Cybersecuritymonitor

2020

Cybersecuritymonitor

2020

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
2020–2021	2020 tot en met 2021
2020/2021	Het gemiddelde over de jaren 2020 tot en met 2021
2020/'21	Oogstjaar, boekjaar, schooljaar enz., beginnend in 2020 en eindigend in 2021
2018/'19–2020/'21	Oogstjaar, boekjaar, enz., 2018/'19 tot en met 2020/'21

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 vierde 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 over de cyberweerbaarheid van bedrijven en huishoudens in Nederland. Dat gebeurt met voornamelijk 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, 2018g, 2019f).

De structuur van de monitor is weer opgezet volgens dezelfde lijnen als de afgelopen drie edities. Cybersecurity werd hierin opgesplitst in twee domeinen: maatregelen en incidenten. Bij cybersecuritymaatregelen denken we aan het hele scala van mogelijkheden om de veiligheid van computers, smartphones, laptops, servers en netwerken te verhogen. Cybersecurityincidenten zijn juist 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 verwijzen we naar de voorgaande Cybersecuritymonitors (CBS, 2017f, 2018g, 2019f).

In dit rapport worden in hoofdstuk 2 de cybersecuritymaatregelen besproken, dat wil zeggen de maatregelen die door bedrijven worden genomen om zichzelf meer cyberweerbaar te maken. In hoofdstuk 3 wordt ingegaan op alle cybersecurityincidenten bij Nederlandse bedrijven en personen. Ten slotte gaan we in hoofdstuk 4 in op de geregistreerde cybercrime, dus de cybersecurityincidenten door kwaadwillenden die ook daadwerkelijk slachtoffers gemaakt hebben.

2. Cybersecurity-maatregelen

2.1 Bedrijven

In dit hoofdstuk gaan we in op de maatregelen die bedrijven in Nederland nemen om zichzelf meer cyberweerbaar te maken. We gebruiken hier vooral de cijfers uit de CBS-enquêtes 'ICT-gebruik bedrijven 2017' (CBS, 2017a,b,c,d,e), 'ICT-gebruik bedrijven 2018' (CBS, 2018a,b,c,d,e), 'ICT-gebruik bedrijven 2019' (CBS, 2019c,e,d,b,a) en 'ICT-gebruik bedrijven 2020' (CBS, 2020e,a,f,d,c).

De jaarlijkse enquête 'ICT-gebruik bedrijven' (of kortweg: de ICT-enquête) wordt in samenwerking met de andere EU-landen uitgevoerd. Een deel van de uitvoeringskosten van de ICT-enquête wordt door Eurostat gefinancierd. Het Ministerie van Economische Zaken en Klimaat financiert daarnaast 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 van verschillende bedrijfsgrootteklassen en bedrijfscategorieën. In de Appendix wordt in tabellen A.2 en A.1 een overzicht van respectievelijk alle grootteklassen en bedrijfstakken gegeven. In dit hoofdstuk worden de cijfers van vier grootteklassen uitgelicht: 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 een viertal bedrijfstakken de cijfers zien: 1) Energie-, water- en afvalbeheer, 2) Horeca, 3) Gezondheidszorg en 4) de ICT-sector. Een compleet overzicht van de cijfers van alle grootteklassen en bedrijfstakken kan op Statline (CBS, 2020b) gevonden worden.

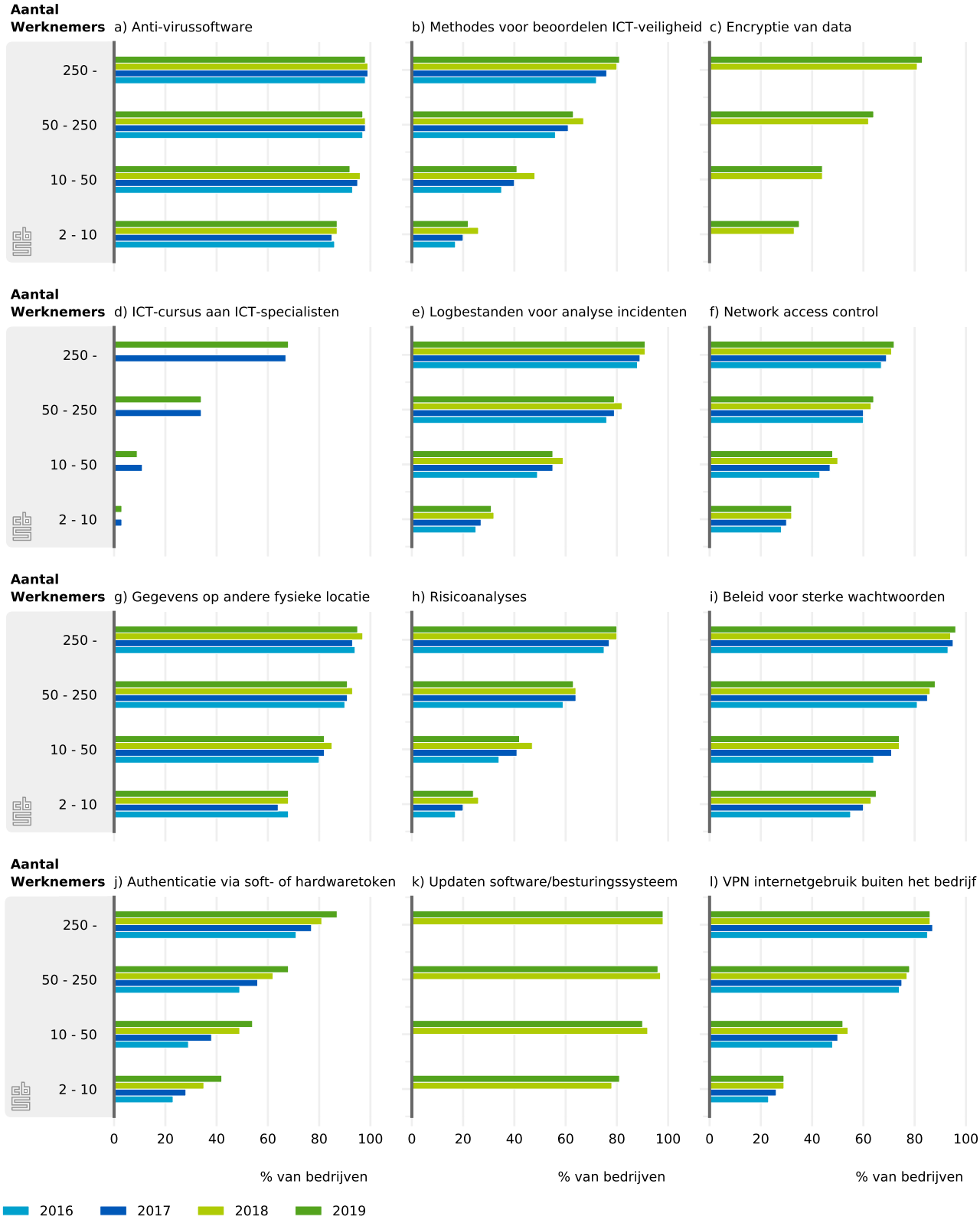
Maatregelen ter verhoging van de cyberweerbaarheid

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 een bedrijf uitvoert: het eigen personeel, een extern bedrijf, of een combinatie van beide.

Eerst bekijken we hoe vaak verschillende cybersecuritymaatregelen door bedrijven toegepast worden. In figuren 2.1.1(a–l) en 2.1.2(a–l) worden over de jaren 2016–2019 [1)] voor verschillende bedrijfsgrootteklasses en bedrijfstakken voor twaalf verschillende maatregelen

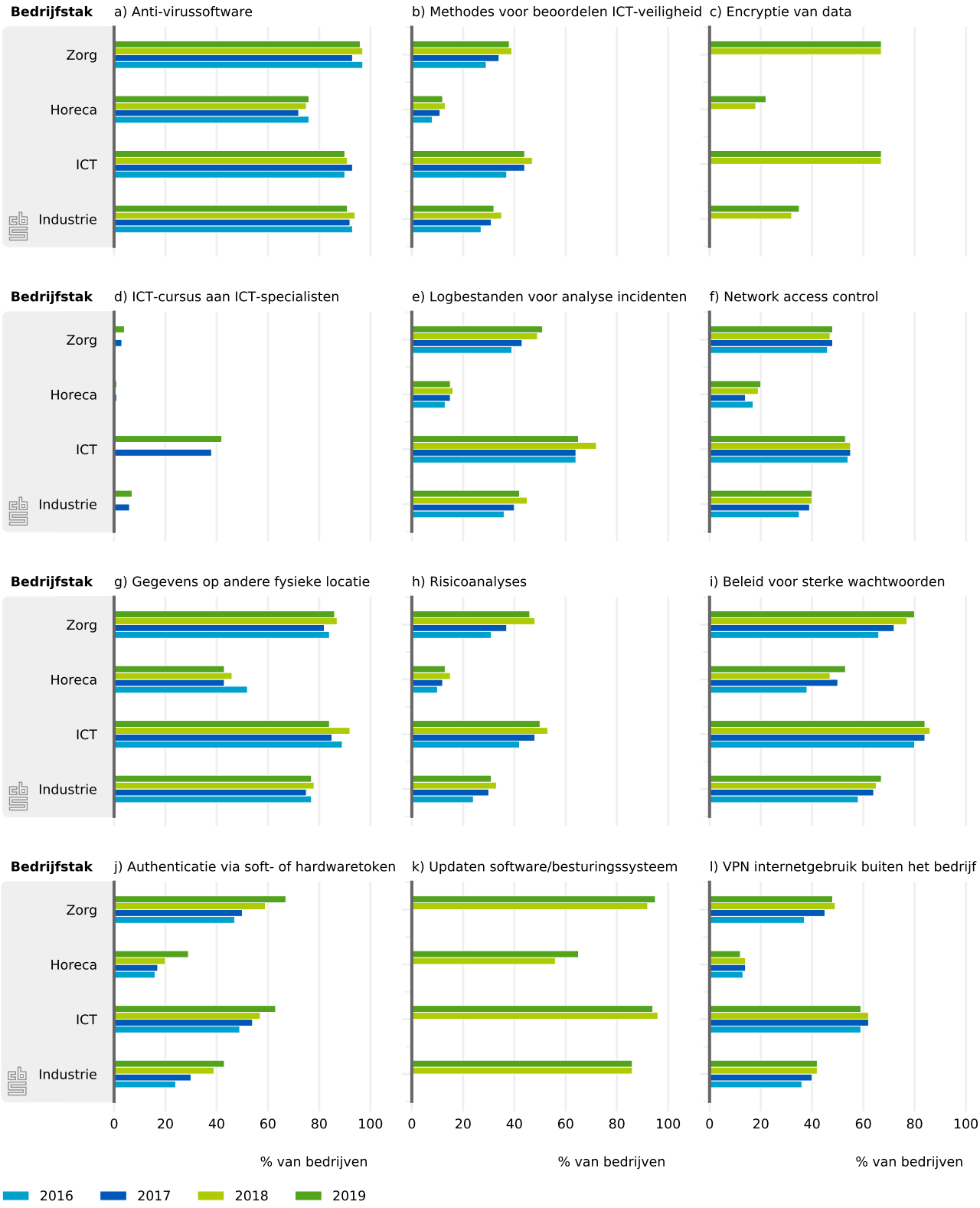
[1)] Let op dat data van een bepaald jaar vaak komt uit de ICT-enquête van het jaar daarna. Zo komt de data die betrekking heeft op 2019 uit de ICT-enquête van 2020(CBS, 2020e).

2.1.1 Genomen ICT-veiligheidsmaatregelen per bedrijfsgrootteklasse voor alle twaalf gevraagde maatregelen over de periode 2016 – 2019. Zie Tabel A.1 voor een volledig overzicht.



Bron: CBS (2017e, 2018e, 2019a, 2020c)

2.1.2 Genomen ICT-veiligheidsmaatregelen per bedrijfstak voor alle twaalf gevraagde maatregelen over de periode 2016 – 2019. Zie Tabel A.2 voor een volledig overzicht.



Bron: CBS (2017e, 2018e, 2019a, 2020c)

de percentages getoond van het aantal bedrijven dat de maatregelen dat jaar heeft toegepast. We lichten voor de duidelijkheid slechts vier bedrijfsgrootteklasse en vier bedrijfstakken uit. Het volledige overzicht kan op StatLine (CBS, 2020b) gevonden worden. 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 je toch kan stellen dat 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 dus 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 2016–2019 te zien dat iedere maatregel vaker door grote dan door kleine bedrijven genomen wordt. Dit is echter voor sommige maatregelen duidelijker waarneembaar dan voor andere. Voor bijvoorbeeld een heel gangbare maatregel als het gebruik van anti-virussoftware (figuur 2.1.1(a)) zijn de verschillen tussen grote en klein bedrijven niet zo groot: meer dan 80 procent van alle bedrijven gebruikt anti-virussoftware, ongeacht de bedrijfsgrootteklasse. Echter, bij een moeilijker toe te passen maatregel zoals het gebruik van een Virtual Private Netwerk (VPN) (figuur 2.1.1(l)) zien we wel grotere verschillen tussen kleine en grote bedrijven: minder dan 30 procent van de bedrijven met 2 tot 10 werknemers maakt gebruik van VPN, tegen meer dan 80 procent van de bedrijven met 250 of meer werknemers. Dat grotere bedrijven meer maatregelen treffen is niet vreemd: grotere bedrijven hebben immers vaker een grotere en meer complexe ICT-infrastructuur en daarom is een breder scala aan beveiligingsmaatregelen nodig om het bedrijf cyberweerbaar te laten zijn.

Toename authenticatie met soft- of hardware-token

Het gebruik van een soft- of hardware token voor het inloggen bij een bedrijf is de laatste vier jaar flink toegenomen. Deze zogenaamde two-factor authenticatie[2)] is een stuk veiliger omdat naast een wachtwoord ook nog een extra code ingevoerd moet worden die per loginsessie verandert. Deze code kan verkregen worden via een speciaal apparaatje met afleesscherm of via een App op de smartphone zoals *Authy*, *Google Authenticator* of *RSA SecureID*. Op deze manier wordt inloggen een stuk veiliger, want zelfs als een wachtwoord onderschept wordt, kan de extra gegeneerde code om in te kunnen loggen extra bescherming bieden.

