidsincidenten per grootteklasse zien we dat voor de meeste bedrijfstakken een afname van het percentage van bedrijven per bedrijfstak dat een ICT-veiligheidsincident met een interne oorzaak en door een aanval van buiten meldt. Voor grote bedrijven zien we een stijging in het percentage bedrijven binnen de categorie ‘Onthulling door cyberinbraak’. Deze toename is alleen zichtbaar binnen de Financiële dienstverlening.

Kostenverdeling van de ICT-veiligheidsincidenten

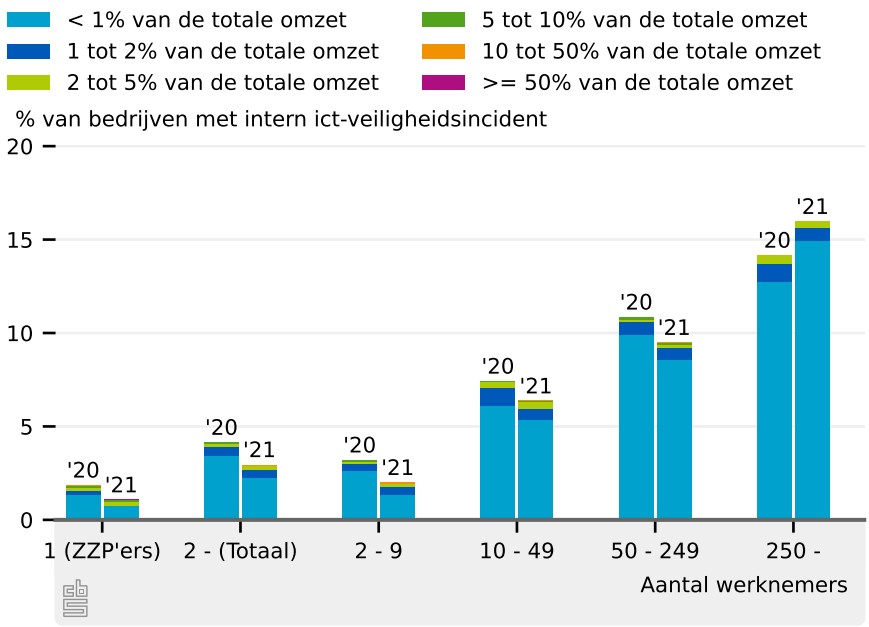
Kostenverdeling van ICT-veiligheidsincidenten met interne oorzaak

Tenslotte wordt gekeken naar de hoogte van de kosten van de ICT-veiligheidsincidenten als percentage van de omzet. Figuren 3.1.5(a) en 3.1.5(b) tonen de hoogte van de kosten van de interne ICT-veiligheidsincidenten per grootteklasse en bedrijfstak voor de laatste referentiejaren 2020 en 2021. De hoogte van de samengestelde staafjes geeft het percentage bedrijven weer met kosten die volgden uit een intern ICT-veiligheidsincident en komen dus overeen met de hoogte van de lichtgekleurde delen van de staafjes die in de grafieken 3.1.1(a) en 3.1.2(a) te zien waren. Dit keer wordt met kleur aangegeven hoe hoog deze kosten waren als percentage van de omzet van het bedrijf opgedeeld in 6 categorieën: ‘minder dan 1 %’, ‘1 tot 2 %’, ‘2 tot 5 %’, ‘5 tot 10 %’, ‘10 tot 50 %’ en ‘50 % of meer’ van de totale omzet. In de meeste gevallen waren de kosten minder dan 1 procent van de bedrijfsomzet: voor 3 op de 4 bedrijven met 2 of meer werknemers die een ICT-veiligheidsincident met kosten hadden. Daarnaast waren de kosten vaak tussen de 1 en 2 procent of tussen de 2 en 5 procent van de omzet. Voor grote bedrijven gaat hier dan, gezien de hogere omzet, om grote bedragen. In 2022 meldt 3 procent van de kleine bedrijven met 2 tot 10 werknemers die een ICT-veiligheidsincident gehad hebben, dat de kosten tussen 10 tot 50 % van de omzet waren. Dit impliceert dat het incident een behoorlijke grote impact op het bedrijf heeft gehad.

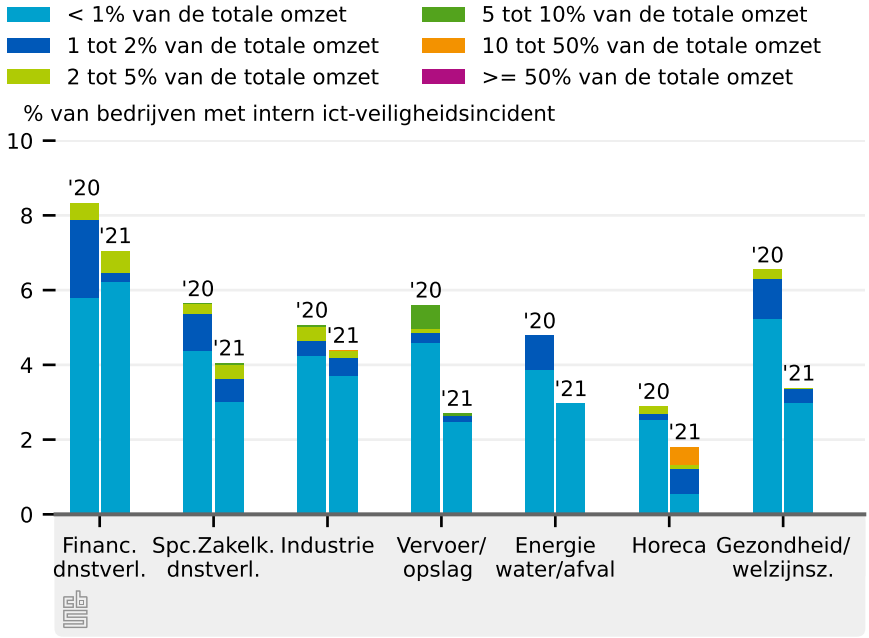
Figuur 3.1.5(b) laat dezelfde kostenverdeling voor interne ICT-veiligheidsincidenten per bedrijfstak zien. Hierbij worden alle bedrijven met 2 of meer werknemers meegenomen (ZZP

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)

dus niet). Meest opvallend is dat er relatief veel interne ICT-veiligheidsincidenten in de Financiële sector zijn, met ook relatief veel incidenten met kosten hoger dan 1 procent van de omzet. De Horeca heeft in 2021 te maken met de hoogste kosten bij interne ICT-incidenten: bij 1 op de 4 Horeca bedrijven die een intern ICT-veiligheidsincident met kosten hadden, waren de kosten tussen 10 en 50% van de totale omzet. Dit hangt samen met het feit dat de horeca veel kleine bedrijven bevat met een relatief lage omzet, zodat de kosten van ICT-veiligheidsincidenten eerder een groter percentage van de omzet omvat.

Kostenverdeling van ICT-veiligheidsincidenten door aanval van buitenaf

Figuren 3.1.6(a) en 3.1.6(b) geven de kostenverdeling van de ICT-veiligheidsincidenten door een aanval van buitenaf per grootteklasse en bedrijfstak weer. De hoogte van de samengestelde staafjes geeft dit keer het percentage bedrijven weer met kosten die volgden uit ICT-veiligheidsincident door een aanval van buiten en komen dus overeen met de hoogte van de lichtgekleurde delen van de staafjes in de grafieken 3.1.1(b) en 3.1.2(b). Zoals we al eerder gezien hebben, is het percentage van bedrijven met een ICT-veiligheidsincident ten gevolge van een aanval van buitenaf over het algemeen kleiner dan het percentage van bedrijven met een incident met interne oorzaak. Figuur 3.1.6(a) laat zien dat grote bedrijven vaker kosten hebben ten gevolge van een ICT-veiligheidsincident door een aanval dan kleine bedrijven. In 2021 meldde iets minder bedrijven kosten te hebben dan in 2020. In de meeste gevallen van de incidenten bedragen de kosten minder dan 1 procent van de omzet van het bedrijf. Opvallend is dat vooral in 2020 er bedrijven waren met kosten ten gevolge van een ICT-veiligheidsincident door een aanval van buitenaf die tussen de 10 en 50 procent van de bedrijfsomzet lagen, zelfs voor de grote bedrijven van 250 of meer werknemers. Dit soort ICT-veiligheidsincidenten moeten dus een behoorlijke impact op de bedrijven hebben. In 2021 komen dit soort aanvallen niet meer voor.

De kostenverdeling van ICT-veiligheidsincidenten door een aanval van buiten per bedrijfstak wordt getoond in figuur 3.1.6(b). Deze figuur laat zien dat de Financiële dienstverlening relatief vaak dit soort incidenten heeft, ook met hoge kosten tot gevolg. Ook worden in 2021 in deze sector beduidend meer incidenten gemeld dan in 2020, met een stijging van 2,2 naar 3,4 procent van de bedrijven die kosten had door een ICT-veiligheidsincident door een aanval van buiten. Ook bedroegen de kosten in 2021 relatief vaker meer dan 1 procent van de omzet, alhoewel het in 2020 vaker voorkwam dat de kosten tussen de 10 en 50 procent van de omzet lagen.

Ransomware-aanvallen

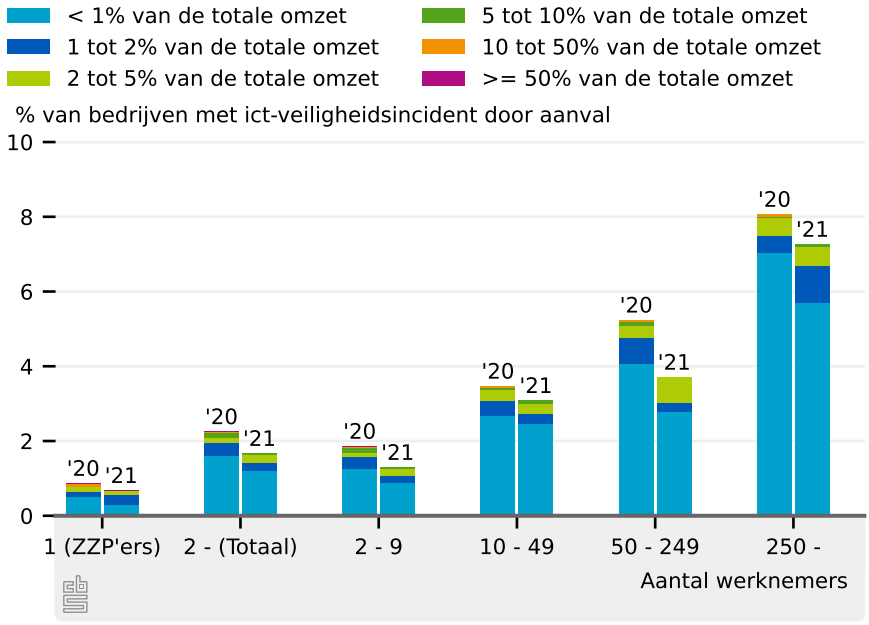
In de ‘ICT-gebruik bij bedrijven’-enquête is het afgelopen jaar ook specifiek naar ransomware-aanvallen gevraagd (CBS, 2022a). Bij een ransomware-aanval worden de ICT-systemen van een bedrijf of particulier door middel van malware geblokkeerd, om zo het slachtoffer te chanteren om losgeld (ransom) te 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 (**?**), en daarom is het belangrijk te monitoren hoe vaak dit voorkomt bij bedrijven in Nederland.

