Cybersecuritymonitor

2019

Cybersecuritymonitor

2019

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
2018–2019	2018 tot en met 2019
2018/2019	Het gemiddelde over de jaren 2018 tot en met 2019
2018/’19	Oogstjaar, boekjaar, schooljaar enz., beginnend in 2018 en eindigend in 2019
2016/’17–2018/’19	Oogstjaar, boekjaar, enz., 2016/’17 tot en met 2018/’19

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 derde 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 aan de hand van met name 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, 2017a) en (CBS, 2018g).

De structuur van de monitor is wederom opgezet volgens dezelfde lijnen als de afgelopen twee 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 ten gevolge van kwaadwillenden wordt ook wel aangeduid als cybercrime. Voor een uitgebreidere toelichting verwijzen we naar de voorgaande Cybersecuritymonitors (CBS, 2017a; CBS, 2018g).

In dit rapport worden in hoofdstuk 2 de cybersecuritymaatregelen besproken. We splitsen dit hoofdstuk op in de maatregelen die door bedrijven en de maatregelen die door personen worden genomen. 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, dat wil zeggen de cybersecurityincidenten door kwaadwillenden die ook daadwerkelijk slachtoffers gemaakt hebben.

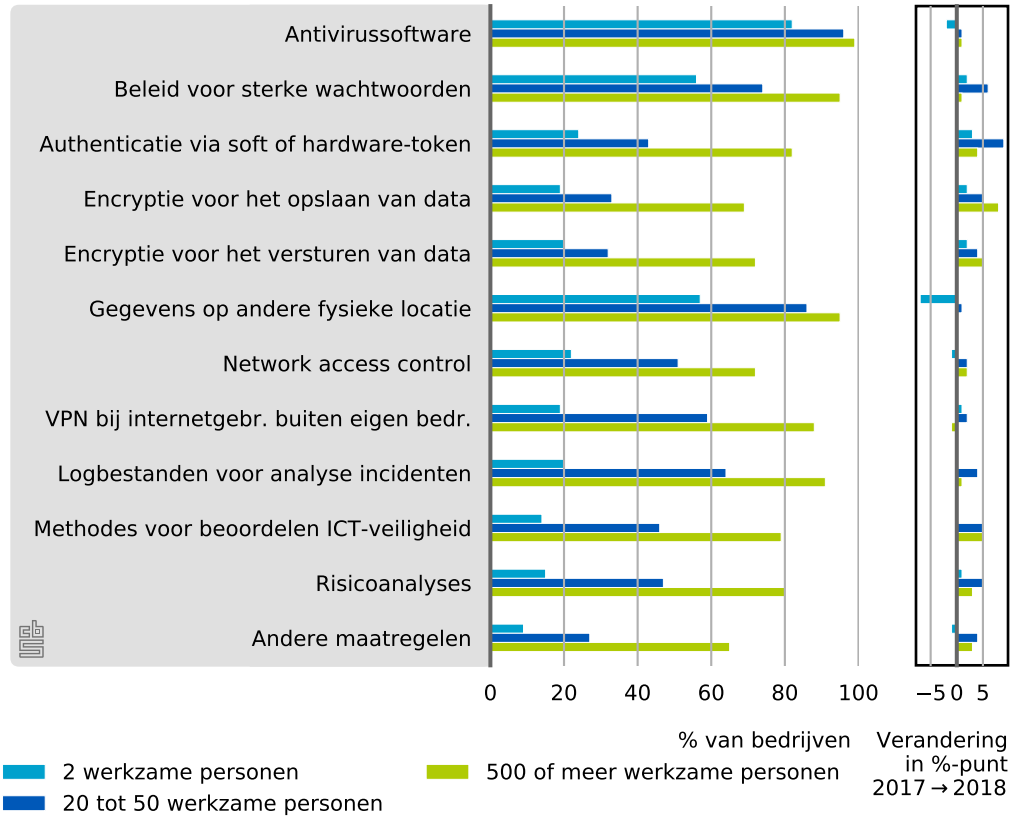
2. Cybersecurity-maatregelen

2.1 Bedrijven