Voor grote bedrijven is het gebruik van soft- of hardware tokens toegenomen van 71 procent in 2016 tot 87 procent in 2019, zoals te zien in figuur 2.1.1(j). We zien bij alle bedrijfsgrootteklassen dat deze manier van inloggen steeds vaker gebruikt wordt. Zo maken de middelgrote bedrijven met 10 tot 50 werknemers een inhaalslag met een dekking die gestegen is van 29 procent in 2016 naar 54 procent in 2019. Voor kleine bedrijven (2 tot 10 werknemers) zien we zelfs bijna een verdubbeling van het gebruik van hardware-tokens van 23 procent 2017 naar 42 procent in 2019. Overigens bieden steeds meer websites de mogelijkheid tot het gebruik van two-factor authenticatie aan, dus het is aannemelijk dat deze manier van inloggen nog meer in gebruik zal groeien.

ICT-veiligheidsmaatregelen per bedrijfstak

Figuur 2.1.2 laat het aantal maatregelen voor enkele bedrijfstakken zien. 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

[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.

cybersecurity blijkbaar een minder belangrijke rol speelt, zoals de horeca. Wel moet in het achterhoofd gehouden worden dat ook een rol speelt dat de horecagroep relatief meer kleine bedrijven bevat, wat gezien de hierboven beschreven samenhang van het aantal maatregelen met de bedrijfsgrootte ook minder maatregelen impliceert. Bovendien, een horecaonderneming heeft vaak minder ICT-systemen nodig voor de werkzaamheden, dus ligt het voor de hand dat er ook minder ICT-beveiligingsmaatregelen genomen worden.

Aantal genomen ICT-veiligheidsmaatregelen

We hebben gezien dat grote bedrijven vaker meer verschillende ICT-maatregelen nemen dan kleine bedrijven. Dit wordt meer kwantitatief weergegeven in figuren 2.1.3 en 2.1.4, waarbij we per bedrijfsgrootte en bedrijfstak het percentage bedrijven laten zien dat een zeker aantal maatregelen neemt. Kijkend naar de verdeling van het aantal maatregelen per bedrijfsgrootteklasse (figuur 2.1.3) valt te zien dat kleine bedrijven hoger scoren op een kleiner aantal maatregelen, terwijl grote bedrijven juist vaker meerdere maatregelen tegelijk nemen. Van de bedrijven met 250 of meer werknemers neemt zelfs bijna de helft van de bedrijven alle tien maatregelen die uitgevraagd zijn. [3)]

In figuur 2.1.4 kunnen we weer zien dat ICT-bedrijven over het algemeen de meeste maatregelen nemen, terwijl in de horeca vaker wat minder maatregelen afdoende gevonden wordt. Op zich is dit niet opmerkelijk, omdat de noodzaak in de horeca voor bijvoorbeeld het gebruik van VPN-verbindingen veel minder is.

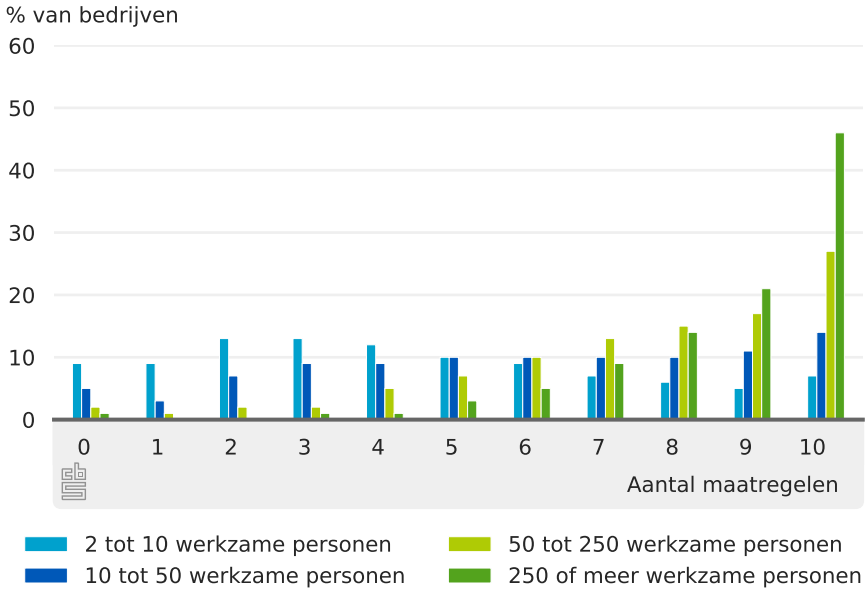
Een kwart van de bedrijven neemt meer dan vijf maatregelen

Uit de verdelingen van het aantal maatregelen kunnen we ook afleiden hoeveel bedrijven minimaal de helft van de gevraagde maatregelen nemen. Dit wordt in figuur 2.1.5 en figuur 2.1.6 per respectievelijk bedrijfsgrootteklasse en bedrijfstak getoond voor de jaren 2016 tot en met 2019. In figuur 2.1.5 is nu goed te zien dat het aantal bedrijven dat vijf of meer maatregelen neemt tot 2018 toegenomen is. In 2019 stagneert deze toename voor de grootste bedrijven met meer dan 50 werknemers, terwijl het aantal bedrijven dat meer dan 5 maatregelen neemt voor bedrijven met 10 tot 50 werknemers zelfs iets afgenomen is. Deze afname moet wel gerelativeerd worden, omdat in 2019 nog steeds meer bedrijven in de groep 10 tot 50 werknemers meer dan vijf maatregelen nemen dan in 2017.

In figuur 2.1.6 wordt per bedrijfstak het aantal bedrijven getoond dat meer dan vijf ICT-veiligheidsmaatregelen treft. Zoals al eerder waargenomen was, is te zien dat in de ICT en in de Zorg een relatief grote groep bedrijven meer dan vijf maatregelen treft (rond de 70 procent), terwijl dit voor de horeca een stuk lager ligt met ongeveer 20 procent. Wel kunnen we zien dat ook per bedrijfstak de afgelopen vier jaar steeds meer bedrijven meer ICT-veiligheidsmaatregelen tegelijkertijd neemt. Ook stagneerde in 2019 het aantal bedrijven met veel ICT-veiligheidsmaatregelen per bedrijfstak in vergelijking met 2018.

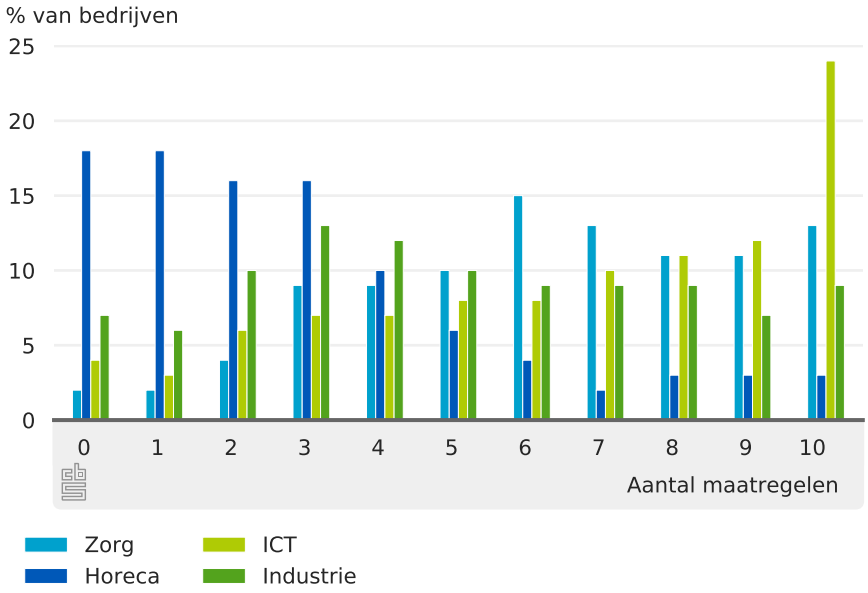
[3)] Van de twaalf maatregelen die in figuur 2.1.1 en figuur 2.1.2 getoond worden, nemen we er maar tien mee in figuur 2.1.3 en figuur 2.1.4 waar we het totaal aantal maatregelen dat bedrijven nemen tonen. Dit omdat de maatregelen 'ICT-cursus aan specialisten' (d) en 'Updaten software' (k) niet over alle jaren beschikbaar zijn.

2.1.3 Verdeling van het aantal cybersecuritymaatregelen per bedrijfsgrootteklasse, 2019



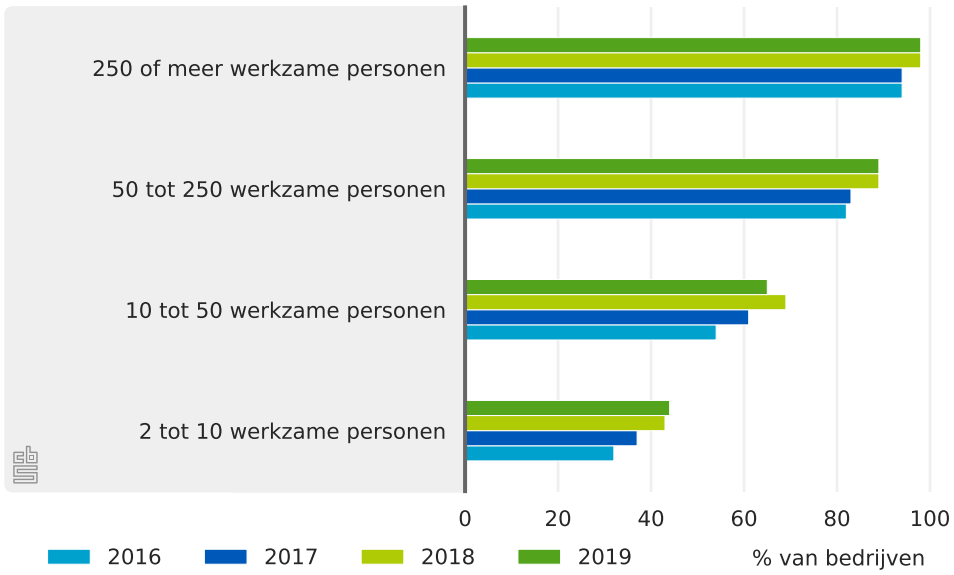
Bron:CBS (2020e)

2.1.4 Verdeling van het aantal cybersecuritymaatregelen per branche, 2019



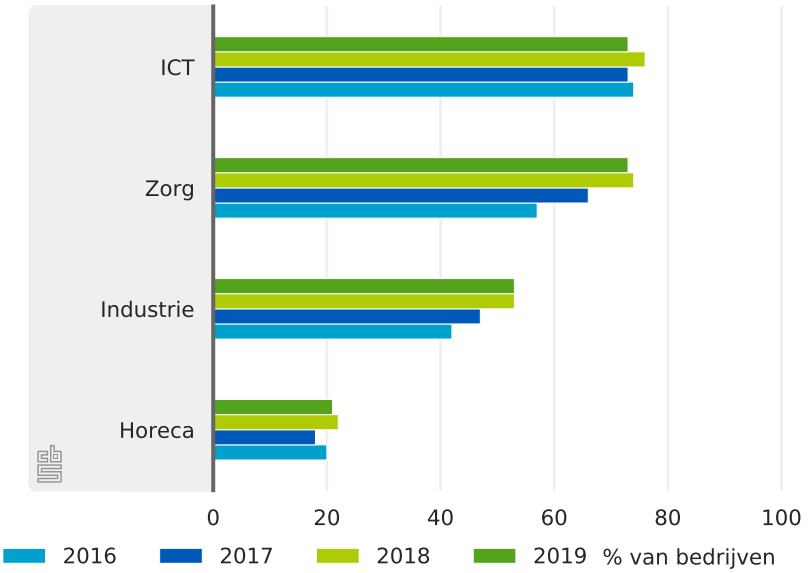
Bron:CBS (2020a)

2.1.5 Percentage van bedrijven dat minimaal vijf van de tien gevraagde cybersecuritymaatregelen neemt per bedrijfsgrootteklasse



Bron: CBS (2020e)

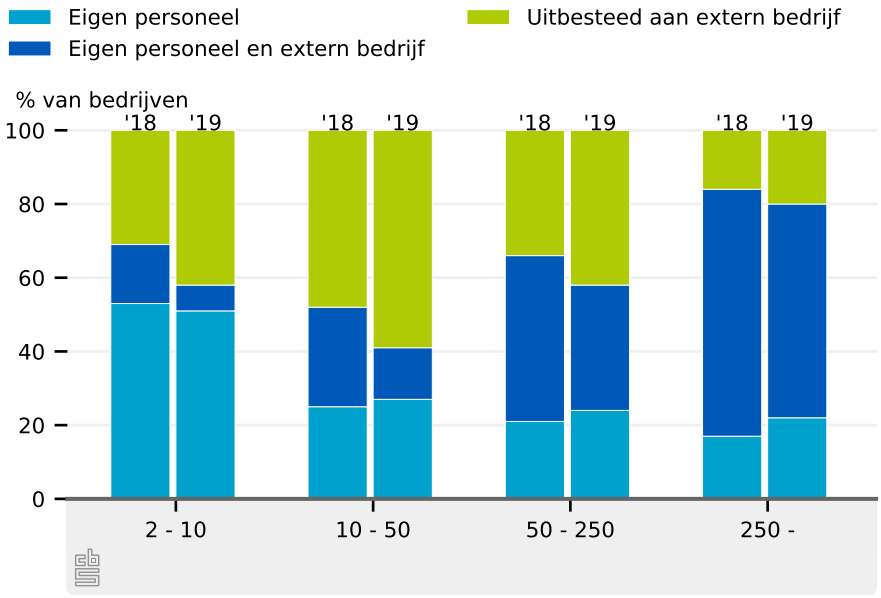
2.1.6 Percentage van bedrijven dat minimaal vijf van de tien gevraagde cybersecuritymaatregelen neemt per bedrijfstak



Bron:CBS (2020a)

Uitvoering ICT-veiligheidswerkzaamheden

2.1.7 Uitvoering ICT-veiligheidswerkzaamheden per bedrijfsgrootteklasse



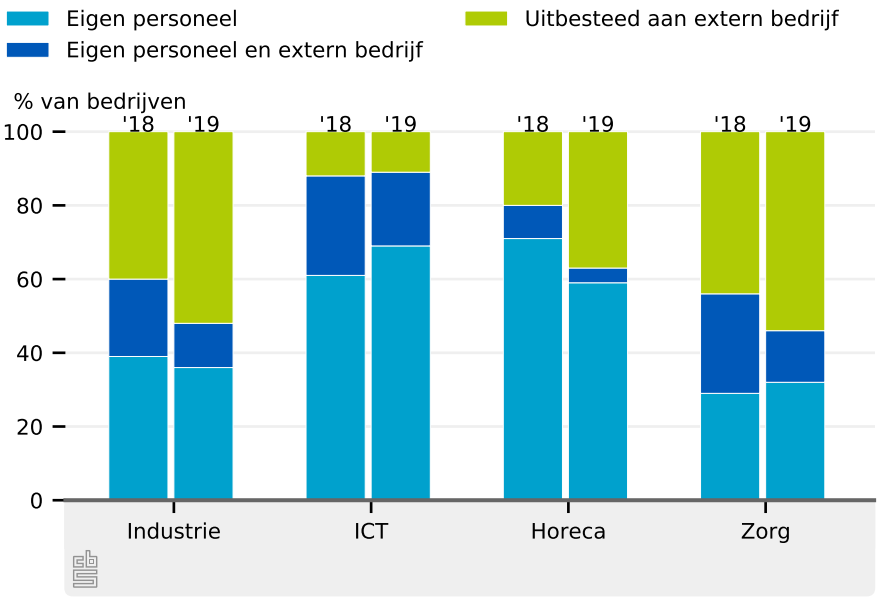
Bron: CBS (2019a, 2020c)

De organisatie van de ICT-beveiliging wordt in figuur 2.1.7 en figuur 2.1.8 onder de loep genomen. Er wordt per bedrijfsgrootteklasse en bedrijfstak gekeken naar wie in 2018 en 2019 de ICT-veiligheidswerkzaamheden binnen het bedrijf uitvoert: eigen personeel, een extern bedrijf of een mix van beide. Meest opvallend is dat dit voor kleine bedrijven vaker door *alleen* eigen personeel gedaan wordt: ongeveer de helft van de kleine bedrijven doet de ICT-beveiliging zelf, terwijl dit voor grote bedrijven zo'n 20 procent is. Aan de andere kant wordt in het geval van kleine bedrijven de ICT-beveiliging vaker *alleen* door een extern bedrijf gedaan: bij ongeveer 40 procent van de kleine bedrijven tegen 20 procent van de grote bedrijven. Bij grote bedrijven zal het dus vaker voorkomen dat zowel externe bedrijven als het eigen personeel de ICT-beveiliging doet. Dit is niet opmerkelijk, omdat een groot bedrijf complexe zaken kan uitbesteden en meer personeel heeft dat de wat meer standaardwerkzaamheden prima zelf kan doen.