Aantal ransomware-aanvallen

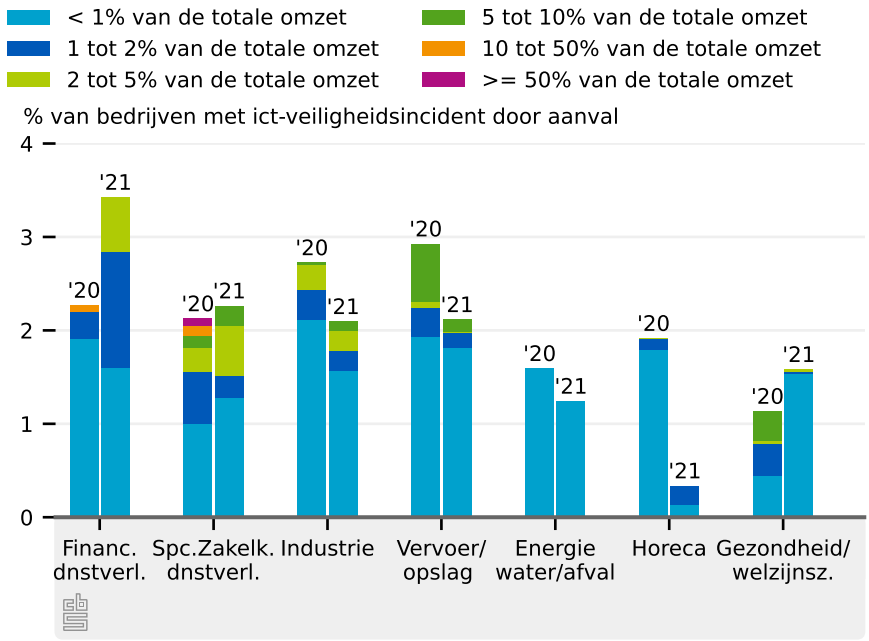
Figuur 3.1.7 laat zien dat in 2021 in totaal 6 300 ransomware-aanvallen bij bedrijven zijn geweest, waarvan 4 000 bij ZZP’ers en 2 300 bij bedrijven met 2 of meer personen. In dit

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

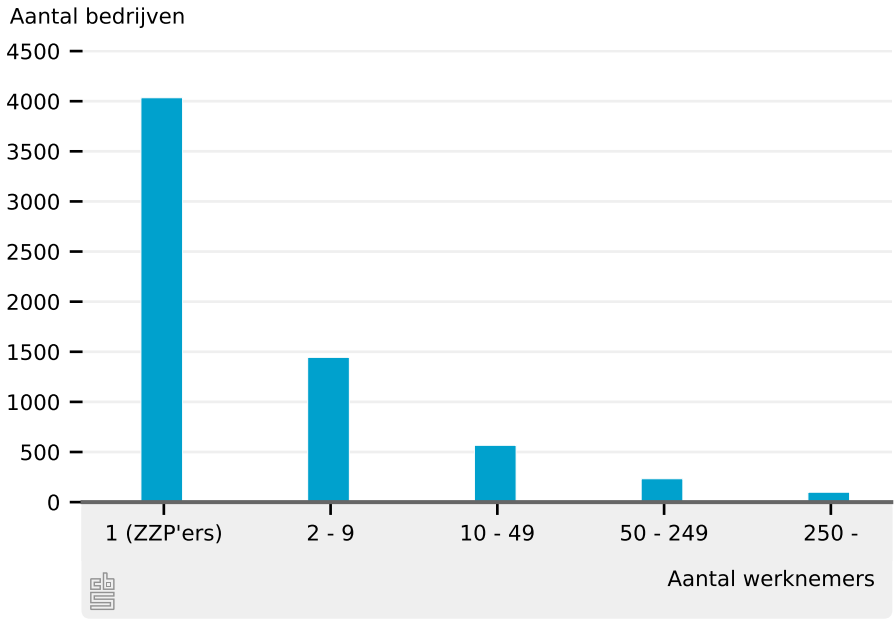


(b) Bedrijfstak



Bron: CBS (2021e, 2022a)

3.1.7 Aantal bedrijven per grootteklasse die in 2021 een ransomware-aanval gehad hebben.



Bron: CBS (2022a)

figuur wordt het aantal unieke bedrijven aangegeven dat aangeeft een Ransomware-aanval te hebben gehad, om de omvang van het probleem goed weer te geven. Tabel 3.1.8 geeft naast de absolute getallen ook het percentage van bedrijven per grootteklasse weer dat meldt een ransomware-aanval gehad te hebben.

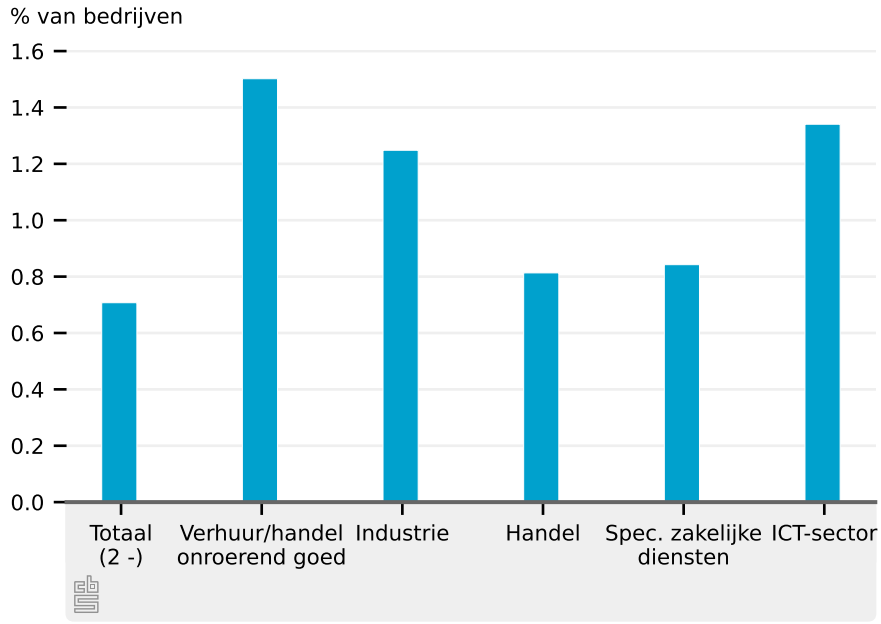
Hieruit blijkt procentueel gezien grote bedrijven meer last hebben van ransomware-aanvallen dan kleine bedrijven. Ransomware-aanvallen hebben zich bij 0,3 procent van de ZZP'ers in Nederland voorgedaan, terwijl 4 procent van de bedrijven met 250 of meer werknemers zegt een Ransomware-aanval gehad te hebben.

3.1.8 Aantal ransomware-aanvallen in 2021 per grootteklasse en het percentage per groep.

	Ransomware-aanval gehad	
Bedrijfsgrootte	Aantal	Percentage
1 werkzame persoon (ZZP'er)	4 000	0,3
Totaal (2 of meer werkzame personen)	2 300	0,7
Grote bedrijven (10 of meer werkzame personen)	900	1,5
2 tot 10 werkzame personen	1 400	0,5
10 tot 50 werkzame personen	570	1,2
50 tot 250 werkzame personen	230	2,3
250 of meer werkzame personen	100	4,0

Figuur 3.1.9 toont de percentages van bedrijven die een ransomware-aanval gehad per bedrijfstak voor bedrijven met 2 of meer werknemers. De bedrijfstak 'Verhuur en handel onroerend goed' is de bedrijfstak die het meest door ransomware getroffen is: 1,5 procent

3.1.9 Percentage van bedrijven per bedrijfstak met 2 of meer werknemers die in 2021 een ransomware-aanval gehad hebben.



Bron: CBS (2022a)

van de bedrijven uit deze sector melden een ransomware-aanval gehad te hebben. Ook de ICT-sector scoort relatief hoog. Een overzicht van alle cijfers is op Statline terug te vinden.

Bedrijven betalen meestal geen losgeld

3.1.10 Percentage van de bedrijven met in 2021 een ransomware-aanval die losgeld betaald hebben en die losgeld betaald hebben waarbij het losgeld niet geleid heeft tot het (deels) ontsleutelen van de ICT-systemen van het bedrijf.

	Losgeld betaald	
Bedrijfsgrootte	Totaal [%]	Zonder resultaat [%]
1 werkzame persoon (ZZP'er)	0,1	0,0
Totaal (2 of meer werkzame personen)	11	5,8
2 tot 10 werkzame personen	14	9,1
10 tot 50 werkzame personen	5,1	0,7
50 tot 250 werkzame personen	5,2	0,6
250 of meer werkzame personen	4,1	0,0

In tabel 3.1.10 wordt per grootteklasse weergegeven hoeveel bedrijven losgeld betaald hebben. Van alle bedrijven met 2 of meer werknemers betaalt gemiddeld 11 procent van de bedrijven losgeld. Dit komt met name door het hoge percentage van 14 procent van de kleine bedrijven met 2 tot 10 werknemers die toch besluiten losgeld te betalen. Maar ook bij de grote bedrijven van 250 of meer werknemers betaalt nog steeds 4,1 procent van de bedrijven losgeld. Alleen bij ZZP'ers lijkt het bijna niet voor te komen dat er losgeld betaald wordt. Belangrijk is ook te constateren dat voor ruim de helft van de gevallen waarbij losgeld betaald wordt, dit niet leidt tot het (deels) ontsleutelen van de ICT-systemen, omdat 5,8 procent van de bedrijven met 2 of meer werknemers die een ransomware-aanval hebben gehad zeggen na betaling niet de ICT-system ontsleuteld gekregen te hebben.

Kostenverdeling van het losgeld en andere kosten

In figuren 3.1.11(a) en 3.1.11(b) wordt per grootteklasse en bedrijfstak de verdeling van de hoogte van het losgeld gegeven als percentage van de omzet van het bedrijf. Gemiddeld voor alle bedrijven met 2 of meer werknemers betaalt 11 procent van de bedrijven losgeld. In ongeveer de helft van de gevallen bedraagt het losgeld meer dan 50 procent van de omzet. Het is te zien dat dit voornamelijk komt door de kleine bedrijven met 2 tot 10 werknemers waarbij de omzet in het algemeen lager is. De impact voor het bedrijf dat zo'n hoog percentage van de omzet aan losgeld betaalt is groot, vooral als je mee neemt dat in een groot aantal gevallen het betalen van losgeld niet leidt tot het ontsleutelen van de data van het bedrijf. Van grote bedrijven met 250 of meer werknemers betaalt ongeveer een kwart van de bedrijven die losgeld betalen een bedrag tussen 1 en 2 procent van de totale omzet. De schade voor het bedrijf kan dus behoorlijk zijn.