In deze sectie gaan we in op de maatregelen die bedrijven in Nederland nemen om zichzelf meer cyberweerbaar te maken. We gebruiken hier met name de cijfers uit de CBS enquête 'ICT-gebruik bedrijven 2018' (CBS, 2018a; CBS, 2018b; CBS, 2018c; CBS, 2018d; CBS, 2018e). Zoals de naam al aangeeft, besteedt deze jaarlijkse ICT-enquête aandacht aan het ICT-gebruik van bedrijven. Dit levert ook cijfers op die samenhangen met de cybersecurity van bedrijven. We kunnen hierin onderscheid maken tussen de maatregelen die door bedrijven worden genomen om het bedrijf te beveiligen tegen aanvallen van buitenaf aan de ene kant en de ICT-veiligheidsincidenten aan de andere kant. De maatregelen worden in dit hoofdstuk beschreven, terwijl de incidenten in het volgende hoofdstuk aan bod komen.

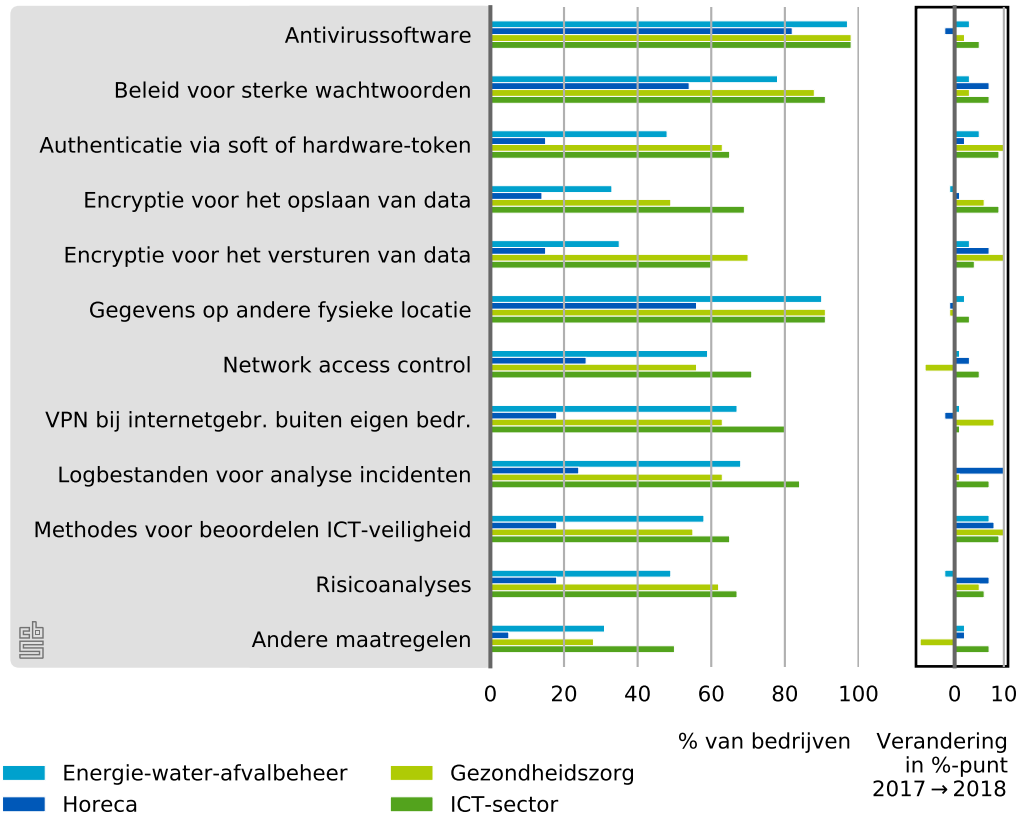
De ICT-enquête wordt gehouden onder ongeveer 12 duizend aselect getrokken Nederlandse bedrijven van verschillende bedrijfsgrootteklasses en bedrijfscategorieën. In de Appendix wordt in tabellen A.1 en A.2 een overzicht van respectievelijk alle grootteklassen en bedrijfstakken gegeven. In dit hoofdstuk worden alleen de cijfers van een selectie van de grootteklassen uitgelicht: de kleine (2 werkzame personen), medium (20 tot 50 werkzame personen) en grote (500 of meer werkzame personen) bedrijven. Daarnaast laten we alleen 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, 2019 gevonden worden en een deel wordt in Appendix A weergegeven.