Als we in figuur 2.1.8 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 binnen ICT-bedrijven bedrijven voldoende expertise voor handen 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.

Ten slotte kunnen we waarnemen dat in 2019 in vergelijking met 2018 bij alle bedrijfsgrootten en bedrijfstakken het aantal bedrijven dat de ICT-beveiliging doet met zowel het eigen personeel als via een extern bedrijf iets is afgenomen.

2.1.8 Uitvoering ICT-veiligheidswerkzaamheden per bedrijfstak



Bron: CBS (2019a, 2020c)

2.2 Websites

In de vorige paragraaf is getoond hoe bedrijven met maatregelen hun ICT-infrastructuur weerbaar maken tegen dreigingen. In deze paragraaf staan de maatregelen centraal 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. We kijken eerst naar het gebruik van een van die maatregelen, namelijk het toepassen van DNSSEC om de authenticiteit van .nl-domeinnamen te beschermen. Vervolgens besteden we nog aandacht aan het gebruik van internetstandaarden in het algemeen bij bedrijven.

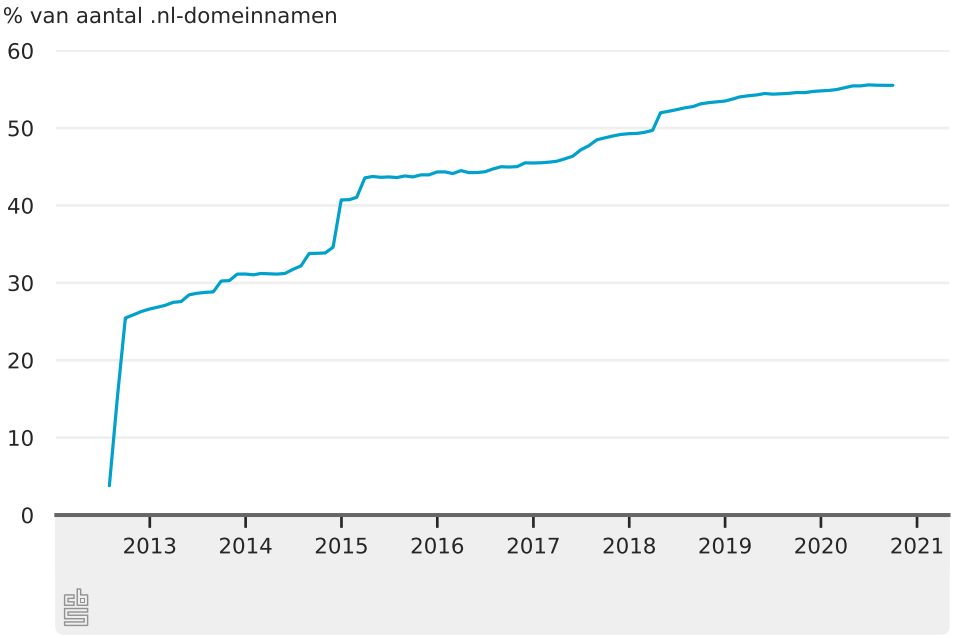
Punt-nl domeinnamen met DNSSEC

Een manier om de veiligheid van een website te verhogen is het toepassen van DNSSEC. DNSSEC is een beveiligingssysteem voor DNS, het internettelefoonboek dat zorgt voor de vertaling van domeinnamen naar IP-adressen. Op zich werkt DNS prima, maar de vertaling van domeinnaam naar IP-adres is niet beveiligd. Dat is een risico, want een kwaadwillende kan verkeer van een gebruiker omleiden naar een vals IP-adres. Het op deze manier misleiden van een internetgebruiker is een beproefde methode om iemand vertrouwelijke gegevens of zelfs geld te ontfutselen. DNSSEC breidt DNS uit met een extra beveiliging: de vertaling van domeinnaam naar IP-adres wordt voorzien van een digitale handtekening. Een internetgebruiker kan die handtekening automatisch laten controleren. Op die manier wordt voorkomen dat hij of zij naar een vals IP-adres wordt geleid. DNSSEC is hiermee een belangrijk wapen in de strijd tegen phishing en pharming. Beide methoden zijn immers gebaseerd op het omleiden van internetgebruikers naar een valse website.

In figuur 2.2.1 is te zien dat het percentage .nl-domeinnamen met DNSSEC gestaag toeneemt. Tussen 1 juni 2012 en 1 oktober 2020 is dit percentage toegenomen van 0 tot 56 procent. Hierbij verliep de toename in de eerste jaren van deze periode wat sneller dan in de latere

jaren. De domeinnaamregistratie en het bijhouden van het gebruik van DNSSEC wordt door de Stichting Internet Domeinregistratie Nederland (SIDN, 2020) uitgevoerd. [4)]

2.2.1 Percentage .nl-domeinnamen met DNSSEC



Bron: SIDN (2020)

Gebruik internetstandaarden bij bedrijven

Achtergrond

In 2020 is het CBS in opdracht van het Ministerie van Economische Zaken en Klimaat in samenwerking met Forum Standaardisatie een onderzoek begonnen naar het gebruik van internetstandaarden bij websites van bedrijven in Nederland. In dit onderzoek heeft het CBS gebruikgemaakt van de website Internet.nl (Platform Internetstandaarden, 2021). Uitgebreide resultaten van het onderzoek zullen medio 2021 worden gepubliceerd (CBS, 2021). Hieronder worden al wat eerste resultaten gepresenteerd.

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

- IPv6: bereikbaarheid via een modern internetadres.

4) De hier getoonde data worden bijgehouden en gepubliceerd door SIDN. (NBIP, 2018).

- DNSSEC: gebruik van een ondertekende domeinnaam.
- https: gebruik van een beveiligde verbinding.
- Beveiligingsopties: gebruik van ingestelde Applicatie-beveiligingsopties.

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

Uiteraard kan deze tool al direct door bedrijven gebruikt worden om hun eigen domeinnaam op veiligheid te toetsen. Indien het resultaat tegenvalt, kan dit bedrijven motiveren om extra beveiligingsmaatregelen toe te passen. In principe is het echter ook mogelijk om de tool te gebruiken om een statistische analyse op domeinnamen van bedrijven in Nederland uit te voeren. Op deze manier kunnen we per bedrijfstak en bedrijfsgrootte in kaart brengen hoe het met de veiligheid van websites van bedrijven is gesteld. Dit is het doel van het onderzoek dat het CBS in 2020 in samenwerking met Platform Internetstandaarden (2021) is gestart.

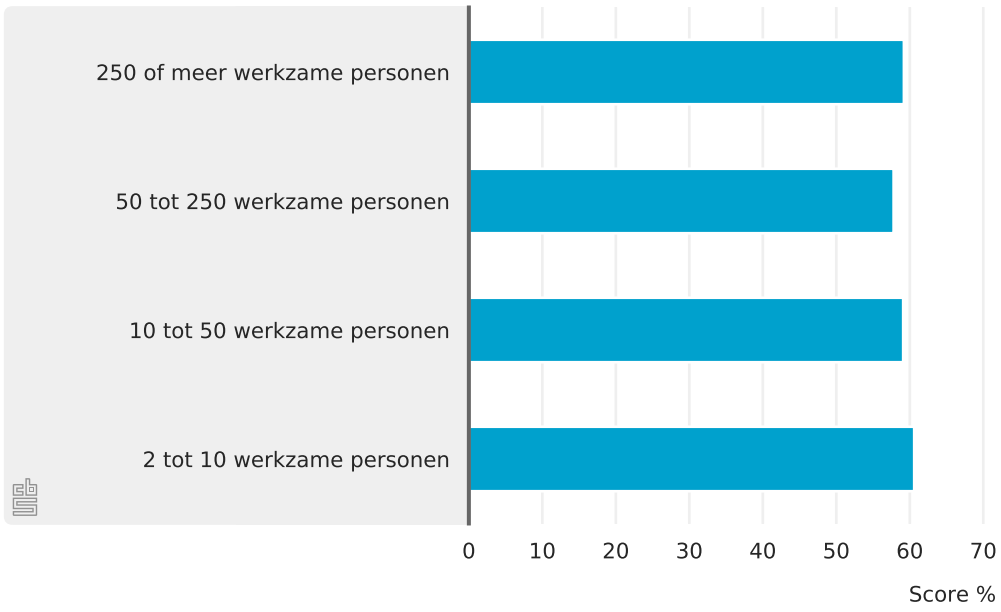
In het onderzoek wordt gebruikgemaakt van alle ongeveer 12 duizend domeinnamen die in de ICT-enquête door bedrijven zijn aangeleverd. Omdat deze bedrijven een representatieve steekproef vormen van alle bedrijven in Nederland kunnen we de resultaten van het onderzoek gebruiken om wat te zeggen over de veiligheid van websites van alle bedrijven. De eerste resultaten van de statistische analyse worden in het vervolg van deze paragraaf getoond. Medio 2021 wordt in een onderzoeksrapport een diepere analyse gepresenteerd CBS (2021).

Eindscore niet afhankelijk van bedrijfsgrootte, wel van bedrijfstak

In figuur 2.2.2 wordt de verdeling van de eindscore van Internet.nl per bedrijfsgrootteklasse getoond. Opvallend is dat de gemiddelde eindscores voor bedrijven bij alle bedrijfsgrootteklassen ongeveer 60 procent zijn. Waar we eerder hierboven nog constateerden dat kleine bedrijven vaak minder maatregelen dan grote bedrijven treffen om hun ICT-systemen te beveiligen, lijkt het er dus op dat de beveiliging van websites van kleine bedrijven even goed, zo niet beter, uitgevoerd wordt dan bij websites van grote bedrijven. Een verklaring zou kunnen zijn dat kleine bedrijven vaker ICT-specialisten inhuren om hun website te bouwen en dat hierbij nieuwere standaarden worden gebruikt. Grote bedrijven hebben wellicht vaker een website die al wat langer geleden ontwikkeld is in een tijd dat er nog minder aandacht was voor standaarden en dat deze later ook niet alsnog zijn toegepast bij onderhoudswerkzaamheden.

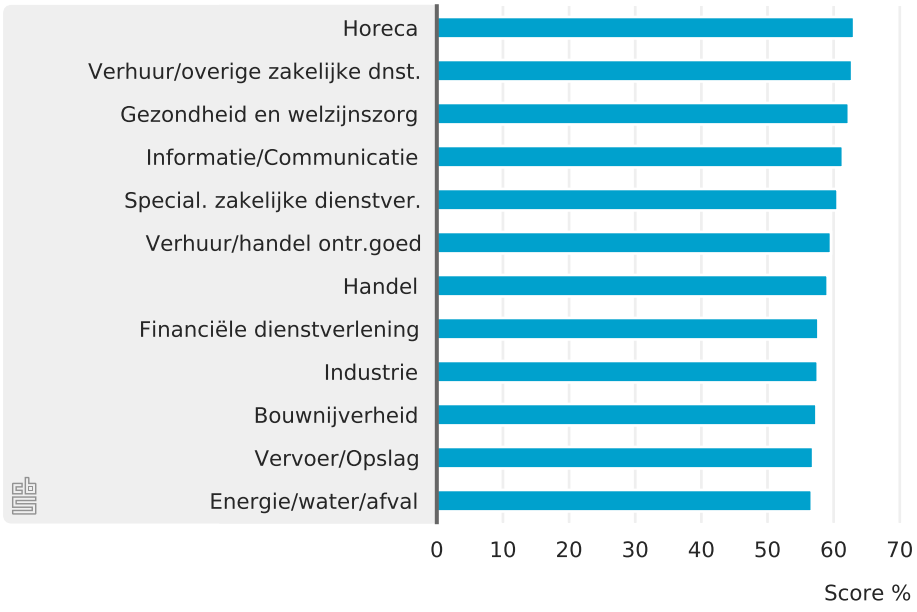
Een ander interessant inzicht is de gemiddelde eindscore per bedrijfstak zoals in figuur 2.2.3 getoond wordt. Hierbij zijn duidelijkere verschillen in gemiddelde eindscore te zien: de websites van de branch 'Energie/water/afval' scoren gemiddeld zo'n 55 procent op basis van Internet.nl, terwijl dit voor de websites van bedrijven in de Horeca bijna 10 procentpunt hoger is, namelijk een gemiddelde eindscore van 64 procent. Ook dit lijkt weer strijdig met onze eerdere constatering dat de Horeca vaak wat achterloopt op het gebied van cyberweerbaarheid van gebruikte ICT-systemen. Wederom ligt als meest voor de hand liggende verklaring voor de hand dat de bouw van veel websites van horeca ondernemingen recenter en vaker door ICT-specialisten is uitgevoerd.