In figuur 3.1.11(b) is het met name opvallend dat in de 'Handel' relatief veel bedrijven losgeld betalen en dat het betaalde bedrag ook hoog is: in 70 procent van de gevallen wordt meer dan 50 procent van de omzet betaald. Dit duidt erop dat voornamelijk kleine bedrijven in de handel getroffen zijn. Inderdaad zijn het alleen de kleine Handels bedrijven met 2 tot 10 werknemers die 50 procent of meer van de omzet betalen.

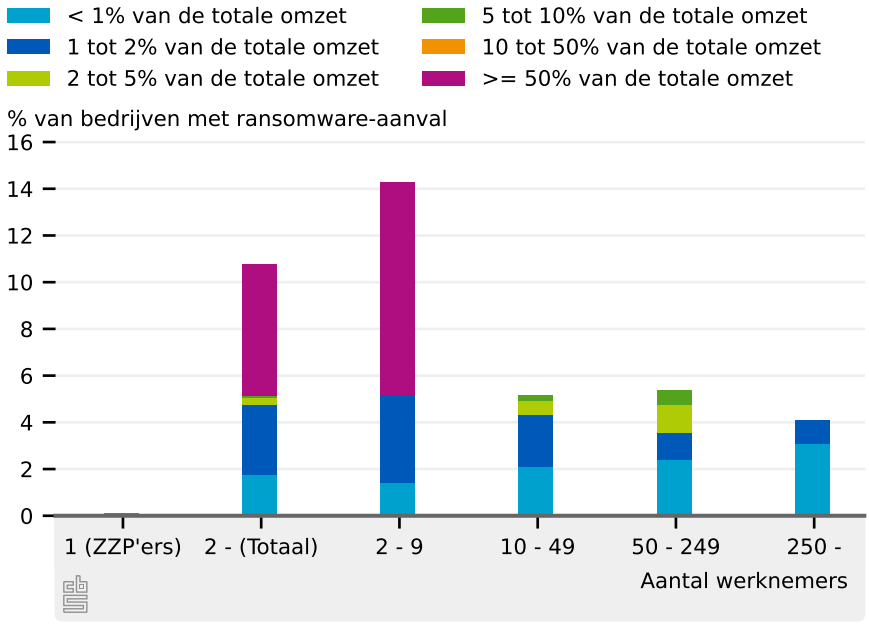
Naast losgeld kan een bedrijf natuurlijk ook andere kosten aan een ransomware-aanval overhouden, zoals bijvoorbeeld het vervangen van getroffen ICT-systemen, het inhuren van ICT-specialisten om de schade te beperken, maar ook het eventuele productieverlies ten gevolge van de ransomware-aanval. Figuren 3.1.12(a) en 3.1.12(b) geven per grootteklasse en bedrijfstak de verdeling van de overige kosten weer als gevolg van de ransomware-aanval. Het is meteen duidelijk dat bedrijven met een ransomware-aanval vaker kosten hebben aan overige zaken dan aan de betaling van losgeld. Zo is in figuur 3.1.12(a) te zien dat voor alle bedrijven met 2 of meer werknemers die een ransomware-aanval gehad hebben bijna de helft (48 procent) meldt dat ze andere kosten dan losgeld aan de aanval hebben gehad. Weer zijn deze kosten uitgesplitst naar percentages van de omzet. In de meeste gevallen blijven de kosten onder de 1 procent van de omzet, maar te zien is dat voor kleine percentages bedrijven de overige kosten behoorlijk op kunnen lopen: zo meldt bijvoorbeeld 5 procent van de bedrijven met 50 tot 250 werknemers dat de overige kosten tussen de 10 en 50 procent van de omzet van het bedrijf liggen. Als per bedrijfstak in figuur 3.1.12(b) gekeken wordt, valt op dat met name de Industrie veel andere kosten heeft aan een ransomware-aanval. Maar ook de 'Handel', 'Bouwnijverheid' en 'Speciale zakelijk dienstverlening' scoren relatief hoog.

Hulp vraag bij politie en cybersecuritybedrijven

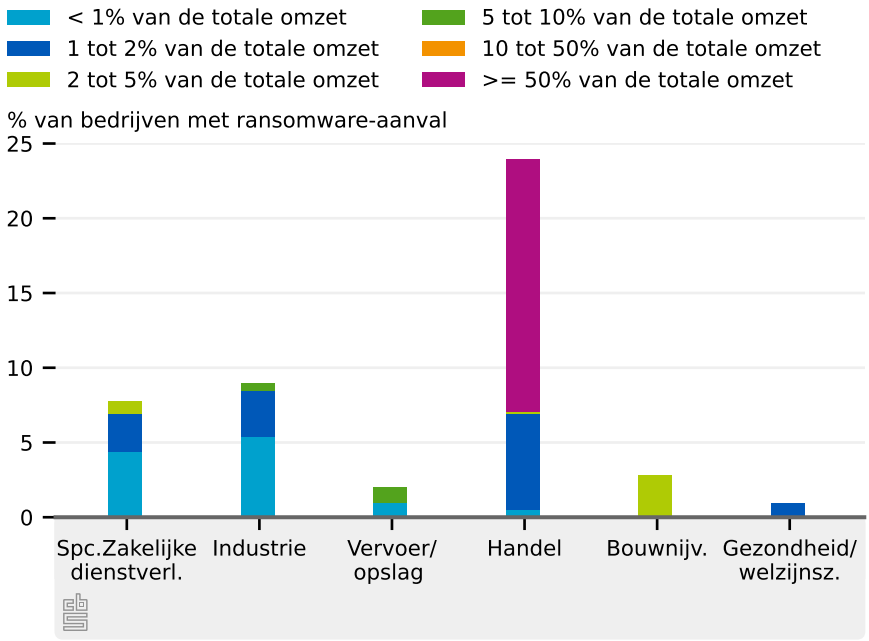
Figuur 3.1.13 toont het percentage van de bedrijven die een ransomware-aanval gehad hebben en hulp vragen bij de politie of een cybersecuritybedrijf. Van alle bedrijven met 2 of meer werknemers die een ransomware-aanval gehad hebben schakelt 39 procent de hulp in van een cybersecuritybedrijf en 13 procent stapt naar de politie. Uiteraard kan een bedrijf ook zowel naar de politie stappen als een cybersecuritybedrijf inschakelen. Het is wel opvallend dat met name kleine bedrijven minder vaak naar de politie stappen, zo'n 5 procent van de bedrijven met 2 tot 10 werknemers die een ransomware-aanval gehad hebben, tegen 33 procent die naar een cybersecuritybedrijf stapt. Bij grote bedrijven wordt nog steeds meestal de hulp van een cybersecuritybedrijf ingeroepen, maar gaat ook een groot percentage alsnog

3.1.11 Percentage van bedrijven met een ransomware-aanval die losgeld betaald hebben per grootteklasse (a) en bedrijfstak met 2 of meer werknemers (b). De percentages zijn opgesplitst naar de hoogte van het losgeld als percentage van de totale omzet.

(a) Grootteklasse



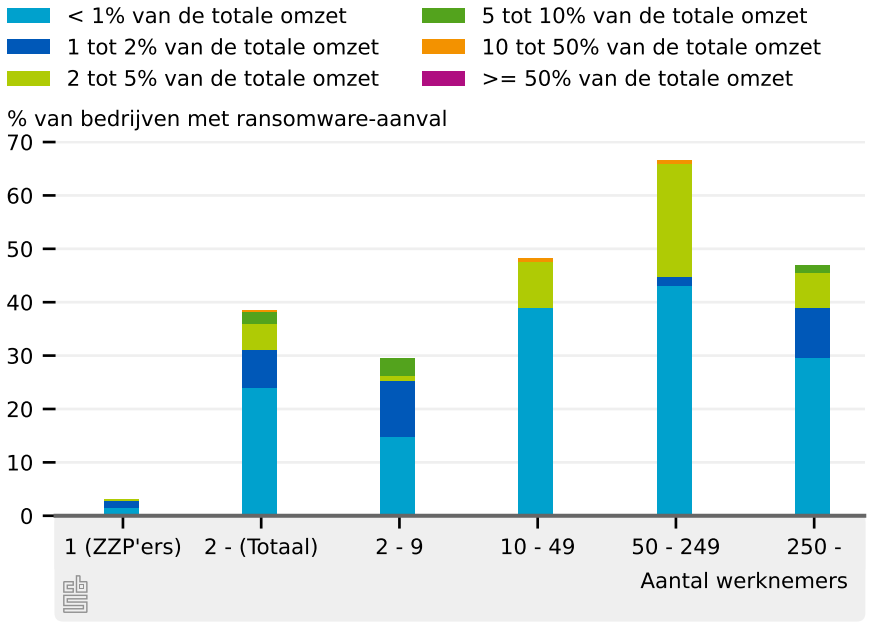
(b) Bedrijfstak



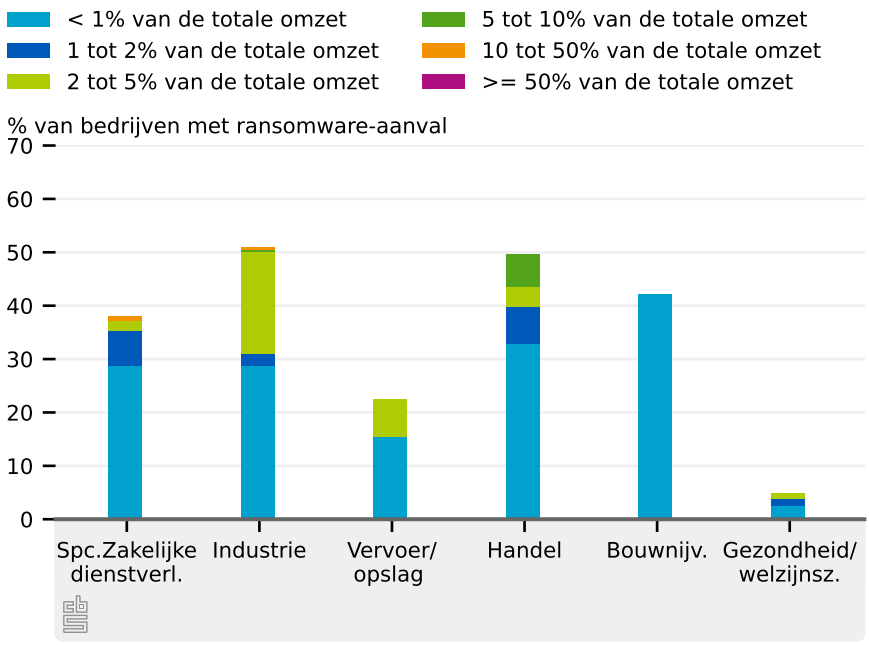
Bron: CBS (2022a)

3.1.12 Percentage van bedrijven met ransomware-aanval die andere kosten gehad hebben (anders dan losgeld) per grootteklasse (a) en bedrijfstak met 2 of meer werknemers (b). De percentages zijn opgesplitst naar de hoogte van de kosten als percentage van de totale omzet.