2.1.1 Genomen cybersecuritymaatregelen per bedrijfsgrootteklasse, 2018



Bron: CBS, 2018a

2.1.2 Genomen cybersecuritymaatregelen per bedrijfstak, 2018



Bron: CBS, 2018b

Maatregelen ter verhoging van de cyberweerbaarheid

Voor bedrijven zijn vier indicatoren opgenomen die iets zeggen over de cybersecurity van deze bedrijven. Ten eerste is aan bedrijven gevraagd welke ICT-veiligheidsmaatregelen ze hebben getroffen. Twee andere indicatoren gaan over de organisatie van de ICT- beveiliging van bedrijven. Hoeveel bedrijven maken daadwerkelijk werk van ICT- beveiliging en de bescherming van data bijvoorbeeld in de vorm van beveiligingstests en het gebruik van beveiligingssoftware? Daaraan gekoppeld is de vraag door wie deze werkzaamheden in overwegende mate worden uitgevoerd. Zijn kleinere bedrijven in staat dit zelf te doen of besteden ze dit toch vooral uit? Daarnaast is aan bedrijven gevraagd naar hun beleid in zake het uitvoeren van software-updates (security-patches). De vierde indicator betreft het gebruik van betaalde clouddiensten door bedrijven en met name de vraag of hier een aparte server voor wordt gebruikt of een server die ook gebruikt wordt door andere bedrijven, instellingen of personen. Het gebruik van een server die uitsluitend gereserveerd is voor het betreffende bedrijf is immers veiliger.

Eerst bekijken we hoe vaak verschillende cybersecuritymaatregelen door bedrijven toegepast worden. In figuren 2.1.1 en 2.1.2 wordt voor verschillende bedrijfsgrootteklasses en bedrijfstakken voor twaalf maatregelen het percentage getoond van bedrijven dat een maatregel toepast.[1)] In beide figuren wordt aan de rechterzijde de verandering van dit

1) We lichten voor de duidelijkheid slechts drie bedrijfsgrootteklasse en vier bedrijfstakken uit; het volledige overzicht

percentage in procentpunten ten opzichte van 2017 weergegeven. Dit laatste stelt ons in staat een indruk te krijgen van de ontwikkeling van de cyberweerbaarheid van bedrijven. Uiteraard kan met deze twaalf maatregelen nooit een compleet beeld van het beveiligingsniveau van bedrijven gegeven worden, maar er ontstaat wel een globale indruk.

Bedrijven nemen meer maatregelen tegen cyberdreigingen

In het algemeen kan je zeggen dat het ICT-beveiligingsniveau van een bedrijf hoger is naarmate er meer maatregelen tegelijkertijd genomen worden. In figuur 2.1.1 is duidelijk te zien dat voor alle maatregelen geldt dat grote bedrijven beter scoren dan kleine bedrijven. Deze trend is consistent voor alle bedrijfsgrootteklasses (zie tabel A.3 achterin de publicatie). Uiteraard hebben grotere bedrijven vaker een grotere en meer complexe ICT-infrastructuur en derhalve is een breder scala aan beveiligingsmaatregelen nodig om het bedrijf cybersecure te houden. Figuur 2.1.2 laat het aantal maatregelen voor een aantal bedrijfstakken zien. Deze voorbeelden laten zien dat bedrijven die meer met ICT bezig zijn (ICT-sector) of bedrijven die een groot belang hebben bij het cybersecure houden van hun data (Gezondheidszorg) beter scoren dan andere sectoren waar 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.