2.2.2 Gemiddelde Internet.nl-score per bedrijfsgrootteklasse



Bron: CBS (2021); Platform Internetstandaarden (2021)

2.2.3 Gemiddelde Internet.nl-score per bedrijfstak.

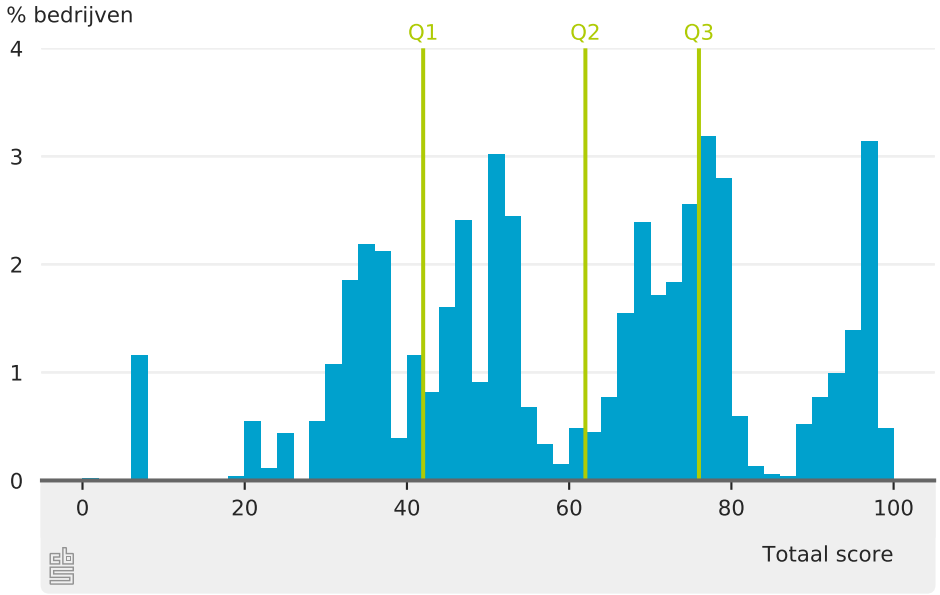


Bron: CBS (2021); Platform Internetstandaarden (2021)

Verdeling van de eindscore aanzienlijk

Alhoewel de gemiddelde score van alle websites van bedrijven in Nederland zo rond de 60 procent ligt, is er wel sprake van een behoorlijke spreiding. De verdeling van de eindscore voor alle bedrijven in Nederland is te zien in figuur 2.2.4. De verdeling kent een aantal pieken rond de 30, 50, 70 en 90 procent. Dit zou te maken kunnen hebben met het feit dat de eindscore bepaald wordt aan de hand van meer dan 200 kenmerken die op een website gescand worden, en dat sommige van die kenmerken mogelijk in clusters voorkomen. In figuur 2.2.4 zijn verder nog drie kwartielen Q1, Q2, en Q3 weergegeven. Het eerste kwartiel Q1 geeft aan dat 25 procent van de bedrijven een eindscore lager dan 44 procent haalt. Het tweede kwartiel Q2, ook bekend als de mediaan, geeft aan dat de helft van alle bedrijven een score hoger dan 64 procent haalt. Het derde kwartiel geeft ten slotte aan dat 25 procent van de bedrijven een score hoger dan 76 procent haalt.

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



Bron: CBS (2021); Platform Internetstandaarden (2021)

Verdeling van de eindscore per kenmerk

Alhoewel we tot nu toe geconcludeerd hebben dat grote en kleine bedrijven ongeveer dezelfde gemiddelde eindscore van 60 procent halen, zien we toch verschillen als we de verschillende kenmerken op bedrijfsniveau gaan analyseren. Voor deze analyse verwijzen we graag door naar de nog te publiceren rapportage (CBS, 2021) waarin deze verschillen zullen worden besproken en ook wat dieper op de methodologie van het onderzoek zal worden ingegaan.

3. Cybersecurity-incidenten

In het voorgaande hoofdstuk hebben we gekeken naar de maatregelen die bedrijven en personen nemen om meer cyberweerbaar te worden. Nu gaan we kijken naar de incidenten die plaatsvinden ondanks alle maatregelen die genomen worden. We onderscheiden hierbij gewone incidenten die door eigen toedoen ontstaan en de incidenten ten gevolge van een aanval van buitenaf. Bij de laatste vorm spreken we ook wel van 'cybercrime'. Cybercrime kan worden omschreven als 'alle delicten die gepleegd worden met behulp van ICT' (CBS, 2018g). We praten dus over delicten (strafbare feiten) door toedoen van cybercriminelen. Te denken valt 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 ten gevolge van een aanval van buitenaf. Voor beide groepen onderscheiden we weer drie type incidenten: 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:

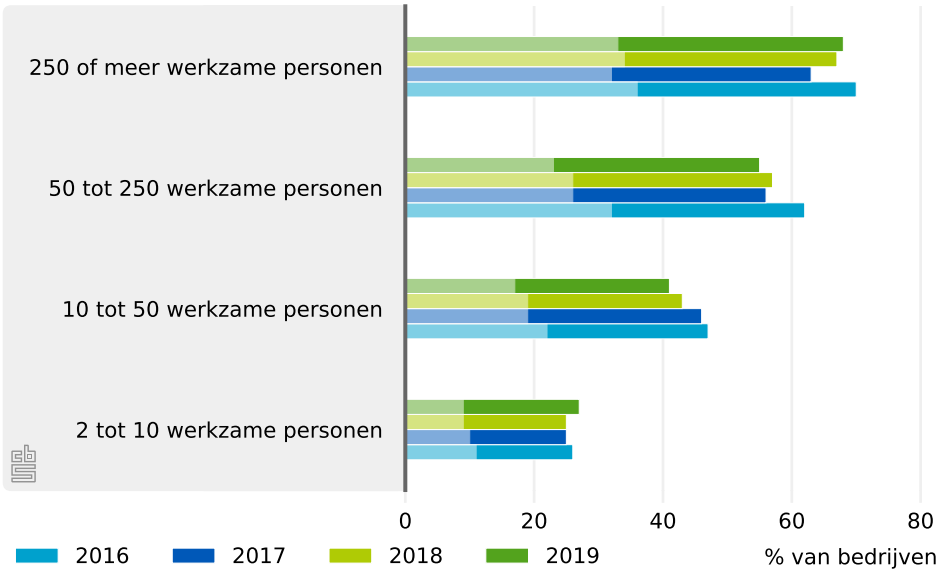
1. *Uitval van ICT-systeem* als gevolg van een ICT-gerelateerd veiligheidsincident, zoals een hardware- of softwarestoring.
2. *Datavernietiging of dataverminking* als gevolg van een ICT-gerelateerd veiligheidsincident, zoals een hardware- of softwarestoring.
3. *Dataonthulling* door onopzettelijk toedoen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

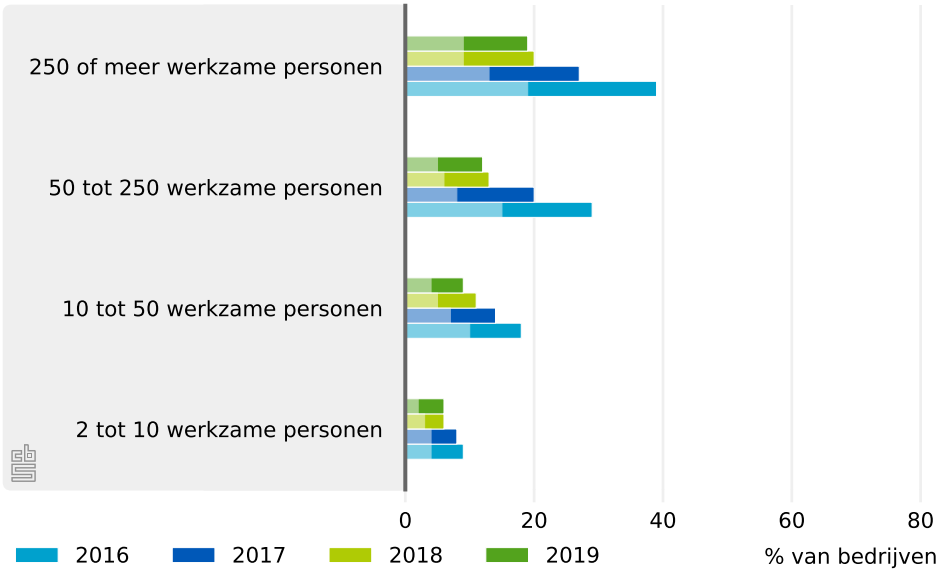
3.1.1 ICT-veiligheidsincidenten door interne oorzaak per bedrijfsgrootteklasse, waarbij het lichtekleurde deel het aandeel van incidenten dat met kosten gepaard ging weergeeft.



Lichtgekleurde deel: incidenten met kosten

Bron: CBS (2017e, 2018e, 2019a, 2020c)

3.1.2 ICT-veiligheidsincidenten door aanval van buitenaf per bedrijfsgrootteklasse, waarbij het lichtgekleurde deel het aandeel van incidenten dat met kosten gepaard ging weergeeft.



Lichtgekleurde deel: incidenten met kosten

Bron: CBS (2017e, 2018e, 2019a, 2020c)

Cybersecurityincidenten per bedrijfsgrootte

In de ICT-enquête wordt aan een representatieve steekproef van bedrijven gevraagd hoe vaak ze te maken hebben gehad met elk van de genoemde ICT-veiligheidsincidenten. Ook wordt gevraagd of er kosten waren verbonden aan de ICT-veiligheidsincidenten. Deze vragen zijn nu vier opeenvolgende jaren voorgelegd. We bekijken nu eerst naar de resultaten per bedrijfsgrootteklasse. Daarna zullen we ook kijken naar de ontwikkeling van ICT-veiligheidsincidenten per bedrijfstak.

Grote bedrijven hebben steeds vaker incidenten

In figuren 3.1.1 en 3.1.2 wordt voor de periode 2016–2019 per bedrijfsgrootteklasse het percentage van bedrijven getoond dat minstens één ICT-veiligheidsincident heeft gehad ten gevolge van respectievelijk een interne oorzaak of een aanval van buitenaf. Voor beide figuren worden dus de in paragraaf 3.1.1 genoemde typen incidenten (uitval ICT-system, datavernietiging, en dataonthulling) samengenomen. Het lichtgekleurde deel van de staafdiagrammen geeft het percentage van bedrijven weer dat aangeeft dat er ook kosten met het ICT-incident gemoeid waren.

Meest opvallend is dat grote bedrijven over de jaren heen consistent meer incidenten rapporteren dan kleine bedrijven voor zowel interne incidenten als incidenten door een aanval van buitenaf. Dit kan meerdere oorzaken hebben. Voor de interne incidenten, zoals uitval van ICT-systemen door hardware of software storingen, speelt mee dat grote bedrijven vaker een grotere, meer complexe ICT-infrastructuur hebben: met meer computers en andere hardware binnen het bedrijf wordt de kans uiteraard groter dat er in een jaar ook wat kapot gaat. Als je kijkt naar incidenten door een aanval van buitenaf kunnen we aannemen dat grote bedrijven vaak interessanter voor cybercriminelen zijn omdat er meer te halen valt of de (publiciteits) schade groter is. Wat verder nog een rol speelt, is dat bij grote bedrijven vaak meer ICT-specialisten werken, wat ook de kans groter maakt dat ICT-veiligheidsincidenten gedetecteerd worden die misschien bij kleine bedrijven onder de radar blijven.

De helft van de ICT-veiligheidsincidenten gaat gepaard met kosten

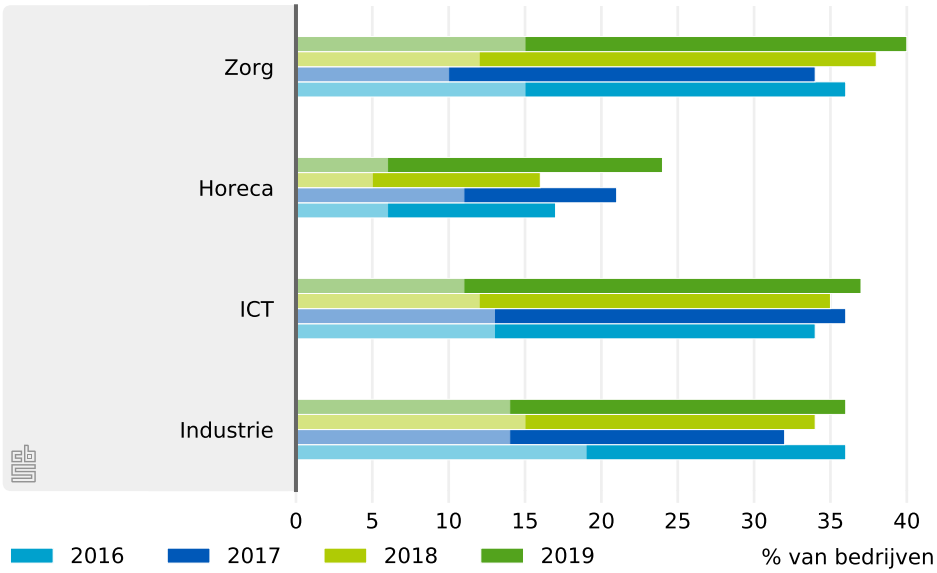
In figuren 3.1.1 en 3.1.2 is te zien dat lang niet alle ICT-veiligheidsincidenten met kosten gepaard gaan. Ongeveer de helft van de bedrijven die ICT-veiligheidsincidenten rapporteren, zegt hier ook kosten aan gehad te hebben. Even vaak komt het dus voor dat er wel sprake was van een ICT-veiligheidsincident, maar dat dit niet direct tot kosten heeft geleid. Dit geldt voor zowel incidenten met een interne oorzaak als incidenten ten gevolge van een aanval van buitenaf.

Aantal bedrijven met ICT-veiligheidsincidenten neemt af

Ten slotte kunnen we uit figuren 3.1.1 en 3.1.2 aflezen dat voor de meeste bedrijfsgrootteklassen het totaal aantal interne en externe ICT-veiligheidsincidenten over de laatste vier jaar is afgenomen. Voor de incidenten met een interne oorzaken is dit niet heel duidelijk, zeker niet voor de grootste bedrijven: bij deze groep zien we een juist toenemende trend over de jaren 2017–2019. 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.