(a) Grootteklasse



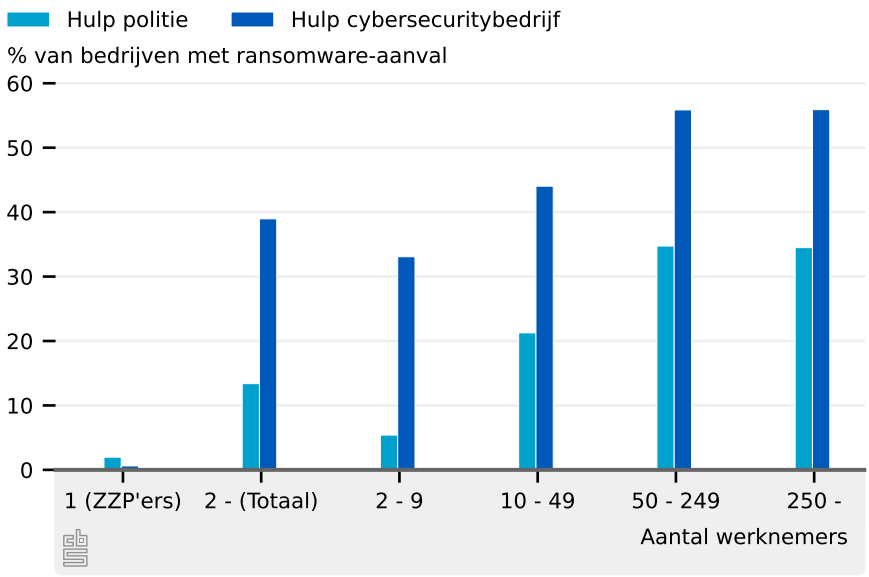
(b) Bedrijfstak



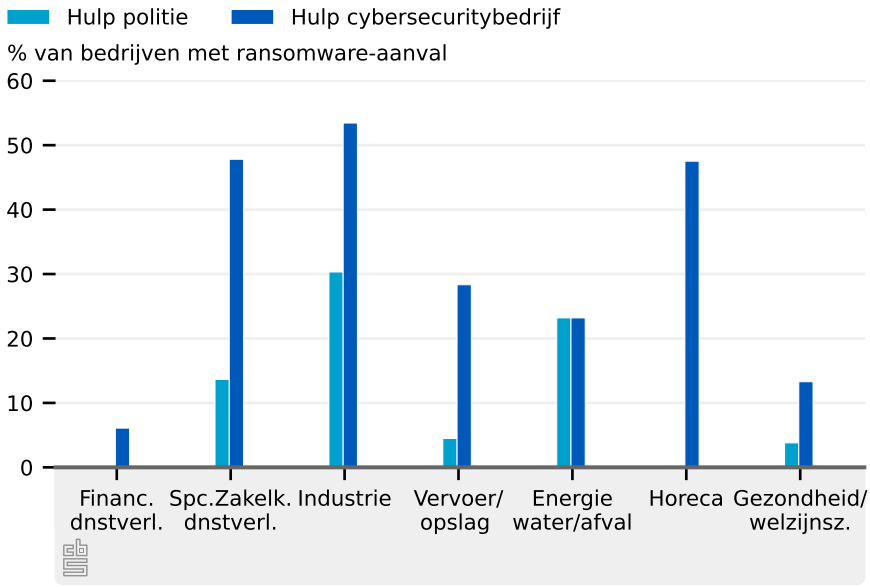
Bron: CBS (2022a)

3.1.13 Percentage van bedrijven met ransomware-aanval die de hulp hebben in geschakeld van bij politie of bij een cybersecuritybedrijf per grootteklasse (a) en bedrijfstak met 2 of meer werknemers (b).

(a) Grootteklasse



(b) Bedrijfstak



Bron: CBS (2022a)

naar de politie. De verdeling per bedrijfstak zoals in figuur 3.1.13(b) getoond laat ook zien dat bedrijfstakken andere strategieën gebruiken: in de 'Energie water/afval' wordt even vaak naar de politie gegaan als dat er een cybersecuritybedrijf ingeschakeld wordt, terwijl in de horeca en financiële dienstverlening bijna nooit naar de politie gegaan wordt.

Grote bedrijven zijn vaker verzekerd tegen ICT-veiligheidsincidenten

Ten slotte zien we in figuren 3.1.14(a) en 3.1.14(b) hoeveel bedrijven per grootteklasse en bedrijfstak een verzekering tegen ICT-veiligheidsincidenten afgesloten hebben. Van alle bedrijven met 2 of meer werknemers heeft 17 procent van de bedrijven een verzekering afgesloten tegen ICT-veiligheidsincidenten. Hoe groter het bedrijf is, hoe groter dit percentage is: slechts 5 procent van de ZZP'ers is verzekerd, terwijl van de bedrijven met 250 of meer werknemers 44 procent een verzekering tegen ICT-veiligheidsincidenten afgesloten heeft. Van de bedrijfstakken in figuur 3.1.14(b) is te zien dat voornamelijk de financiële sector met 41 procent van de bedrijven met een verzekering goed verzekerd is.

Meldingen datalekken bij Autoriteit Persoonsgegevens

Uit het voorgaande is gebleken dat met name grotere bedrijven melden dat ze ICT-veiligheidsincidenten meemaakten in de vorm van dataonthullingen, zowel door eigen toedoen (bijvoorbeeld door het verliezen van een USB-stick) als door cybercrime. In Nederland zijn bedrijven verplicht melding te doen van onthulling van persoonsgegevens bij de Autoriteit Persoonsgegevens (AP).

De meldplicht van datalekken geldt in Nederland sinds 2016 en is in EU-verband verder geformaliseerd en gepreciseerd door de Algemene Verordening Gegevensbescherming (AVG) die sinds 25 mei 2018 van toepassing is. Van een datalek is sprake als privacygevoelige gegevens mogelijk in handen van derden zijn gevallen of waar derden toegang tot hebben gehad. Ook hierbij geldt dat de oorzaak van dit soort datalekken soms onbedoeld en terug te voeren is op slordige omgang door de houder van de gegevens. Echter, aan de andere kant van het spectrum staat het moedwillig hacken van dit soort gegevens om te illustreren hoe slecht deze gegevens beveiligd zijn, of om er daadwerkelijk iets mee te gaan doen, bijvoorbeeld te verkopen.

Ruim 20 duizend meldingen van datalekken in 2022

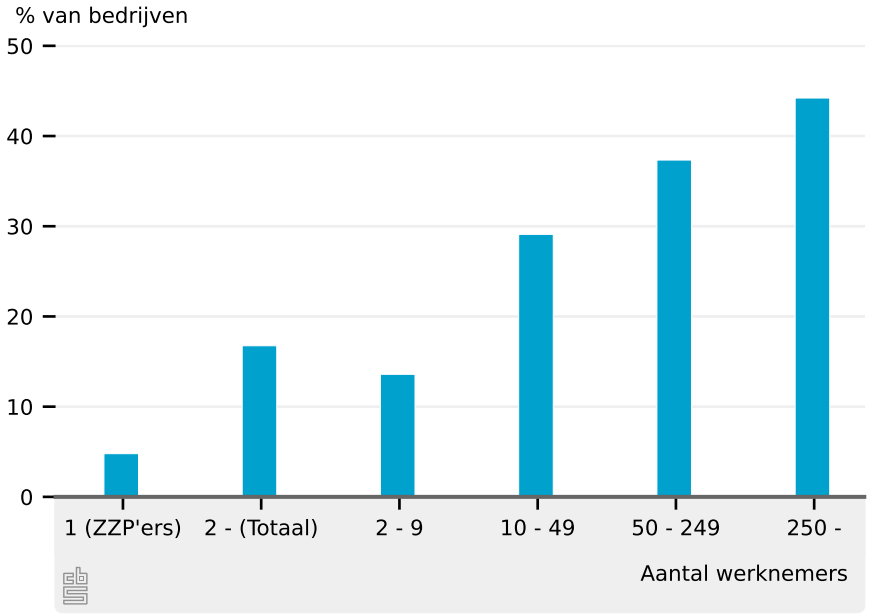
In 2022 zijn 21 151 datalekken gemeld bij de Autoriteit Persoonsgegevens. Dat betekent een afname van 14,9 procent ten opzichte van het jaar ervoor en een afname van 21,5 procent ten opzichte van 2019 waarin het aantal meldingen piekte op 26 956 datalekken.

De gezondheids- en welzijnssector (waaronder ziekenhuizen, apotheken en GGZ-instellingen) had het hoogste aandeel in het aantal meldingen van datalekken in 2022, namelijk 41 procent. In absolute aantallen is het aantal meldingen daar wel afgenomen van ongeveer 9 200 naar 8 670. Ook bij het openbaar bestuur (zoals Rijksoverheid en gemeenten) en in de financiële sector kwamen relatief veel meldingen van datalekken voor (respectievelijk 23 en 9 procent). Bij de financiële sector is het aantal datalekmeldingen sinds 2019 wel fors afgenomen. Gezamenlijk waren deze drie sectoren dus goed voor 73 procent van alle gemelde datalekken in 2021 (figuur 3.1.15).