De verandering van het percentage bedrijven dat een maatregel toepast, wordt in procentpunten weergegeven aan de rechterzijde van figuren 2.1.1 en 2.1.2. We kunnen constateren dat over het algemeen meer maatregelen genomen worden. Het percentage van bedrijven dat een maatregel neemt is namelijk het afgelopen jaar tot wel 10 procentpunt toegenomen. Alleen het gebruik van anti-virussoftware blijft min of meer gelijk omdat deze maatregel al breed genomen wordt. Dit is ook niet gek als we bedenken dat anti-virussoftware tegenwoordig al standaard in Windows 10 is ingebouwd (Windows Defender).

Toename authenticatie met soft- of hardware-token

Interessanter is de constatering dat de middelgrote bedrijven (20 tot 50 werkzame personen) een behoorlijke inhaalslag gemaakt hebben met het invoeren van authenticatie via soft- of hardware-token. 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 wijze wordt inloggen een stuk veiliger, want zelfs als je wachtwoord onderschept wordt, zal je nog in bezit moeten komen van de extra gegeneerde code om in te kunnen loggen. Grote bedrijven (500 of meer werkzame personen) liepen met een dekking van 81 procent van de bedrijven al voorop met deze manier van inloggen, maar we kunnen zien dat middelgrote bedrijven een inhaalslag gemaakt hebben met een dekking die gestegen is van 34 procent in 2017 naar 43 procent in 2018; een stijging van 9 procentpunt oftewel 25 procent. Voor kleine bedrijven zien we een lichte stijging van het gebruik van soft- of hardware-tokens van 21 procent 2017 naar 24 procent in 2018, een stijging van 14 procent. Overigens bieden steeds meer websites de mogelijkheid tot het gebruik van two-factor authenticatie aan, dus we kunnen verwachten dat deze manier van inloggen steeds wijder gebruikt gaat worden.

kan in tabellen A.3 en A.4 of op StatLine (CBS, 2019) gevonden worden.

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.