Voor de ICT-veiligheidsincidenten door een aanval van buitenaf is de afname voor alle bedrijfsgrootteklassen echter onmiskenbaar. Zo is te zien dat in 2016 bijna 40 procent van de grote bedrijven (250 of meer werknemers) met een ICT-veiligheidsincident te maken heeft gehad, terwijl dat in 2019 minder dan 20 procent was. Een halvering van het aantal

3.1.3 ICT-veiligheidsincidenten door interne oorzaak per bedrijfstak, waarbij de lichtgekleurde deel het aandeel van incidenten dat met kosten gepaard ging weergeeft.



Lichtgekleurde deel: incidenten met kosten

Bron: CBS (2017e, 2018e, 2019a, 2020c)

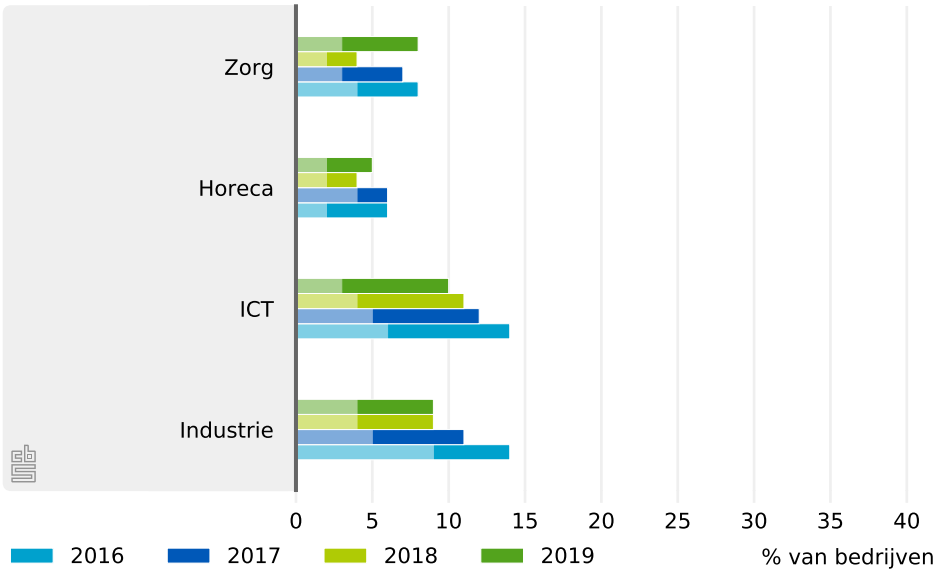
meldingen over de afgelopen vier jaar dus. Ook als je alleen naar de incidenten met kosten kijkt, kan je zien dat het aantal meldingen gehalveerd is: in 2016 gaf 19 procent van de grote bedrijven aan een ICT-veiligheidsincident met kosten gehad te hebben, terwijl dat in 2019 nog maar 9 procent was. Deze afname van het aantal ICT-veiligheidsincidenten door een aanval van buitenaf is waarneembaar voor alle bedrijfsgrootteklassen. Toch zal verderop aangetoond worden dat deze afname wel iets genuanceerder bekeken moet worden, omdat het beeld een gemiddelde betreft en de ontwikkelingen per type incident ook een rol spelen.

Cybersecurityincidenten per bedrijfstak

In figuren 3.1.3 en 3.1.4 wordt voor de periode 2016–2019 het aantal ICT-veiligheidsincidenten met respectievelijk interne en externe oorzaak per bedrijfstak uitgesplitst voor alle 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.

Opvallend is dat het aantal incidenten met interne oorzaak niet heel duidelijk met de bedrijfstak samenhangt. Voor de bedrijfstakken die we in figuur 3.1.3 bekijken, vinden we dat ongeveer een derde van de bedrijven een intern incident heeft gemeld, waarvan weer ongeveer de helft kosten met zich meebracht. Alleen de horeca meldt aanzienlijk minder incidenten: in 2019 meldde ongeveer 20 procent van de horecabedrijven een veiligheidsincident. Op zich is dit niet heel vreemd omdat in de horeca waarschijnlijk gewoon minder met een computer gewerkt wordt, zodat de kans op uitval door een hardware- of softwarestoring ook kleiner is.

3.1.4 ICT-veiligheidsincidenten door aanval van buitenaf per bedrijfstak, waarbij het lichtgekleurde deel het aandeel van incidenten dat met kosten gepaard ging weergeeft.



Lichtgekleurde deel: incidenten met kosten

Bron: CBS (2017e, 2018e, 2019a, 2020c)

Voor incidenten door een aanval van buitenaf vinden we vooral lage percentages van bedrijven die hier melding van maken: voor ICT-bedrijven en de industriebedrijven zo rond de 10 procent; voor de zorg en horeca tussen de 5 en 7 procent van de bedrijven. Opnieuw zien we bij de ICT en de industrie dat het percentage van bedrijven dat een incident door een aanval van buitenaf meldt over de laatste vier jaar afgenomen is. Deze trend vonden we voor de jaren 2016–2018 ook terug bij de horeca en gezondheidszorgbedrijven, maar het laatste jaar zien we hier weer een toename van het aantal incidenten door een aanval van buitenaf.

Cybersecurityincidenten per type incident

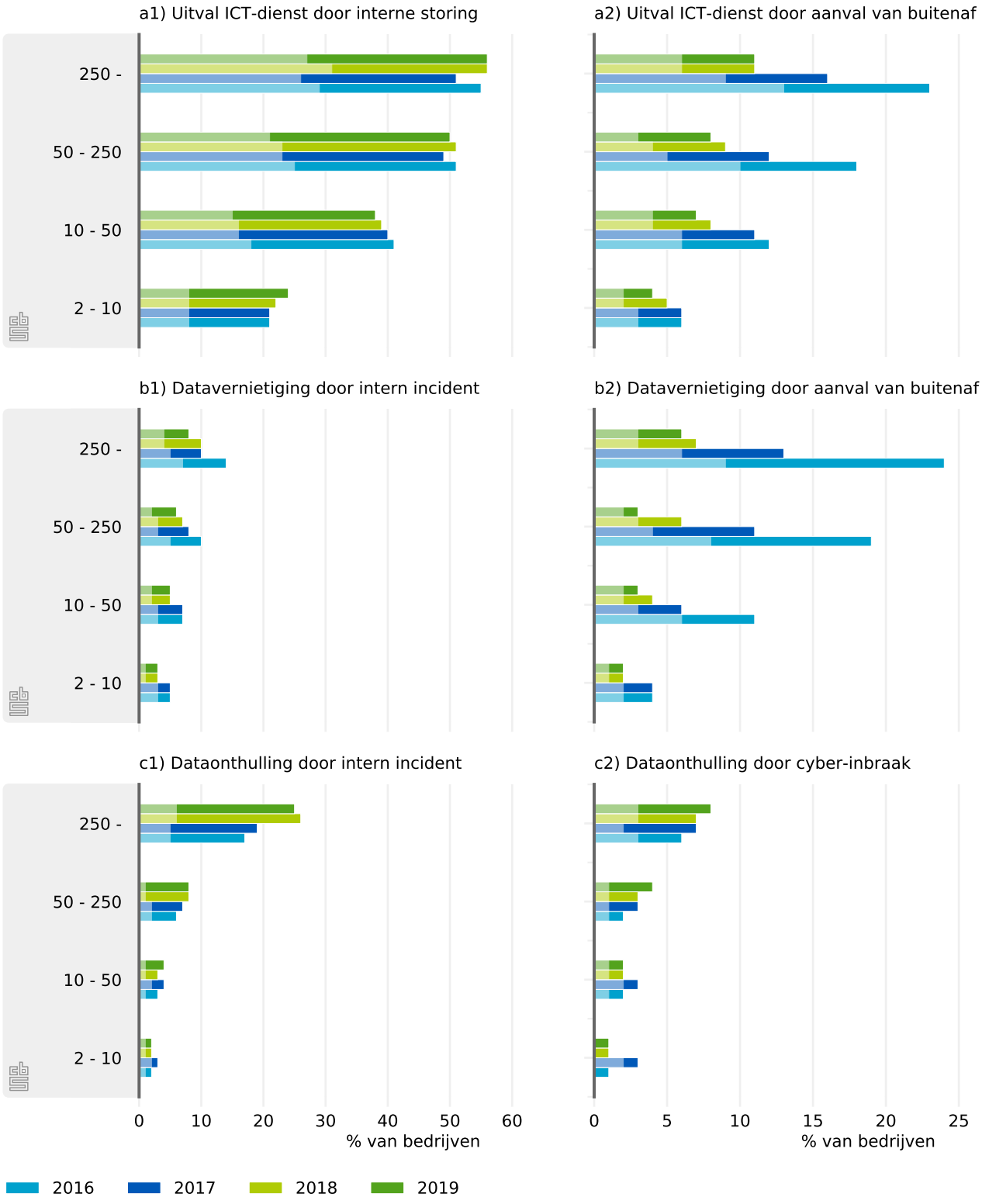
We hebben tot nu toe gekeken naar het percentage bedrijven dat een incident gemeld heeft opgesplitst naar interne incidenten en door een aanval van buitenaf. De belangrijkste conclusie was dat voornamelijk het percentage bedrijven dat een incident meldt door een aanval van buitenaf over de laatste vier jaar afgenomen is. We zullen nu kijken wat de bijdragen van de 3 typen incidenten zijn: uitval, datavernietiging en dataonthulling.

Cybersecurityincidenten per type incident per grootteklasse

In figuren 3.1.5(a1–c1) toont de linker kolom de interne ICT-veiligheidsincidenten voor respectievelijk uitval van ICT-systemen, datavernietiging en dataonthulling.
Figuren 3.1.5(a2–c2) geven de incidenten door een aanval van buitenaf voor dezelfde drie typen incidenten.

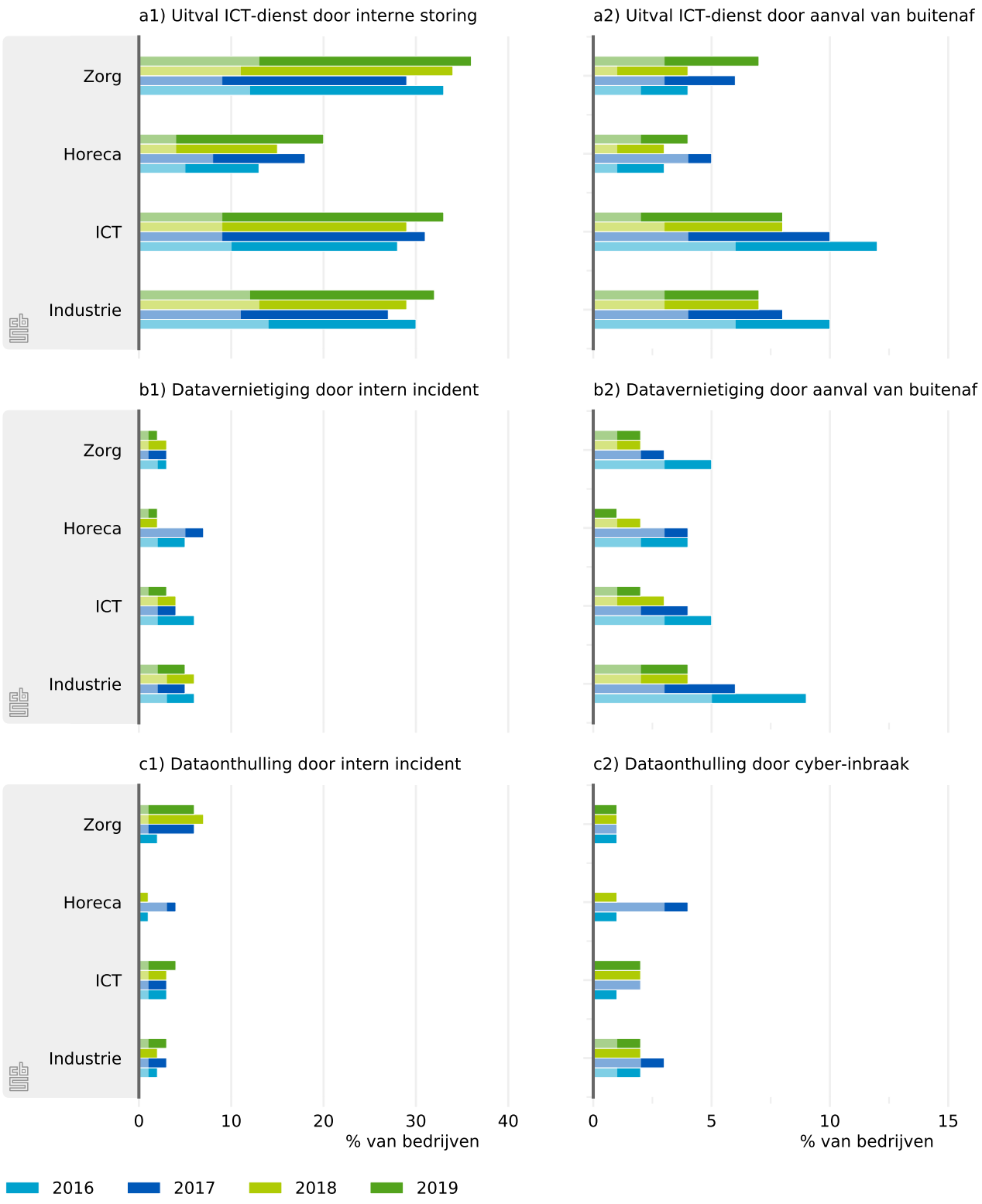
Er was eerder al geconcludeerd dat het aantal interne incidenten toeneemt met de bedrijfsgrootte. Als we naar de drie typen interne incidenten kijken dan zien we dat deze

3.1.5 ICT-veiligheidsincidenten per categorie per bedrijfsgrootteklasse, waarbij het lichtgekleurde deel het aandeel van incidenten dat met kosten gepaard ging weergeeft. Zie Tabel A.1 voor een volledig overzicht.



Bron: CBS (2017e, 2018e, 2019a, 2020c)

3.1.6 ICT-veiligheidsincidenten per categorie per bedrijfstak, waarbij het lichtgekleurde deel het aandeel van incidenten dat met kosten gepaard ging weergeeft. Zie Tabel A.2 voor een volledig overzicht.