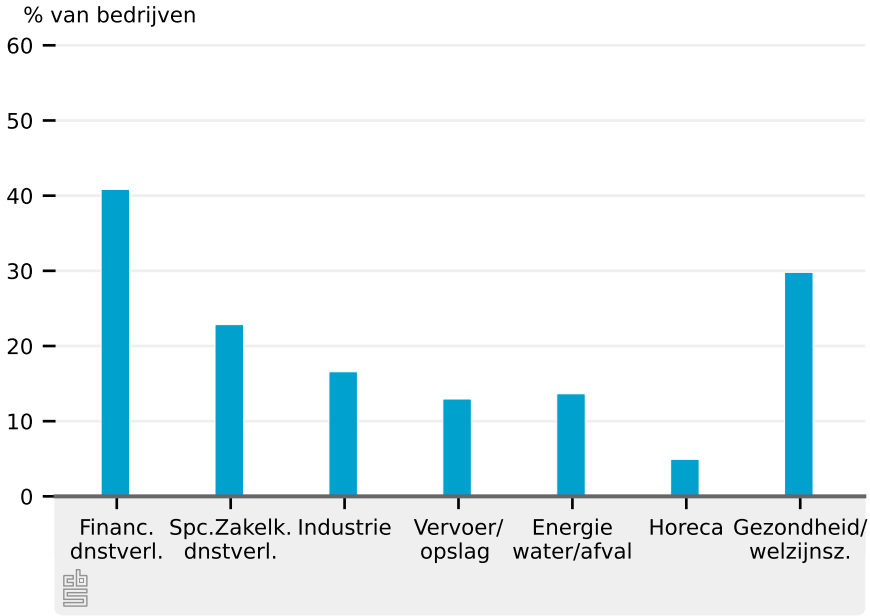
In eerdere jaren vormden deze drie bedrijfstakken ook al de top-3 van sectoren met de meeste gerapporteerde datalekken. In bijna alle eerdere jaren kwamen de meeste meldingen

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

(a) Grootteklasse

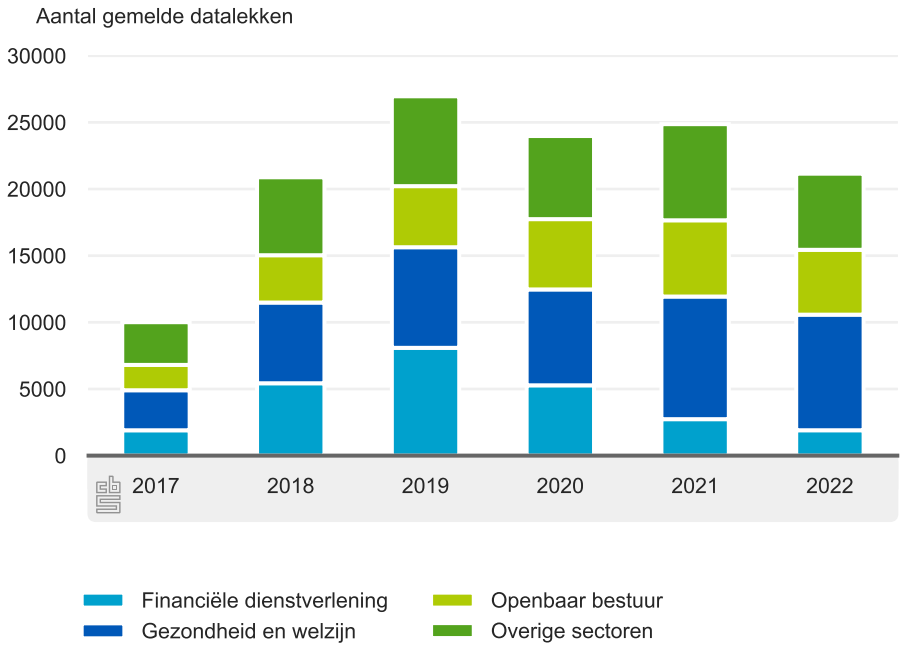


(b) Bedrijfstak



Bron: CBS (2022a)

3.1.15 Top-3 bedrijfstakken met meldingen van datalekken bij de Autoriteit Persoonsgegevens naar bedrijfstak en organisatie



Bron: Autoriteit Persoonsgegevens (2023)

uit de gezondheids- en welzijnssector. Alleen in 2019 was het aantal gerapporteerde datalekken nog hoger binnen de financiële sector.

In de genoemde sectoren worden veel en 'gevoelige' persoonsgegevens verwerkt en opgeslagen. Ook het aantal bedrijven en instellingen en organisaties in een sector speelt een rol bij de hoeveelheid meldingen.

Datalek vaak door persoonsgegevens bij verkeerde ontvanger

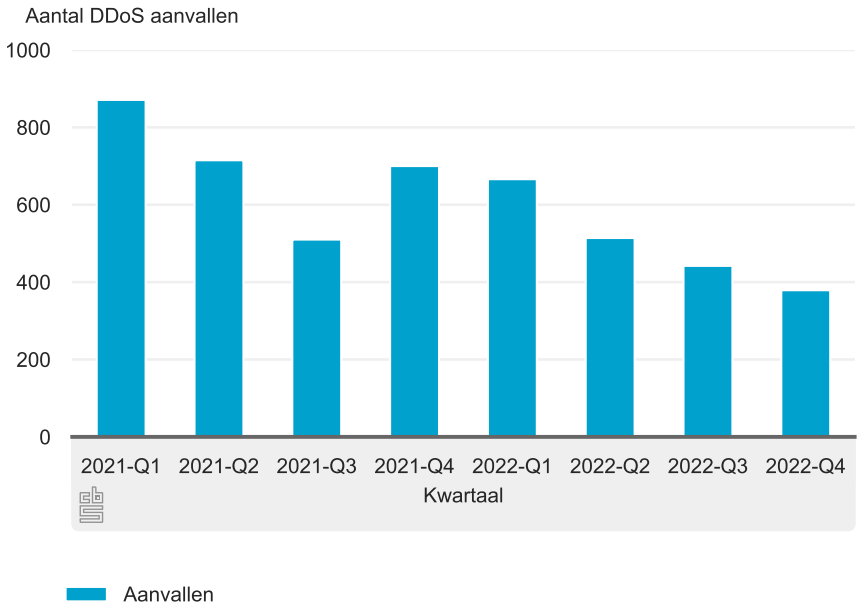
In 2022 was verreweg de meest gemelde oorzaak van het ontstaan van een datalek een brief, postpakket of email met persoonsgegevens die verstuurd of afgegeven werd aan de verkeerde ontvanger(s) (10 192 meldingen per post en 3 347 meldingen per e-mail) Daarna was de meest voorkomende oorzaak is 'Hacking, malware en/of phishing' (cyberaanvallen) en omvatte 11 procent van het aantal meldingen in 2022 (1 825 meldingen). In 2021 was deze categorie incidenten goed voor 9 procent (2210 meldingen) van het totaal aantal meldingen. Overige oorzaken waren persoonsgegevens die toegevoegd werden aan een verkeerd dossier, verloren of gestolen gegevensdragers (zoals usb-sticks) en persoonsgegevens die in het klantportaal aan de verkeerde klant getoond werden.

DDoS-aanvallen

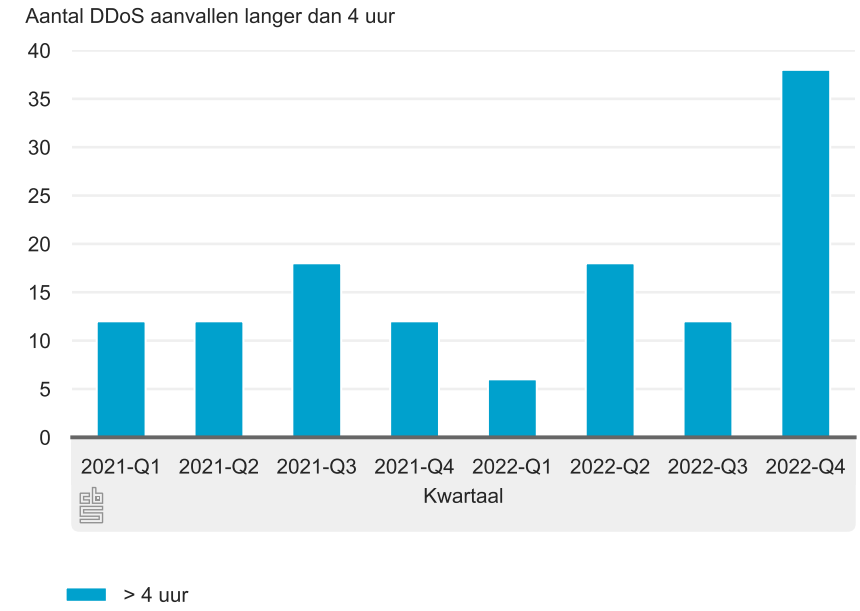
Bij de Nationale anti-DDoS-Wasstraat (NaWas) werden 2 001 DDoS-aanvallen (Distributed Denial of Service aanvallen) geteld in 2022 tegenover 2 796 in het jaar daarvoor (NBIP (2023)). Het gaat hier om aanvallen waarbij een aanvallende partij een server tijdelijk of langdurig onbeschikbaar probeert te maken door deze vanaf meerdere kanten te overspoelen met aanvragen. Bij de NaWas zijn rond de 100 deelnemers aangesloten, waaronder voornamelijk internetproviders. Figuur 3.1.16(a) geeft het aantal DDoS-aanvallen zoals per kwartaal door

3.1.16 Aantal DDoS-aanvallen per kwartaal, 2021-2022[1)]

(a) Aantal aanvallen



(b) Aantal aanvallen langer dan 4 uur



Bron: NBIP (2023)
[1)] Van de bij NaWas aangesloten organisaties.

de NaWas gemeten is; figuur 3.1.16(b) geeft het aantal intensieve DDoS-aanvallen met een duur van langer dan 4 uur. Het aantal DDoS-aanvallen is gedurende het jaar afgenomen, terwijl er tegelijkertijd een toename in de duur en intensiviteit heeft plaatsgevonden. In het eerste kwartaal vonden er nog 666 aanvallen plaatsvonden, in het 4e kwartaal waren dit er 379. Tegelijkertijd neemt de duur (tijd) en de omvang van de aanvallen toe. In het eerste kwartaal waren er 6 aanvallen die langer duurden dan 4 uur, maar er in het laatste kwartaal waren dit er 38. In totaal waren er in 2022 74 aanvallen die langer duurden dan 4 uur, terwijl dit er in 2021 54 waren. Dit is een toename van bijna 50 procent. De meest krachtige aanval gemeten vond plaats in het vierde kwartaal en had een capaciteit van 381 Gbps. In 2021 was de krachtigste aanval 308 Gbps.

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.

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 toegenomen

Het slachtofferschap van online criminaliteit is sinds 2012 met 22 procent toegenomen (figuur 4.1.1). Vooral de laatste jaren is er sprake van een stijgende tendens. Van de onderscheiden vormen van online criminaliteit nam het slachtofferschap van aankoopfraude vanaf 2012 het sterkst toe (index 2021 = 219), gevolgd door verkoopfraude (index 2021 = 165) en online pesten (index 2021 = 126). Het percentage slachtoffers van hacken is vrij stabiel over de tijd. Met identiteitsfraude kwamen juist minder mensen in aanraking, zij het dat er de laatste jaren sprake is van een licht stijgende tendens.

In 2021 was 17 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 2021 was 20 procent van de 15- tot 25-jarigen slachtoffer van online criminaliteit, van de 65-plussers 12 procent. Van alle slachtoffers van online criminaliteit deed 19 procent aangifte bij de politie.