Lichtgekleurde deel: incidenten met kosten

Bron: CBS (2017e, 2018e, 2019a, 2020c)

toename voornamelijk toe te schrijven is in aan de uitval van ICT-systemen door een hardware- of softwarestoring, zoals te zien is in figuur 3.1.5(a1): ongeveer 20 procent van de kleine bedrijven rapporteert een uitval door een storing, terwijl dit voor grote bedrijven zo'n 55 procent is. Datavernietiging door een hardware storing komt bij minder dan 10 procent van de bedrijven voor; bovendien is de koppeling aan de bedrijfsgrootte minder sterk aanwezig. Wel is te zien dat ook dataonthulling vaker bij grote dan bij kleine bedrijven voorkomt, maar omdat het hier om kleine percentages gaat, draagt deze categorie een stuk minder bij aan het totaal van interne incidenten. De ontwikkeling in de tijd is voor de interne incidenten minder duidelijk en varieert van categorie tot categorie. Bij de dataonthulling door een intern incident, getoond in figuur 3.1.5(a3), is een duidelijke *toename* in de tijd te zien voor de grote bedrijven van 250 of meer werknemers. Dit in tegenstelling tot de afname die we bij het totaal van interne incidenten gevonden hebben. Het maakt nogal uit naar welk type incident je kijkt.

Figuur 3.1.5(a2–c2) laat zien dat alle typen incidenten ten gevolge van een aanval van buitenaf weer toenemen met de bedrijfsgrootte, zoals we al eerder bij het totaal van incidenten door een aanval constateerden. Er was eerder geconstateerd dat het percentage bedrijven dat incidenten rapporteert door een aanval van buitenaf afneemt over de tijd. Maar net als bij de interne incidenten is dit 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, met name 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.

Meldingen datalekken bij Autoriteit Persoonsgegevens

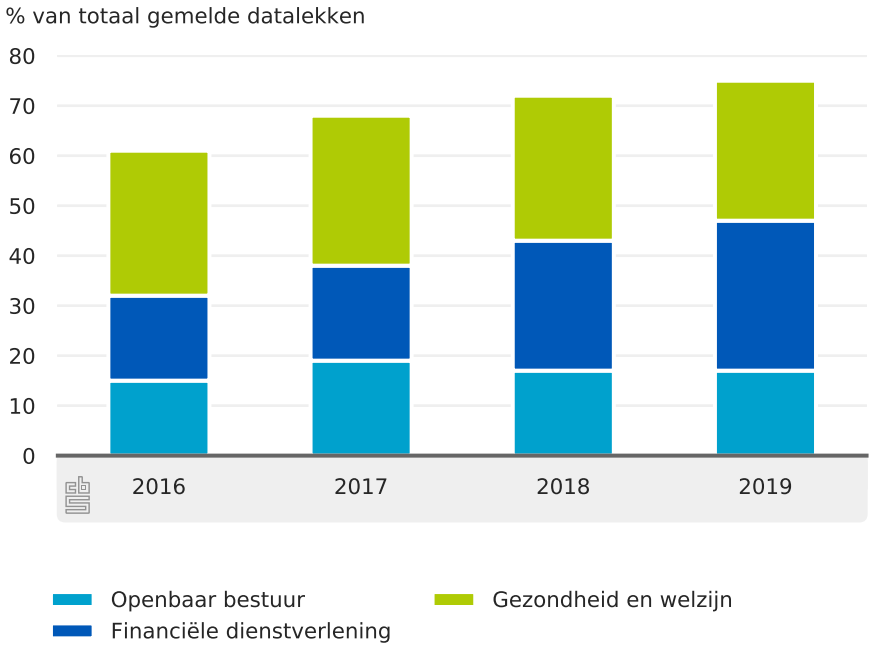
Uit het voorgaande is gebleken dat over de afgelopen vier jaar meer bedrijven melden dat ze ICT-veiligheidsincidenten meemaakten in de vorm van het dataonthullingen, zowel door eigen toedoen (zoals het verliezen van een USB-stick door eigen personeel) als door cybercrime. In Nederland zijn bedrijven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

27 duizend meldingen van datalekken

In 2019 zijn 26 956 datalekken gemeld bij de Autoriteit Persoonsgegevens, terwijl dit er in 2018 nog 20 881 waren. [1)] De meldplicht datalekken geldt in Nederland al sinds 2016. Deze meldplicht is in EU-verband verder geformaliseerd en gepreciseerd door de Algemene verordening gegevensbescherming (AVG) die sinds 25 mei 2018 van toepassing is. Het gaat hier over privacygevoelige gegevens die mogelijk in handen van derden zijn gevallen of waar derden toegang tot hebben gehad. Ook hier geldt dat de oorzaak van dit soort datalekken soms onbedoeld is en terug te voeren is op slordige omgang door de houder van de gegevens. Aan de andere kant van het spectrum staat het moedwillig hacken van dit soort gegevensbronnen om te illustreren hoe slecht deze gegevens beveiligd zijn, of om er daadwerkelijk iets mee te gaan doen, bijvoorbeeld te verkopen.

1) Autoriteit Persoonsgegevens (2019b).

3.1.7 Melding van datalekken bij de Autoriteit Persoonsgegevens naar bedrijfstak en organisatie



Bron: Autoriteit Persoonsgegevens (2019a)
N.B. 25 mei 2018 werd de Algemene verordening gegevensbescherming (AVG) van kracht.

Meeste meldingen uit de financiële dienstverlening

Het overgrote deel van de gemelde datalekken is afkomstig uit de gezondheidszorg (ziekenhuizen, apotheken, GGZ-instellingen e.d.), de financiële sector (betaalservices, banken, verzekeringen e.d.) en het openbaar bestuur (gemeenten, rijksoverheid e.d.). In 2016 waren deze drie sectoren goed voor 61 procent van alle gemelde datalekken, in 2017 was dit opgelopen tot 68 procent en in 2019 tot 75 procent. Dit zijn ook voorbeelden van sectoren waar veel en 'gevoelige' persoonsgegevens worden verwerkt en opgeslagen. Van deze drie sectoren kwamen tot 2019 de meeste meldingen uit de gezondheidszorg. In 2019 kwamen de meeste meldingen vanuit de financiële dienstverlening.

Aan de andere kant zegt het ook weer niet alles dat er veel meldingen uit deze sectoren komen en niet uit bijvoorbeeld de energiesector. Het aantal bedrijven, instellingen en organisaties in de gezondheidssector is immers ook vele malen groter dan het aantal bedrijven in de energiesector. Daar het absolute aantal gemelde datalekken fors is toegenomen gaat het ook voor deze sectoren om sterk toenemende aantallen datalekken. In 2016 kwam 61 procent van alle gemelde datalekken nog overeen met ongeveer 3 500 meldingen. In 2019 was de genoemde 75 procent goed voor 15 duizend meldingen.

Vijf procent datalekken door hack

Bij twee derde (66 procent) van de gemelde datalekken gaat het om het versturen of afgeven van persoonsgegevens aan een verkeerde ontvanger. Dit was ook het meest gemelde type datalek in 2018 (63 procent) en in 2017 (47 procent). Bij dit type datalek kan het gaan om een e-mail met daarin gevoelige persoonsgegevens die wordt verzonden naar de verkeerde ontvanger. Bijvoorbeeld door een typefout of omdat er in het e-mailprogramma een verkeerde geadresseerde wordt geselecteerd. Daarnaast komt het voor dat personen hun

eigen gegevens opvragen bij organisaties, maar door een administratieve fout vervolgens ook persoonsgegevens van anderen ontvangen. In 2020 was 5 procent van het aantal gemelde datalekken veroorzaakt door het via hacken, malware en/of phishing toegang krijgen tot de betreffende gegevens (902 meldingen). In 2018 was dit nog 4 procent (2017: 6 procent).

Uit de resultaten van de ICT-enquête bleek dat bij de grote bedrijven met 250 of meer werknemers er ongeveer twee keer zoveel bedrijven een incident melden door een interne oorzaak dan een incident door een aanval van buiten. Dit hoeft niet in tegenspraak te zien met de constatering dat bij de Autoriteit Persoonsgegevens het aantal meldingen door een aanval van buiten slechts 5 procent uit maakt van het totaal aantal meldingen. De ICT-enquête rapporteert immers het percentage bedrijven dat een incident gehad heeft, terwijl de AP het aantal meldingen zelf meet. Eén bedrijf kan meerdere meldingen doen, dus de getallen zijn niet direct met elkaar te vergelijken. Wat wel overeenkomt, is dat beide bronnen een toename van het aantal incidenten met onthullingen van gegevens laten zien.

Omvang datalekken en hacken

In de ruime meerderheid van de gevallen, namelijk 64 procent in 2019, raakt het datalek één persoon. In veel mindere mate (4 procent) treft het datalek meer dan 500 personen. Datalekken die meer dan 500 personen raken, worden vaak veroorzaakt door hacking, malware en/of phishing. Datalekken door hacking en phishing komen met name voor in de zorg (18 procent). Van de genoemde 902 datalekken in 2019 door hacking, malware en/of phishing was in 30 procent van de gevallen het aantal betrokken personen meer dan 500. Datalekken door hacking, malware en/of phishing kwamen in 2019 relatief vaak voor in de zakelijke dienstverlening (14 procent), de zorg (13 procent) en het onderwijs (13 procent).

De voorgaande voorbeelden van incidenten illustreren dat niet alles wat er mis kan gaan met ICT kwade opzet is. De primaire oorzaak van een incident komt niet altijd vanuit ‘cyberspace’ maar kan ook voortkomen uit menselijke tekortkomingen (slordigheid, vergeetachtigheid, onbekwaamheid e.d.).

DDoS-aanvallen

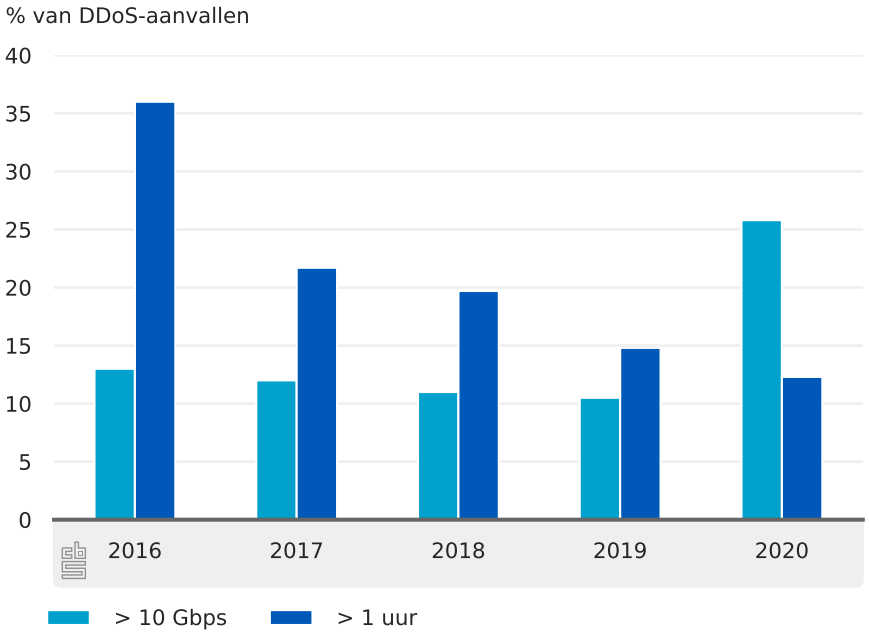
Van kwade opzet is wel sprake bij een zogeheten (Distributed) Denial of Service aanval (DDoS). Bij zo’n aanval wordt een bepaalde dienst (bijvoorbeeld een website) onbereikbaar gemaakt voor de gebruikelijke bezoekers. Een DDoS-aanval op een website wordt vaak uitgevoerd door de website te bestoken met veel netwerkverkeer opdat deze omvalt. De in de figuur 3.1.8 gepresenteerde cijfers zijn afkomstig van de Stichting Nationale Beheersorganisatie Internet Providers (NBIP) en hebben betrekking op de DDoS-aanvallen van de bij hen aangesloten partijen die gebruikmaken van de Nationale anti-DDoS-Wasstraat (NaWas). Dit is een hulpmiddel dat DDoS-aanvallen onschadelijk maakt en waar de aangesloten partijen (collectief) gebruik van maken. Het zijn dus niet alle DDoS-aanvallen waar Nederlandse websites mee te maken hebben, maar wel een groot deel daarvan. [2)] Het absolute aantal DDoS-aanvallen is hierdoor wellicht iets minder veelzeggend dan de karakteristieken van de DDoS-aanvallen, ook omdat het aantal deelnemers van deze dienst gestaag toeneemt (van 53 in 2016 tot 97 in 2020).

Kenmerken van DDoS-aanvallen zijn de omvang (Gbps) en de duur (tijd). In 2019 had 11 procent van de DDoS-aanvallen een omvang van meer dan 10 Gbps. Dit is vergelijkbaar

2) De bij de NaWas aangesloten organisaties vertegenwoordigen ca. 2,5 miljoen .nl-domeinnamen (NBIP, 2020).

met de voorgaande jaren. In 2019 duurde 15 procent van de aanvallen langer dan een uur. Dit is minder dan in de voorgaande jaren. In 2020 wordt echter gemeld dat het aandeel van DDoS-aanvallen van langer dan een uur behoorlijk toegenomen is, tot meer dan 25 procent. Hierbij moet opgemerkt worden dat de grootte van een DDoS-aanval niet per se maatgevend is voor de schade die een DDoS-aanval aanbrengt. Ook de complexiteit van de aanval speelt een rol; een DDoS-aanval waarbij meerdere technieken gecombineerd worden, een zogenaamde multivector aanval, is veel moeilijker te mitigeren. Daarnaast is het soort DDos-aanval waar websites mee geconfronteerd worden onderwerp van ontwikkeling. Het mitigeren van een DDos-aanval vergt dus een continue inspanning met betrekking tot het up-to-date houden van de software van de NaWas. Het absolute aantal door de NaWas verwerkte DDos-aanvallen in 2019 en 2020 was respectievelijk 919 en 929 (2018: 938; 2017: 826; 2016: 680).

3.1.8 DDoS-aanvallen naar grootte en duur[1)]



Bron: NBIP (2020)

[1)] DDos-aanvallen van bij de NaWas aangesloten organisaties. Deelnemers aan de NaWas zijn niet gelimiteerd tot (kleinere) ISPs. Er zijn ook enkele grote organisaties die meedoen, zoals banken en verzekeraars.

4.
Cybercrime

We presenteren in dit hoofdstuk enkele cijfers uit de bij de politie geregistreerde misdrijven waar cybercrime in is opgenomen. In de Cybersecuritymonitor van vorig jaar (CBS, 2019f) is ook statistische informatie over cybercrime opgenomen verkregen uit van de publicatie Digitale Veiligheid en Criminaliteit (DVC), zie (CBS, 2018h). Dit onderzoek is niet meer herhaald, dus deze gegevens worden hier weglaten. In dit hoofdstuk presenteren we dus alleen de bij de politie geregistreerde gegevens over cybercrime.

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.

4.1 Computervredebreuk

Eén van de cybercrime-incidenten die door de politie als zodanig geregistreerd wordt, is de zogenaamde computervredebreuk: het binnendringen van een netwerk of computersysteem zonder toestemming van de eigenaar. Computervredebreuk is de juridische term voor dit delict, maar gangbaarder in het spraakgebruik is ook wel het hacken van een computersysteem. We gebruiken hier de termen door elkaar. In de publicatie van vorig jaar (CBS, 2019f) zijn de hackincidenten gepubliceerd die niet bij de politie geregistreerd zijn, maar uit de DVC-publicatie (CBS, 2018h) volgden. Van deze cijfers zijn geen nieuwe gegevens bekend. Om deze reden zijn in deze publicatie alle niet-geregistreerde gegevens over cybercrime weggelaten.

Geregistreerde computervredebreuk

In deze paragraaf gaan we in op de bij de politie geregistreerde computervredebreuk. We kijken eerst naar de computervredebreukincidenten omdat deze met een eigen

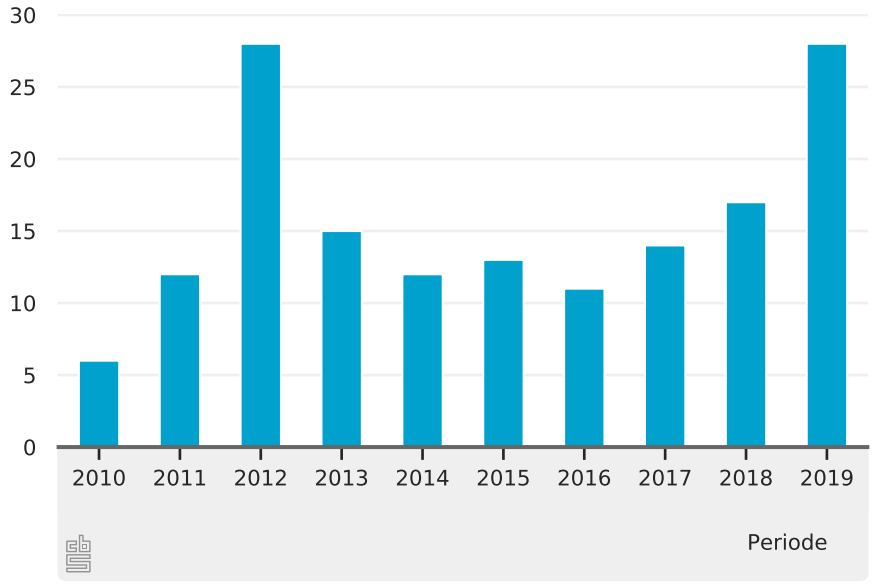
4.1.1 Bij de politie geregistreerde computervredebreuk

	2013	2014	2015	2016	2017	2018	2019	Eenheid
Totaal geregistreerde computervredebreuk	2525	2045	2225	1875	2320	2945	4865	*aantal*
Geregistreerde misdrijven, relatief	0,2	0,2	0,2	0,2	0,3	0,4	0,6	*% van alle misdrijven*
Geregistreerde misdrijven per 100 000 inw.	15	12	13	11	14	17	28	*per 100 000 inw.*
Totaal opgehelderde computervredebreuk	255	195	165	170	185	390	355	*aantal*
Opgehelderde misdrijven, relatief	10	9,5	7,4	9	8,1	13,3	7,3	*% van geregistreerde computervredebreuk*
Registraties van verdachten	295	235	195	215	260	525	585	*aantal*

Bron: CBS

registratiecode bijgehouden worden. Daarna is binnen het CBS ook een onderzoek gedaan om met behulp van machine-learning een tekstanalyse op de registraties uit te voeren zodat we ook aangiftes kunnen achterhalen die niet met een eigen registratiecode ingevoerd zijn, maar waarbij wel cybercrime de grondslag van de aangifte is.

4.1.2 Aantal geregistreerde computervredebreuken per jaar per 100 duizend inwoners



Bron: CBS

Aantal geregistreerde aangiftes van computervredebreuk blijft constant

De bij de politie geregistreerde computervredebreuk wordt in tabel 4.1.1 samengevat. Figuur 4.1.2 licht van deze tabel het aantal geregistreerde hackincidenten (computervredebreukincidenten) gerelateerd aan de bevolking uit. In 2019 zijn 28 hackincidenten per 100 duizend inwoners geregistreerd. In de publicatie van vorig jaar meldden we dat uit het DVC-rapport (CBS, 2018h) volgde dat er bij 50 hackincidenten per 100 duizend inwoners bij de politie een opgave gedaan is. Alhoewel deze cijfers niet helemaal overeenkomen, kan je toch stellen dat de orde van grootte van beide cijfers gelijk is. Dat het aantal incidenten dat uit een persoonsenquête volgt hoger ligt dan het cijfer zoals bij de politie in het systeem wordt verwerkt, is niet heel vreemd. Zo kan het zijn dat niet bij alle aangiftes de registratiecode voor hacken is meegegeven, zodat een aantal aangiftes wordt gemist. Daarnaast is het natuurlijk ook goed mogelijk dat er in de persoonsenquête ten onrechte ingevuld is dat er aangifte is gedaan, terwijl het in werkelijkheid slechts om een registratie ging. Verder geldt dat ook altijd rekening gehouden moet worden met foutenmarges. Hierdoor lijken de cijfers toch goed overeen te komen.

Cybercrime achterhalen in aangiften

Naast de hierboven genoemde categorieën, komen ook in andere delictstypen cybercrime-aspecten voor. Het CBS heeft tekstanalyse toegepast bij het onderzoeken van processen-verbaal uit 2016 om te achterhalen bij welke geregistreerde misdrijven cybercrime een rol speelt (CBS, 2018f). Daarbij is cybercrime tweeledig gedefinieerd: zowel misdrijven gepleegd met een ICT-middel en gericht op ICT (voorheen cybercrime in enge zin) als klassieke

misdrijven via een ICT-middel gepleegd (gedigitaliseerde criminaliteit) vallen hieronder. Ook als het cybercrime-aspect niet het zwaarste feit in het misdrijf is, wordt het meegenomen.

In 2016 bleek in ruim 72 duizend processen-verbaal sprake van cybercrime. Dat komt bij ongeveer 820 duizend onderzochte processen-verbaal neer op bijna 9 procent. Het aandeel cybercrime verschilt sterk per type delict. Zo kunnen in de categorie bedrog - waaronder oplichting valt - bijna alle geanalyseerde processen-verbaal als cybercrime geclassificeerd worden. Bij verkeersmisdrijven is het percentage cybercrime vrijwel nihil.

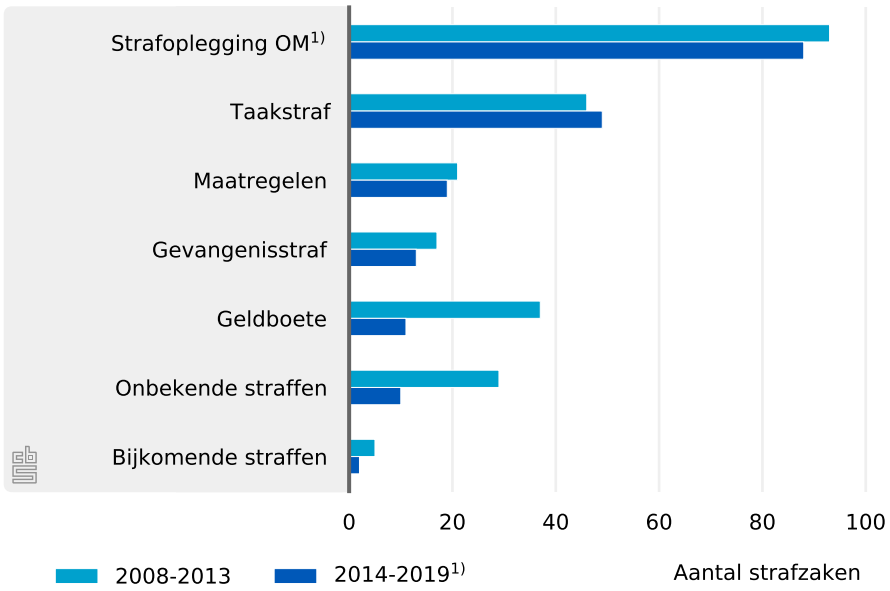
Uit de tekstanalyse blijkt dat in 2,5 procent van alle gevonden cybercrime in 2016 het gaat om misdrijven die bij de politie geregistreerd staan als computercriminaliteit. Meer dan de helft valt onder de categorie bedrog. Twee van de tien cybercrimedelicten vallen onder de categorie valsheidsmisdrijven.

Opgelegde sancties

In figuur 4.1.3 is weergegeven welke sancties het Openbaar Ministerie en de rechter hebben opgelegd aan verdachten van computervredebreuk. In een deel van de gevallen deelt het Openbaar Ministerie zonder tussenkomst van de rechter een strafbeschikking uit, biedt een transactie aan of besluit tot het seponeren van de zaak onder een bepaalde voorwaarde. Vaak bestaan strafbeschikkingen of transacties uit een taakstraf of een geldboete of schadevergoeding. Een deel van de zaken stuurt het Openbaar Ministerie door naar de rechter waarna de rechter een straf of maatregel op kan leggen. We kunnen in tabel 4.1.4 aflezen dat het OM in de periodes 2008–2013 en 2014–2019 respectievelijk 18 en 16 procent van de zaken zelf afdeed met een transactie, strafbeschikking of voorwaardelijk beleidssepot. Het totaal aantal computervredebreukzaken is bovendien van 512 naar 551 toegenomen.

De percentages van de soorten door de rechter opgelegde straffen en maatregelen per periode worden in figuur 4.1.5 gegeven. Het totaal door de rechter afgehandelde strafzaken was 124 voor de periode 2008–2013 en 82 voor de periode 2014–2019. In de periode 2014–2018 bestonden de opgelegde straffen voor het grootste gedeelte uit taakstraffen (37 procent). Het aandeel taakstraffen en gevangenisstraffen is gegroeid van respectievelijk 37 en 14 procent in de periode 2008–2013 naar 60 en 16 procent in de periode 2014–2018. Het aandeel door de rechter opgelegde geldboetes is gedaald van 30 naar 13 procent.

4.1.3 Door Openbaar Ministerie en rechter opgelegde straffen en maatregelen voor computervredebreuk



Bron: CBS

1) Door het OM afgedaan met transactie, strafbeschikking of voorwaardelijk beleidssepot. Alle overige straffen in deze figuur zijn door de rechter opgelegd.

4.1.4 Aantal computervredebreuk zaken afgehandeld door de rechter of het OM

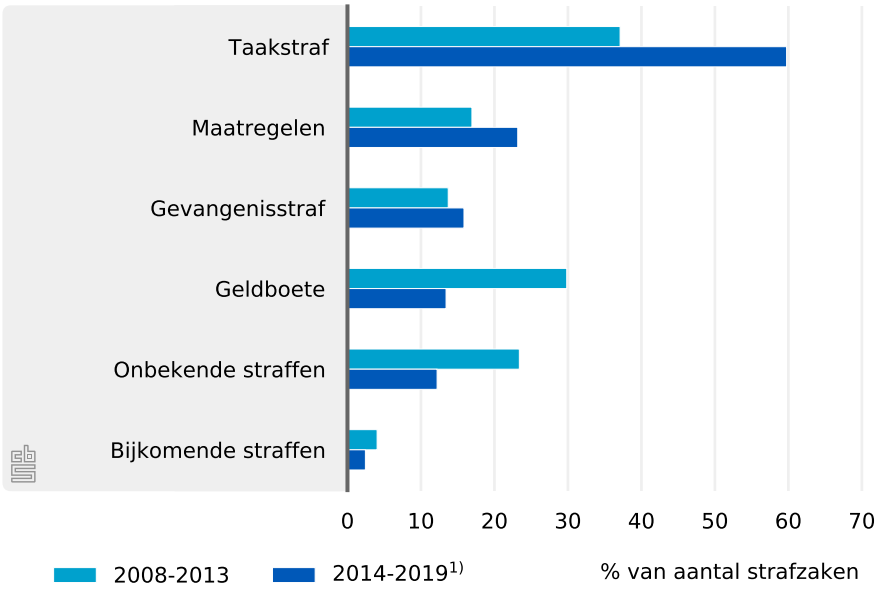
	2008–2013	2014–2019 1)
Totaal door OM genomen beslissingen	512	551
– waaronder strafoplegging OM2)	93	88
Schuldig verklaard door rechter	124	82

Bron: CBS

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

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

4.1.5 Door de rechter opgelegde straffen en maatregelen voor computervredebreuk als percentage van het totaal aantal computervredebreukstrafzaken[1)]



Bron: CBS

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

Bijlagen

Bijlage A

Tabellen

A.1 Definities

A.1 Overzicht van de bedrijfsgroottes

Code	Bedrijfsgrootte
Totaal	2 of meer werkzame personen
2–250	2 tot 250 werkzame personen
2	2 werkzame personen
3–5	3 tot 5 werkzame personen
5–10	5 tot 10 werkzame personen
10–20	10 tot 20 werkzame personen
20–50	20 tot 50 werkzame personen
50–100	50 tot 100 werkzame personen
100–250	100 tot 250 werkzame personen
250–500	250 tot 500 werkzame personen
500+	500 of meer werkzame personen

A.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.1 1) Gebruikte ICT-maatregelen voor alle grootteklassen als percentage van het aantal bedrijven, 2016 - 2019