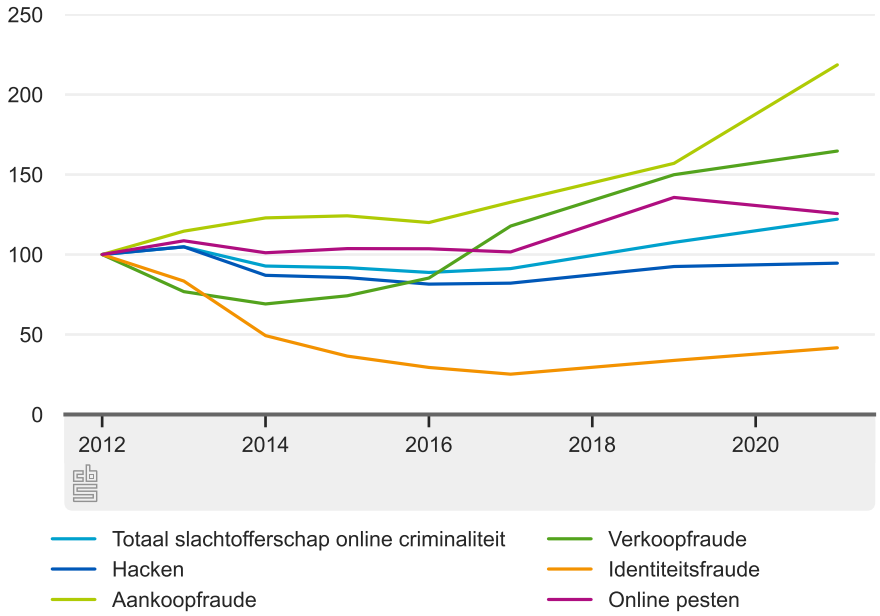
Meer cijfers over online criminaliteit zijn te vinden in de Veiligheidsmonitor 2021 (CBS, 2022h) van het CBS. Daarnaast zijn cijfers over dit onderwerp beschikbaar via StatLine (CBS, 2022g) en in de maatwerktabel behorende bij de Veiligheidsmonitor 2021 (CBS, 2022i).

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.

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

4.1.1 Online criminaliteit -geïndexeerde trends ten opzichte van 2012 (=100)[1,2)]



1) De cijfers zijn gebaseerd op de Veiligheidsmonitor oude stijl

2) In 2018 en 2020 heeft geen meting plaatsgevonden

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). Vaak 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.

1 op de 5 computervredebreukzaken afgehandeld met sanctie zonder tussenkomst rechter

Het totaal aantal keren dat het OM een beslissing nam bij computervredebreukzaken nam toe van 437 in 2010–2015 tot 646 in 2016–2021. Dat betekent een toename van bijna 50 procent. In de periode 2016–2021 werden 118 van de in totaal 646 (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 2010–2015, toen nog 37 procent 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 2016–2021 werden 140 zaken doorgestuurd naar de rechter. Dat is een toename van 21 procent in vergelijking met de periode 2010–2015.

4.2.1 Aantal computervredebreuk zaken afgehandeld door de rechter of het OM

	2010–2015	2016–2021 [1)]
Totaal door OM genomen beslissingen	437	646
– strafoplegging OM[2)]	160	118
– door OM doorgestuurd naar de rechter (dagvaarding en oproep na verzet)	116	140
Straf opgelegd door rechter	77	84

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).

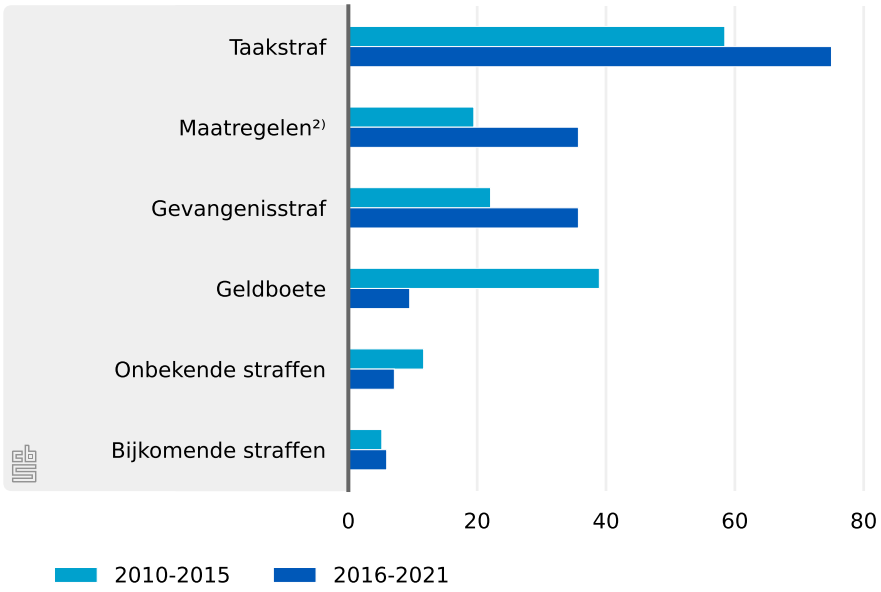
[2)] Door het OM afgedaan met transactie, strafbeschikking of voorwaardelijk beleidssepot.

In de periode 2016–2021 werden 107 computervredebreukzaken afgedaan door de rechter. Ongeveer evenveel als in de periode 2010–2015. Bij 84 (bijna 80 procent) van de computervredebreukzaken die door de rechter zijn afgedaan in 2016–2021 deelde de rechter een straf uit tegenover 68 procent van de zaken in de periode 2010–2015. De meeste overige door de rechter afgedane zaken leiden tot vrijspraak dan wel een schuldigverklaring zonder straf.

Rechter geeft vaak taakstraf

Voor de zaken die bij de rechter tot een straf leiden betreft dit relatief vaak een taakstraf. In driekwart van de zaken waarbij door de rechter een straf werd opgelegd in 2016–2021 betrof dit een taakstraf. Dat is meer dan in 2010–2015 toen nog 58 procent werd afgedaan met een taakstraf. Het aandeel door de rechter opgelegde boetes is gedaald van 39 procent in 2010–2015 naar 10 procent in 2016–2021. Het aandeel opgelegde gevangenisstraffen is daarentegen toegenomen. Bij meer dan 1 op de drie schuldigverklaringen in de periode 2016–2021 waarbij door de rechter een straf werd opgelegd betrof dit een gevangenisstraf.

4.2.2 Door rechter opgelegde straffen en maatregelen voor computervredebreuk als percentage van het totaal aantal schuldigverklaringen door de rechter met strafoplegging bij computervredebreuk[1)]



Bron: CBS

[1)] Een strafzaak kan meerdere straffen toegekend krijgen (bijvoorbeeld taakstraf en geldboete), dus het totaal overstijgt de 100 procent.

[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
Totaal	2 of meer werkzame personen
1	1 werkzame persoon (ZZP'er)
2–9	2 tot 10 werkzame personen
10–49	10 tot 50 werkzame personen
50–249	50 tot 250 werkzame personen
2–249	2 tot 250 werkzame personen
250–499	250 tot 500 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 Maatregelen

A.2.1 1) Gebruikte ICT-maatregelen voor alle grootteklassen als percentage van het aantal bedrijven, 2016 -2021

Maatregel	Bedrijfsgrootte	2016	2017	2018	2019	2020	2021
antivirussoftware	Totaal	87	85	89	89	87	85
	1 werkzame persoon (ZZP'ers)	.	.	.	.	82	64
	2 tot 10 werkzame personen	86	83	87	87	85	83
	10 tot 50 werkzame personen	93	94	96	92	95	96
	50 tot 250 werkzame personen	97	98	98	97	98	98
	250 of meer werkzame personen	98	98	99	98	99	99
	2 tot 250 werkzame personen	87	85	89	89	87	85
Authenticatie via soft- of hardwaretoken	Totaal	26	30	39	46	45	46
	1 werkzame persoon (ZZP'ers)	.	.	.	.	38	34
	2 tot 10 werkzame personen	24	27	35	42	41	41
	10 tot 50 werkzame personen	29	38	49	54	60	62
	50 tot 250 werkzame personen	48	54	62	68	75	81
	250 of meer werkzame personen	71	76	81	87	89	93
	2 tot 250 werkzame personen	25	30	39	45	45	45
Beleid voor sterke wachtwoorden	Totaal	57	61	65	68	66	68
	1 werkzame persoon (ZZP'ers)	.	.	.	.	66	53
	2 tot 10 werkzame personen	55	58	63	65	62	65
	10 tot 50 werkzame personen	64	70	74	74	77	80
	50 tot 250 werkzame personen	81	84	86	88	90	91
	250 of meer werkzame personen	93	94	94	96	96	98
	2 tot 250 werkzame personen	57	61	65	68	65	68
Encryptie van data	Totaal	25	29	37	38	37	36
	1 werkzame persoon (ZZP'ers)	.	.	.	.	31	25
	2 tot 10 werkzame personen	23	27	33	35	34	33
	10 tot 50 werkzame personen	29	34	44	44	47	45
	50 tot 250 werkzame personen	46	51	62	64	66	67
	250 of meer werkzame personen	69	74	81	83	85	87
	2 tot 250 werkzame personen	25	29	36	38	37	35
Gegevens op andere fysieke locatie	Totaal	71	67	72	71	66	74
	1 werkzame persoon (ZZP'ers)	.	.	.	.	58	54
	2 tot 10 werkzame personen	68	63	68	68	62	70
	10 tot 50 werkzame personen	80	81	85	82	82	88
	50 tot 250 werkzame personen	90	90	93	91	92	95
	250 of meer werkzame personen	94	93	97	95	96	98
	2 tot 250 werkzame personen	70	66	72	71	66	73
ICT-cursus aan ICT-specialisten	Totaal	3	5	.	6	5	7
	1 werkzame persoon (ZZP'ers)	.	.	.	.	0	0
	2 tot 10 werkzame personen	0	3	.	3	3	4
	10 tot 50 werkzame personen	9	10	.	9	10	14
	50 tot 250 werkzame personen	33	34	.	34	35	41
	250 of meer werkzame personen	68	66	.	68	67	74
	2 tot 250 werkzame personen	3	5	.	5	5	6
Logbestanden voor analyse incidenten	Totaal	31	33	39	37	36	38
	1 werkzame persoon (ZZP'ers)	.	.	.	.	19	17
	2 tot 10 werkzame personen	25	26	32	31	30	32
	10 tot 50 werkzame personen	49	54	59	55	57	60
	50 tot 250 werkzame personen	75	78	82	79	82	83
	250 of meer werkzame personen	88	88	91	91	91	93
	2 tot 250 werkzame personen	30	33	38	37	36	38

Vervolg op volgende pagina…

A.2.1 2) Gebruikte ICT-maatregelen voor alle grootteklassen als percentage van het aantal bedrijven, 2016 - 2021

…vervolg van vorige pagina

Maatregel	Bedrijfsgrootte	2016	2017	2018	2019	2020	2021
Methodes voor beoordelen ICT-veiligheid	Totaal	22	25	31	28	28	29
	1 werkzame persoon (ZZP'ers)	.	.	.	.	13	10
	2 tot 10 werkzame personen	17	20	26	22	23	24
	10 tot 50 werkzame personen	34	40	48	41	45	46
	50 tot 250 werkzame personen	55	60	67	63	68	70
	250 of meer werkzame personen	72	75	80	81	82	86
	2 tot 250 werkzame personen	21	24	31	27	27	29
Network access control	Totaal	31	33	37	37	34	46
	1 werkzame persoon (ZZP'ers)	.	.	.	.	23	20
	2 tot 10 werkzame personen	28	29	32	32	29	40
	10 tot 50 werkzame personen	42	46	50	48	50	71
	50 tot 250 werkzame personen	60	60	63	64	66	88
	250 of meer werkzame personen	67	68	71	72	73	91
	2 tot 250 werkzame personen	31	33	36	36	34	46
Risicoanalyses	Totaal	22	25	31	29	28	29
	1 werkzame persoon (ZZP'ers)	.	.	.	.	15	12
	2 tot 10 werkzame personen	17	20	26	24	23	24
	10 tot 50 werkzame personen	34	40	47	42	45	47
	50 tot 250 werkzame personen	58	62	64	63	67	70
	250 of meer werkzame personen	75	76	80	80	79	83
	2 tot 250 werkzame personen	21	24	31	28	28	29
Updaten software/besturingssysteem	Totaal	.	.	81	84	83	.
	1 werkzame persoon (ZZP'ers)	.	.	.	.	79	.
	2 tot 10 werkzame personen	.	.	78	81	80	.
	10 tot 50 werkzame personen	.	.	92	90	93	.
	50 tot 250 werkzame personen	.	.	97	96	97	.
	250 of meer werkzame personen	.	.	98	98	99	.
	2 tot 250 werkzame personen	.	.	81	83	82	.
VPN internetgebruik buiten het bedrijf	Totaal	29	32	35	35	32	33
	1 werkzame persoon (ZZP'ers)	.	.	.	.	23	19
	2 tot 10 werkzame personen	23	25	29	29	26	28
	10 tot 50 werkzame personen	47	50	54	52	55	55
	50 tot 250 werkzame personen	74	75	77	78	79	77
	250 of meer werkzame personen	85	86	86	86	86	84
	2 tot 250 werkzame personen	28	31	35	35	32	33

A.2.2 1) Gebruikte ICT-maatregelen voor alle bedrijfstakken als percentage van het aantal bedrijven met 2 of meer werknemers, 2016-2021

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

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, 2016-2021

…vervolg van vorige pagina

Maatregel	Bedrijfstak	2016	2017	2018	2019	2020	2021
Encryptie van data	Totaal	25	29	37	38	37	36
	Industrie	22	24	32	35	33	31
	Energie	29	27	37	38	44	33
	Bouwnijverheid	15	20	27	23	26	22
	Handel	20	23	32	33	32	32
	Vervoer	17	20	26	30	26	29
	Horeca	11	12	18	22	18	15
	Informatie en communicatie	58	59	66	65	65	64
	Financiële dienstverlening	38	43	56	56	65	59
	Verhuur en handel onroerend goed	26	16	26	37	37	36
	Specialistische zakelijke diensten	31	36	44	46	44	44
	Verhuur en overige zakelijke diensten	22	29	34	39	37	34
	Gezondheidszorg	51	60	67	67	70	66
	ICT-sector	60	62	67	67	66	70
Gegevens op andere fysieke locatie	Totaal	71	67	72	71	66	74
	Industrie	77	74	78	77	73	80
	Energie	78	72	74	70	63	75
	Bouwnijverheid	64	62	66	66	65	66
	Handel	67	62	71	72	63	72
	Vervoer	61	62	63	65	63	67
	Horeca	52	42	46	43	36	47
	Informatie en communicatie	87	82	89	84	82	90
	Financiële dienstverlening	75	83	85	76	87	84
	Verhuur en handel onroerend goed	69	63	69	64	65	70
	Specialistische zakelijke diensten	83	80	85	80	78	88
	Verhuur en overige zakelijke diensten	70	65	69	70	66	71
	Gezondheidszorg	84	82	87	86	83	86
	ICT-sector	89	84	92	84	81	92
ICT-cursus aan ICT-specialisten	Totaal	3	5	.	6	5	7
	Industrie	5	6	.	7	6	8
	Energie	10	10	.	11	12	13
	Bouwnijverheid	1	2	.	2	2	3
	Handel	2	4	.	5	4	5
	Vervoer	4	3	.	3	3	5
	Horeca	0	1	.	1	0	1
	Informatie en communicatie	13	35	.	38	31	35
	Financiële dienstverlening	9	15	.	13	13	19
	Verhuur en handel onroerend goed	3	3	.	3	2	5
	Specialistische zakelijke diensten	3	6	.	6	6	8
	Verhuur en overige zakelijke diensten	2	5	.	4	3	5
	Gezondheidszorg	3	3	.	4	4	5
	ICT-sector	14	37	.	42	36	43

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, 2016-2021

…vervolg van vorige pagina

Maatregel	Bedrijfstak	2016	2017	2018	2019	2020	2021
Logbestanden voor analyse incidenten	Totaal	31	33	39	37	36	38
	Industrie	36	39	45	42	40	43
	Energie	48	42	54	51	41	48
	Bouwnijverheid	20	22	30	29	26	27
	Handel	29	31	37	35	34	36
	Vervoer	25	29	35	31	33	31
	Horeca	13	15	16	15	15	15
	Informatie en communicatie	60	58	67	63	63	62
	Financiële dienstverlening	50	56	61	59	66	66
	Verhuur en handel onroerend goed	31	25	28	33	31	43
	Specialistische zakelijke diensten	39	41	48	44	44	47
	Verhuur en overige zakelijke diensten	29	33	36	34	34	33
	Gezondheidszorg	39	43	49	51	51	56
	ICT-sector	64	63	72	65	66	70
Methodes voor beoordelen ICT-veiligheid	Totaal	22	25	31	28	28	29
	Industrie	26	30	35	32	33	36
	Energie	35	35	46	35	35	41
	Bouwnijverheid	16	20	30	22	21	22
	Handel	19	22	30	27	27	28
	Vervoer	18	19	27	23	27	26
	Horeca	8	11	13	12	10	14
	Informatie en communicatie	35	43	46	43	39	41
	Financiële dienstverlening	41	48	61	55	61	55
	Verhuur en handel onroerend goed	25	23	31	28	32	30
	Specialistische zakelijke diensten	28	29	37	30	34	34
	Verhuur en overige zakelijke diensten	21	26	30	27	27	28
	Gezondheidszorg	29	34	39	38	37	38
	ICT-sector	37	43	47	44	43	47
Network access control	Totaal	31	33	37	37	34	46
	Industrie	34	38	40	40	37	51
	Energie	37	38	42	51	41	60
	Bouwnijverheid	20	27	34	31	23	37
	Handel	29	32	36	37	33	43
	Vervoer	23	30	30	30	31	36
	Horeca	17	14	19	20	20	21
	Informatie en communicatie	51	50	53	51	47	64
	Financiële dienstverlening	48	53	59	55	61	74
	Verhuur en handel onroerend goed	36	26	28	33	34	47
	Specialistische zakelijke diensten	38	37	42	41	38	61
	Verhuur en overige zakelijke diensten	28	33	35	34	34	44
	Gezondheidszorg	46	47	47	48	48	64
	ICT-sector	54	54	55	53	49	69

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, 2016-2021

…vervolg van vorige pagina

Maatregel	Bedrijfstak	2016	2017	2018	2019	2020	2021
Risicoanalyses	Totaal	22	25	31	29	28	29
	Industrie	24	30	33	31	32	33
	Energie	33	34	34	37	33	40
	Bouwnijverheid	16	20	25	21	17	19
	Handel	20	20	27	26	26	27
	Vervoer	19	22	28	24	27	28
	Horeca	10	12	15	13	12	14
	Informatie en communicatie	39	47	50	48	47	45
	Financiële dienstverlening	39	49	58	51	57	57
	Verhuur en handel onroerend goed	22	22	25	24	27	31
	Specialistische zakelijke diensten	25	30	37	31	33	34
	Verhuur en overige zakelijke diensten	19	25	30	28	29	27
	Gezondheidszorg	31	37	48	46	41	44
	ICT-sector	42	47	53	50	50	51
Updaten software/besturingssysteem	Totaal	.	.	81	84	83	.
	Industrie	.	.	86	86	84	.
	Energie	.	.	84	85	79	.
	Bouwnijverheid	.	.	74	81	78	.
	Handel	.	.	82	83	82	.
	Vervoer	.	.	75	81	76	.
	Horeca	.	.	56	65	68	.
	Informatie en communicatie	.	.	94	94	94	.
	Financiële dienstverlening	.	.	96	93	97	.
	Verhuur en handel onroerend goed	.	.	78	75	73	.
	Specialistische zakelijke diensten	.	.	90	91	89	.
	Verhuur en overige zakelijke diensten	.	.	83	82	80	.
	Gezondheidszorg	.	.	92	95	95	.
	ICT-sector	.	.	96	94	95	.
VPN internetgebruik buiten het bedrijf	Totaal	29	32	35	35	32	33
	Industrie	36	39	42	42	42	41
	Energie	42	45	51	50	43	40
	Bouwnijverheid	20	21	29	26	23	26
	Handel	26	28	34	34	30	31
	Vervoer	23	26	27	26	27	28
	Horeca	13	13	14	12	13	13
	Informatie en communicatie	54	56	58	55	52	54
	Financiële dienstverlening	51	57	53	55	52	55
	Verhuur en handel onroerend goed	34	28	31	31	34	35
	Specialistische zakelijke diensten	36	38	42	44	39	42
	Verhuur en overige zakelijke diensten	25	32	32	31	29	31
	Gezondheidszorg	37	44	49	48	45	47
	ICT-sector	59	61	62	59	58	61

A.3 Incidenten

A.3.1 Incidenten met interne ookzaak en kosten per grootteklasse als percentage van het aantal bedrijven, 2016-2021[1]

		2016		2017		2019		2020		2021	
		Inciden ge-had	ook met kos-ten	Incident ge-had	ook met kos-ten	Incident ge-had	ook met kos-ten	Incider ge-had	ook met kos-ten	Incident ge-had	ook met kos-ten
Interne incidenten	*Aantal werkzame personen*										
Uitval ICT-dienst door ICT-veiligheidsincident	Totaal	26	10	25	10	27	10	13	4	11	3
	1 werkzame persoon (ZZP'ers)	.	.	.	.	.	.	7	1	4	1
	2 tot 10 werkzame personen	21	8	21	8	24	8	10	3	9	2
	10 tot 50 werkzame personen	41	18	40	15	38	15	23	7	22	6
	50 tot 250 werkzame personen	52	25	49	22	50	21	35	10	32	9
	250 of meer werkzame personen	54	28	50	26	56	27	41	13	42	15
	2 tot 250 werkzame personen	25	10	25	9	27	9	13	4	11	3
Vernietiging data door ICT-veiligheidsincident	Totaal	5	3	5	3	3	1	2	1	2	0
	1 werkzame persoon (ZZP'ers)	.	.	.	.	.	.	2	1	1	0
	2 tot 10 werkzame personen	5	2	5	3	3	1	3	1	1	0
	10 tot 50 werkzame personen	7	3	7	3	5	2	3	1	3	1
	50 tot 250 werkzame personen	10	5	8	3	6	2	5	2	4	2
	250 of meer werkzame personen	13	7	10	5	8	4	7	3	6	2
	2 tot 250 werkzame personen	5	2	5	3	3	1	2	1	2	0
Onthulling door intern incident	Totaal	2	1	3	2	2	1	1	0	1	0
	1 werkzame persoon (ZZP'ers)	.	.	.	.	.	.	0	0	0	0
	2 tot 10 werkzame personen	2	1	3	2	2	1	1	0	1	0
	10 tot 50 werkzame personen	3	1	4	1	4	1	2	0	2	0
	50 tot 250 werkzame personen	6	2	7	1	8	1	6	1	5	1
	250 of meer werkzame personen	16	4	19	4	25	6	17	3	18	3
	2 tot 250 werkzame personen	2	1	3	2	2	1	1	0	1	0