Maatregel	Bedrijfsgrootte	2016	2017	2018	2019
Anti-virussoftware	Totaal	87	87	89	89
	2 tot 10 werkzame personen	86	85	87	87
	10 tot 50 werkzame personen	93	95	96	92
	50 tot 250 werkzame personen	97	98	98	97
	250 of meer werkzame personen	98	99	99	99
	2 tot 250 werkzame personen	87	87	89	89
Authenticatie via soft- of hardwaretoken	Totaal	26	31	39	45
	2 tot 10 werkzame personen	23	28	35	42
	10 tot 50 werkzame personen	29	38	49	54
	50 tot 250 werkzame personen	49	56	62	68
	250 of meer werkzame personen	71	77	81	87
	2 tot 250 werkzame personen	25	31	39	45
Beleid voor sterke wachtwoorden	Totaal	57	62	65	68
	2 tot 10 werkzame personen	55	60	63	65
	10 tot 50 werkzame personen	64	71	74	74
	50 tot 250 werkzame personen	81	85	86	88
	250 of meer werkzame personen	93	95	94	96
	2 tot 250 werkzame personen	57	62	65	68
Encryptie van data	Totaal	.	.	37	38
	2 tot 10 werkzame personen	.	.	33	35
	10 tot 50 werkzame personen	.	.	44	44
	50 tot 250 werkzame personen	.	.	62	64
	250 of meer werkzame personen	.	.	81	83
	2 tot 250 werkzame personen	.	.	36	38
Gegevens op andere fysieke locatie	Totaal	71	68	72	71
	2 tot 10 werkzame personen	68	64	68	68
	10 tot 50 werkzame personen	80	82	85	82
	50 tot 250 werkzame personen	90	91	93	91
	250 of meer werkzame personen	94	93	97	95
	2 tot 250 werkzame personen	70	68	72	71
ICT-cursus aan ICT-specialisten	Totaal	.	6	.	6
	2 tot 10 werkzame personen	.	3	.	3
	10 tot 50 werkzame personen	.	11	.	9
	50 tot 250 werkzame personen	.	34	.	34
	250 of meer werkzame personen	.	67	.	68
	2 tot 250 werkzame personen	.	5	.	5
Logbestanden voor analyse incidenten	Totaal	31	34	39	37
	2 tot 10 werkzame personen	25	27	32	31
	10 tot 50 werkzame personen	49	55	59	55
	50 tot 250 werkzame personen	76	79	82	79
	250 of meer werkzame personen	88	89	91	91
	2 tot 250 werkzame personen	30	33	38	37
Methodes voor beoordelen ICT-veiligheid	Totaal	22	25	31	28
	2 tot 10 werkzame personen	17	20	26	22
	10 tot 50 werkzame personen	35	40	48	41
	50 tot 250 werkzame personen	56	61	67	63
	250 of meer werkzame personen	72	76	80	80
	2 tot 250 werkzame personen	21	25	31	27

Vervolg op volgende pagina…

A.1 2) Gebruikte ICT-maatregelen voor alle grootteklassen als percentage van het aantal bedrijven, 2016 - 2019

…vervolg van vorige pagina

Maatregel	Bedrijfsgrootte	2016	2017	2018	2019
Network access control	Totaal	31	34	37	37
	2 tot 10 werkzame personen	28	30	32	32
	10 tot 50 werkzame personen	43	47	50	48
	50 tot 250 werkzame personen	60	60	63	64
	250 of meer werkzame personen	67	69	71	72
	2 tot 250 werkzame personen	31	33	36	36
Risicoanalyses	Totaal	22	25	31	29
	2 tot 10 werkzame personen	17	20	26	24
	10 tot 50 werkzame personen	34	41	47	42
	50 tot 250 werkzame personen	59	64	64	63
	250 of meer werkzame personen	75	77	80	80
	2 tot 250 werkzame personen	21	25	31	28
Bijwerken software/besturingssysteem	Totaal	.	.	81	84
	2 tot 10 werkzame personen	.	.	78	81
	10 tot 50 werkzame personen	.	.	92	90
	50 tot 250 werkzame personen	.	.	97	96
	250 of meer werkzame personen	.	.	98	98
	2 tot 250 werkzame personen	.	.	81	83
VPN-internetgebruik buiten het bedrijf	Totaal	29	32	35	35
	2 tot 10 werkzame personen	23	26	29	29
	10 tot 50 werkzame personen	48	50	54	52
	50 tot 250 werkzame personen	74	75	77	78
	250 of meer werkzame personen	85	87	86	86
	2 tot 250 werkzame personen	28	32	35	35

A.2 1) Gebruikte ICT-maatregelen voor alle bedrijfstakken als percentage van het aantal bedrijven, 2016 - 2019

Maatregel	Bedrijfstak	2016	2017	2018	2019
Anti-virussoftware	Industrie	93	92	94	91
	ICT-sector	90	93	91	90
	Bouwnijverheid	85	86	85	89
	Handel	88	87	91	89
	Vervoer en opslag	84	86	87	87
	Horeca	76	72	75	76
	Informatie en communicatie	87	91	89	90
	Financiële dienstverlening	88	94	97	92
	Verhuur en handel van onroerend goed	80	83	84	82
	Specialistische zakelijke diensten	90	92	93	92
	Verhuur en overige zakelijke diensten	83	87	88	90
	Gezondheids- en welzijnszorg	97	93	97	96
	Energie, water, afvalbeheer	91	84	92	89
Authenticatie via soft- of hardwaretoken	Industrie	24	30	39	43
	ICT-sector	49	54	57	63
	Bouwnijverheid	17	25	31	33
	Handel	21	27	36	43
	Vervoer en opslag	22	26	33	44
	Horeca	16	17	20	29
	Informatie en communicatie	47	51	55	60
	Financiële dienstverlening	45	55	62	64
	Verhuur en handel van onroerend goed	28	32	34	39
	Specialistische zakelijke diensten	31	36	47	52
	Verhuur en overige zakelijke diensten	20	31	39	48
	Gezondheids- en welzijnszorg	47	50	59	67
	Energie, water, afvalbeheer	34	36	43	47
Beleid voor sterke wachtwoorden	Industrie	58	64	65	67
	ICT-sector	80	84	86	84
	Bouwnijverheid	50	55	54	64
	Handel	57	60	66	67
	Vervoer en opslag	56	57	62	65
	Horeca	38	50	47	53
	Informatie en communicatie	77	80	85	82
	Financiële dienstverlening	74	83	81	80
	Verhuur en handel van onroerend goed	51	56	67	59
	Specialistische zakelijke diensten	67	71	71	73
	Verhuur en overige zakelijke diensten	56	63	67	67
	Gezondheids- en welzijnszorg	66	72	77	80
	Energie, water, afvalbeheer	67	60	68	71

Vervolg op volgende pagina…

A.2 2) Gebruikte ICT-maatregelen voor alle bedrijfstakken als percentage van het aantal bedrijven, 2016 - 2019

…vervolg van vorige pagina

Maatregel	Bedrijfstak	2016	2017	2018	2019
Encryptie van data	Industrie	.	.	32	35
	ICT-sector	.	.	67	67
	Bouwnijverheid	.	.	27	23
	Handel	.	.	32	33
	Vervoer en opslag	.	.	26	30
	Horeca	.	.	18	22
	Informatie en communicatie	.	.	66	64
	Financiële dienstverlening	.	.	56	56
	Verhuur en handel van onroerend goed	.	.	26	37
	Specialistische zakelijke diensten	.	.	44	46
	Verhuur en overige zakelijke diensten	.	.	34	39
	Gezondheids- en welzijnszorg	.	.	67	67
	Energie, water, afvalbeheer	.	.	38	38
Gegevens op andere fysieke locatie	Industrie	77	75	78	78
	ICT-sector	89	85	92	84
	Bouwnijverheid	64	63	66	66
	Handel	66	64	71	72
	Vervoer en opslag	61	64	63	65
	Horeca	52	43	46	43
	Informatie en communicatie	87	84	89	84
	Financiële dienstverlening	75	85	85	76
	Verhuur en handel van onroerend goed	69	68	69	64
	Specialistische zakelijke diensten	83	81	85	80
	Verhuur en overige zakelijke diensten	70	66	69	70
	Gezondheids- en welzijnszorg	84	82	87	86
	Energie, water, afvalbeheer	78	76	74	70
ICT-cursus aan ICT-specialisten	Industrie	.	6	.	7
	ICT-sector	.	38	.	42
	Bouwnijverheid	.	2	.	2
	Handel	.	4	.	5
	Vervoer en opslag	.	4	.	3
	Horeca	.	1	.	1
	Informatie en communicatie	.	36	.	38
	Financiële dienstverlening	.	15	.	13
	Verhuur en handel van onroerend goed	.	3	.	3
	Specialistische zakelijke diensten	.	6	.	6
	Verhuur en overige zakelijke diensten	.	5	.	4
	Gezondheids- en welzijnszorg	.	3	.	4
	Energie, water, afvalbeheer	.	10	.	11

Vervolg op volgende pagina…

A.2 3) Gebruikte ICT-maatregelen voor alle bedrijfstakken als percentage van het aantal bedrijven, 2016 - 2019

…vervolg van vorige pagina

Maatregel	Bedrijfstak	2016	2017	2018	2019
Logbestanden voor analyse incidenten	Industrie	36	40	45	42
	ICT-sector	64	64	72	65
	Bouwnijverheid	20	23	30	29
	Handel	29	32	37	35
	Vervoer en opslag	26	30	35	31
	Horeca	13	15	16	15
	Informatie en communicatie	60	60	67	63
	Financiële dienstverlening	50	58	61	59
	Verhuur en handel van onroerend goed	31	27	28	33
	Specialistische zakelijke diensten	39	41	48	44
	Verhuur en overige zakelijke diensten	29	33	36	34
	Gezondheids- en welzijnszorg	39	43	49	52
	Energie, water, afvalbeheer	48	44	54	51
Methodes voor beoordelen ICT-veiligheid	Industrie	27	31	35	32
	ICT-sector	37	44	47	44
	Bouwnijverheid	16	20	30	22
	Handel	19	22	30	27
	Vervoer en opslag	18	20	27	23
	Horeca	8	11	13	12
	Informatie en communicatie	35	44	46	43
	Financiële dienstverlening	41	50	61	55
	Verhuur en handel van onroerend goed	25	25	31	28
	Specialistische zakelijke diensten	28	30	37	30
	Verhuur en overige zakelijke diensten	21	27	30	27
	Gezondheids- en welzijnszorg	29	34	39	38
	Energie, water, afvalbeheer	36	36	47	35
Network access control	Industrie	35	39	40	40
	ICT-sector	54	55	55	53
	Bouwnijverheid	20	27	34	31
	Handel	29	33	36	37
	Vervoer en opslag	23	31	30	30
	Horeca	17	14	19	20
	Informatie en communicatie	51	51	53	51
	Financiële dienstverlening	48	54	59	55
	Verhuur en handel van onroerend goed	36	28	28	33
	Specialistische zakelijke diensten	38	38	42	41
	Verhuur en overige zakelijke diensten	29	33	35	34
	Gezondheids- en welzijnszorg	46	48	47	48
	Energie, water, afvalbeheer	37	40	43	51

Vervolg op volgende pagina…

A.2 4) Gebruikte ICT-maatregelen voor alle bedrijfstakken als percentage van het aantal bedrijven, 2016 - 2019

…vervolg van vorige pagina

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

A.3 Incidenten

A.1 Incidenten en kosten per grootteklasse als percentage van het aantal bedrijven, 2019

	Uitval ICT-dienst door veiligheidsinc.	Uitval ICT-dienst door aanval buitenaf	Dataverniet iging door veiligheidsinc.	Dataverniet iging door aanval van buitenaf	Dataonthulling door ICT-inbraak	Dataonthulling door intern incident
Totaal	27	5	4	2	2	2
Bedrijfsgrootte						
2 tot 250 werkzame personen	27	5	4	2	2	2
2 werkzame personen	18	3	3	2	2	1
3 tot 5 werkzame personen	26	5	4	2	1	2
5 tot 10 werkzame personen	32	6	3	2	1	2
10 tot 20 werkzame personen	35	7	4	3	2	3
20 tot 50 werkzame personen	42	7	5	3	2	5
50 tot 100 werkzame personen	49	7	5	4	3	6
100 tot 250 werkzame personen	51	8	6	3	4	11
250 tot 500 werkzame personen	54	10	8	5	6	17
500 of meer werkzame personen	57	13	8	5	10	32

Bron: CBS (2020e)

A.2 Incidenten per bedrijfstak als percentage van het aantal bedrijven, 2019

	Uitval ICT-dienst door veiligheidsinc.	Uitval ICT-dienst door aanval buitenaf	Dataverniet iging door veiligheidsinc.	Dataverniet iging; aanval van buitenaf	Dataonthulling door ICT-inbraak	Dataonthulling door intern incident
Totaal C-N en Q	40	7	5	3	3	5
Bedrijfstak						
Voedings-, genotm.industrie	39	7	6	5	2	4
Textiel-, kleding-, lederindustrie	45	5	7	0	1	3
Hout-, papier-, grafische industr.	46	8	3	5	1	1
Raffinaderijen en chemie	50	5	6	3	7	4
Kunststof- en bouwmateriaalind.	50	5	7	3	2	3
Basismetaal, metaalprod.-ind.	37	9	6	7	1	2
Elektrische en elektron. Ind.	53	7	5	2	3	3
Machine-industrie	47	5	7	6	3	4
Transportmiddelenindustrie	50	13	9	9	6	7
Overige industrie en reparatie	43	7	6	4	2	5
Energie, water, afvalbeheer	45	8	6	1	2	4
B&U en wegenbouw	39	6	10	3	5	3
Vervoer en opslag	36	9	4	2	2	3
Logiesverstrekking	40	10	4	6	4	3
Eet- en drinkgelegenheden	24	3	2	0	1	1
Uitgeverijen, film,radio en t.v.	48	14	11	7	6	8
Telecommunicatie	69	13	4	4	6	7
IT- en informatiedienstverlening	40	11	6	3	3	8
Banken	35	11	9	4	4	8
Verzekeringen	55	5	3	0	9	28
Financiële advisering	41	11	2	2	4	13
Verhuur/handel onroerend goed	46	5	9	4	4	18
Juridisch en managementadvies	52	8	4	2	4	11
Architecten-, ingenieursbureaus	44	6	5	2	3	4
Research	43	7	7	4	4	6
Reclamewezen/marktonderzoek	36	9	5	4	4	3
Uitzendbureaus en arb.bemidd.	34	5	3	3	2	4
Reisbureaus, reisorganisaties	54	12	10	13	9	5
Gezondheidszorg	48	7	4	1	2	12
Verzorging en welzijn	40	5	6	3	3	15
Management- en technisch advies	49	7	5	2	3	9
Reclame, design, overige dnst.	39	8	4	3	3	4
ICT-sector	41	9	6	3	3	7

Bron: CBS (2020a)

Bibliografie

Autoriteit Persoonsgegevens (2019a). Datalekregistraties.

Autoriteit Persoonsgegevens (2019b). Datalekregistraties.

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). Cybercrime achterhalen in aangiften.

CBS (2018g). Cybersecuritymonitor 2018.

CBS (2018h). Digitale veiligheid en criminaliteit 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). CBS StatLine.

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

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

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

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

CBS (2021). Statistisch onderzoek naar veiligheid websites bedrijven in nederland (verwacht in juni 2021).

NBIP (2018). Statistics.

NBIP (2020). DDoS data report 2020.

Platform Internetstandaarden (2021). Internet.nl.

SIDN (2020). SIDN Labs: .nl stats en data.

Uitgave 2021