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

A.3.2 Incidenten door aanval van buitenaf en kosten per grootteklasse als percentage van het aantal bedrijven, 2016-2021[1]

		2016		2017		2019		2020		2021	
		Incident ge-had	ook met kos-ten	Incident ge-had	ook met kos-ten	Incident ge-had	ook met kos-ten	Incident ge-had	ook met kos-ten	Incident ge-had	ook met kos-ten
Incidenten door aanval	*Aantal werkzame personen*										
Uitval ICT-dienst door aanval van buitenaf	Totaal	8	4	7	4	5	2	5	2	4	1
	1 werkzame persoon (ZZP'ers)	.	.	.	.	.	.	3	0	2	0
	2 tot 10 werkzame personen	6	3	6	3	4	2	4	1	3	1
	10 tot 50 werkzame personen	12	6	11	6	7	4	8	3	6	2
	50 tot 250 werkzame personen	17	9	12	5	8	3	11	4	8	3
	250 of meer werkzame personen	22	12	16	8	11	6	14	5	12	5
	2 tot 250 werkzame personen	7	4	7	4	5	2	5	2	4	1
Vernietiging data aanval van buitenaf	Totaal	6	3	4	3	2	1	2	1	1	1
	1 werkzame persoon (ZZP'ers)	.	.	.	.	.	.	1	0	1	0
	2 tot 10 werkzame personen	4	2	4	2	2	1	2	1	1	0
	10 tot 50 werkzame personen	11	6	6	4	3	2	3	1	2	1
	50 tot 250 werkzame personen	18	8	10	4	3	2	4	2	3	1
	250 of meer werkzame personen	24	9	13	6	6	3	4	2	4	2
	2 tot 250 werkzame personen	6	3	4	2	2	1	2	1	1	1
Onthulling gegevens door ICT-inbraak	Totaal	2	1	3	2	2	0	2	1	2	0
	1 werkzame persoon (ZZP'ers)	.	.	.	.	.	.	2	0	1	0
	2 tot 10 werkzame personen	1	1	3	2	1	0	1	0	1	0
	10 tot 50 werkzame personen	2	1	3	1	2	1	2	1	3	1
	50 tot 250 werkzame personen	2	1	3	1	4	1	4	1	4	1
	250 of meer werkzame personen	5	2	7	2	8	3	9	3	9	2
	2 tot 250 werkzame personen	2	1	3	2	2	0	1	1	2	0

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

A.3.3 Incidenten met interne oorzaak per bedrijfstak als percentage van het aantal bedrijven, 2016-2021[1]

		2016		2017		2019		2020		2021	
		Incident gehad	ook met kosten	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-dienst door ICT-veiligheidsincident	Totaal	26	10	25	10	27	10	13	4	11	3
	Industrie	30	14	27	11	32	12	15	5	14	4
	Energie	29	12	30	13	31	13	16	4	14	3
	Bouwnijverheid	22	9	19	8	21	11	10	4	8	2
	Handel	26	11	25	9	28	9	10	3	10	3
	Vervoer	21	9	19	8	23	9	14	6	10	3
	Horeca	13	5	18	9	20	4	12	3	5	2
	Informatie en communicatie	28	10	30	10	32	8	18	5	16	3
	Financiële dienstverlening	29	11	30	9	34	15	22	8	21	6
	Verhuur en handel onroerend goed	29	11	23	8	22	10	8	3	8	1
	Specialistische zakelijke diensten	29	12	31	12	30	11	16	5	14	4
	Verhuur en overige zakelijke diensten	22	8	24	8	23	7	10	2	10	2
	Gezondheidszorg	33	12	29	9	36	13	22	6	20	3
	ICT-sector	28	10	31	9	33	9	18	4	17	4
Vernietiging data door ICT-veiligheidsincident	Totaal	5	3	5	3	3	1	2	1	2	0
	Industrie	6	3	5	3	5	2	2	1	1	1
	Energie	7	4	7	3	7	2	2	0	2	0
	Bouwnijverheid	5	2	5	3	4	1	1	1	1	0
	Handel	6	3	5	3	3	1	2	1	1	0
	Vervoer	4	2	5	2	3	2	3	2	2	0
	Horeca	5	2	7	4	2	1	3	1	1	0
	Informatie en communicatie	6	2	5	2	3	1	2	0	3	1
	Financiële dienstverlening	4	2	4	1	4	2	4	1	2	2
	Verhuur en handel onroerend goed	8	3	3	2	3	1	2	1	1	0
	Specialistische zakelijke diensten	5	3	6	3	4	2	3	1	2	1
	Verhuur en overige zakelijke diensten	4	2	6	2	4	1	1	0	1	0
	Gezondheidszorg	3	1	3	1	2	1	2	1	2	0
	ICT-sector	6	2	4	2	3	1	3	0	3	1
Onthulling door intern incident	Totaal	2	1	3	2	2	1	1	0	1	0
	Industrie	2	1	3	1	3	1	1	0	1	0
	Energie	5	3	3	1	3	1	3	1	3	0
	Bouwnijverheid	2	1	2	1	1	0	0	0	0	0
	Handel	2	1	3	2	2	1	1	0	1	0
	Vervoer	1	1	3	2	2	1	1	0	2	0
	Horeca	1	0	4	3	0	0	1	0	0	0
	Informatie en communicatie	3	1	3	2	4	1	1	0	1	0
	Financiële dienstverlening	3	1	3	1	5	1	3	0	4	2
	Verhuur en handel onroerend goed	2	1	4	2	4	2	1	0	2	1
	Specialistische zakelijke diensten	2	1	3	1	3	1	2	0	2	0
	Verhuur en overige zakelijke diensten	2	1	3	1	2	1	1	0	1	0
	Gezondheidszorg	2	0	6	1	6	1	5	1	4	0
	ICT-sector	3	1	3	1	4	1	1	0	1	0

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

A.3.4 Incidenten door aanval van buitenaf per bedrijfstak als percentage van het aantal bedrijven, 2016-2021[1]

		2016		2017		2019		2020		2021	
		Inciden ge-had	ook met kos-ten	Incident ge-had	ook met kos-ten	Incident ge-had	ook met kos-ten	Incider ge-had	ook met kos-ten	Incident ge-had	ook met kos-ten
Incidenten door aanval	*Bedrijfstak*										
Vernietiging data aanval van buitenaf	Totaal	6	3	4	3	2	1	2	1	1	1
	Industrie	9	5	6	3	4	2	2	1	1	1
	Energie	9	5	9	4	1	0	1	0	2	0
	Bouwnijverheid	8	3	5	4	3	1	2	1	1	0
	Handel	6	3	5	3	2	1	2	1	1	0
	Vervoer	6	3	5	3	2	1	3	2	2	1
	Horeca	4	1	4	2	1	0	2	1	1	0
	Informatie en communicatie	4	2	4	2	2	1	1	0	1	1
	Financiële dienstverlening	8	4	3	2	3	1	0	0	3	1
	Verhuur en handel onroerend goed	6	2	1	0	3	2	2	1	1	0
	Specialistische zakelijke diensten	5	2	5	3	2	0	2	1	2	1
	Verhuur en overige zakelijke diensten	7	4	5	2	2	1	2	1	2	1
	Gezondheidszorg	5	2	3	1	2	1	1	1	0	0
	ICT-sector	5	2	4	2	2	1	2	0	1	1
Uitval ICT-dienst door aanval van buitenaf	Totaal	8	4	7	4	5	2	5	2	4	1
	Industrie	10	6	8	4	7	3	5	2	4	2
	Energie	8	3	7	3	4	1	8	1	2	1
	Bouwnijverheid	9	4	9	3	5	2	3	2	3	1
	Handel	8	4	7	4	5	2	5	2	4	2
	Vervoer	5	3	8	5	5	2	5	2	4	1
	Horeca	3	1	5	3	4	2	4	1	1	0
	Informatie en communicatie	12	4	11	5	8	2	9	3	6	1
	Financiële dienstverlening	7	2	6	3	7	4	10	2	8	2
	Verhuur en handel onroerend goed	6	3	6	1	4	1	6	0	1	0
	Specialistische zakelijke diensten	9	5	7	4	4	2	5	2	5	2
	Verhuur en overige zakelijke diensten	8	4	8	3	4	2	4	1	3	0
	Gezondheidszorg	4	2	6	3	7	3	5	1	4	1
	ICT-sector	12	5	10	4	8	2	9	3	6	1
Onthulling gegevens door ICT-inbraak	Totaal	2	1	3	2	2	0	2	1	2	0
	Industrie	2	1	3	2	2	1	2	0	1	0
	Energie	2	0	3	2	2	1	1	0	1	0
	Bouwnijverheid	2	0	2	1	1	0	1	1	1	0
	Handel	2	1	3	2	2	0	2	1	2	0
	Vervoer	2	1	3	1	2	1	2	0	1	0
	Horeca	1	0	4	3	0	0	1	1	1	0
	Informatie en communicatie	1	1	2	2	2	0	1	0	1	0
	Financiële dienstverlening	2	1	2	1	3	1	1	0	4	2
	Verhuur en handel onroerend goed	1	1	2	0	2	1	1	0	2	1
	Specialistische zakelijke diensten	2	1	3	2	2	0	2	1	2	1
	Verhuur en overige zakelijke diensten	2	1	2	1	3	1	2	0	2	0
	Gezondheidszorg	1	0	1	1	1	0	1	1	1	0
	ICT-sector	1	1	2	1	2	0	1	0	2	0

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

Bibliografie

Autoriteit Persoonsgegevens (2023). Datalekkenrapportage 2022.

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 (2021f). Cybersecuritymonitor 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). CBS StatLine.

CBS (2022g). Statline Veiligheid en recht 2021.

CBS (2022h). Veiligheidsmonitor 2021.

CBS (2022i). Maatwerktabel Veiligheidsmonitor 2021.

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

SIDN (2023). SIDN Labs: .nl stats en data.

Uitgave 2023