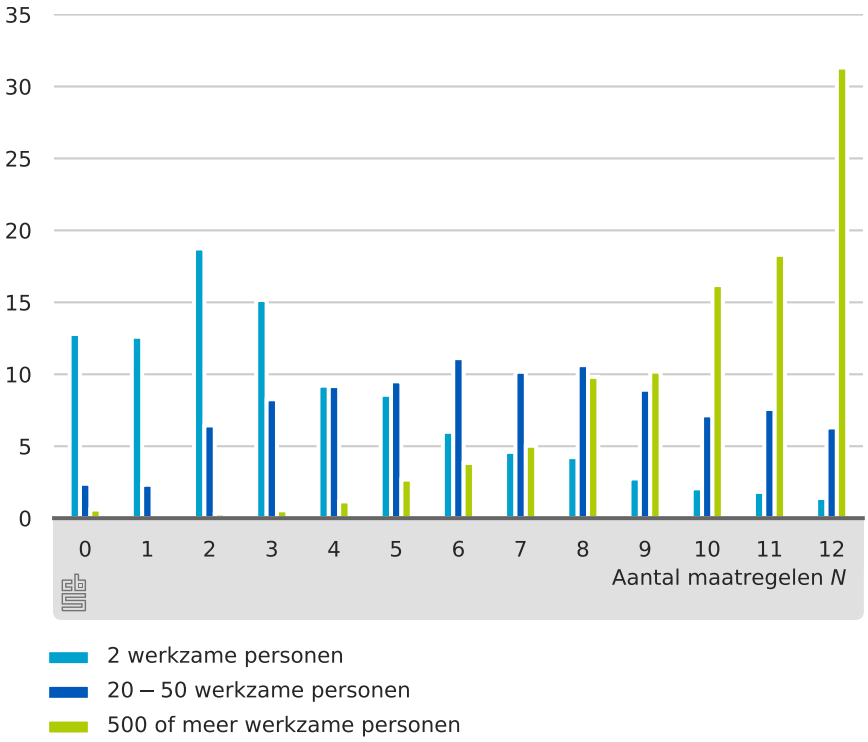
Data-encryptie

Een andere indicatie dat een bedrijf cybersecurity serieus neemt, is het gebruik van data-encryptie voor zowel het opslaan als het versturen van data. Voor deze maatregel zien we dat grote bedrijven de grootste toename van gebruik laten zien, van 61 procent in 2017 naar 69 procent in 2018 voor encryptie van opgeslagen data en van 67 procent naar 72 procent voor encryptie van verstuurde data. Toch laten middelgrote bedrijven ook een lichte toename van gebruik van data-encryptie zien, tot 5 procentpunt.

Grote bedrijven nemen meer maatregelen dan kleine

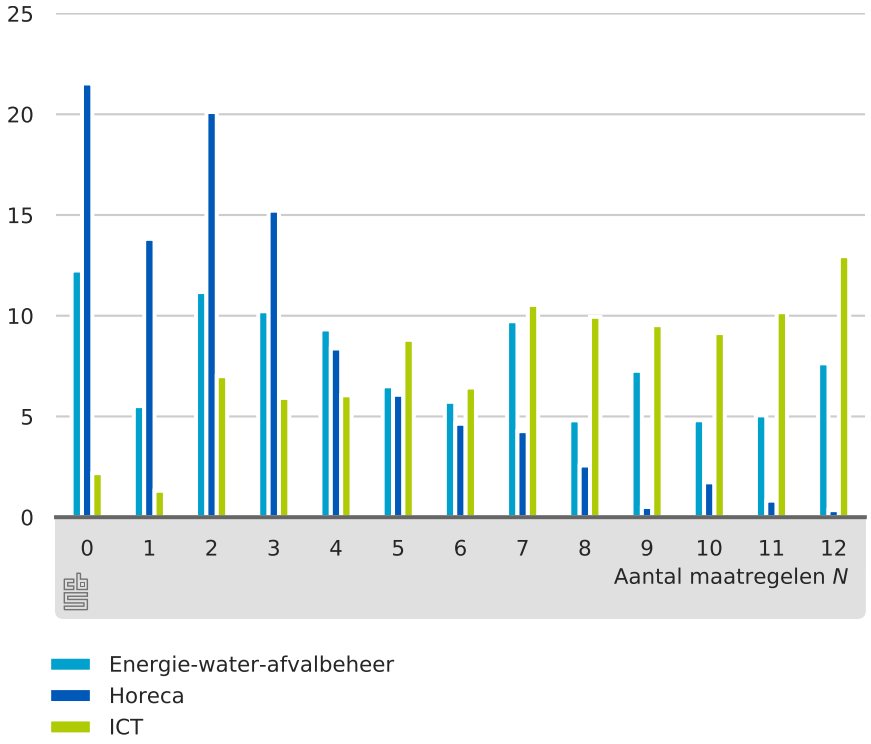
We hebben geconstateerd dat bijna alle cybersecuritymaatregelen vaker genomen worden. Dit kunnen we kwantificeren door het aantal cybersecuritymaatregelen N dat een bedrijf neemt te bekijken. In Figuren 2.1.3 en 2.1.4 wordt de verdeling van het aantal maatregelen (N) die bedrijven nemen, getoond per bedrijfsgrootteklasse en bedrijfstak. In figuur 2.1.3 is aan de verdeling per maatregel wederom duidelijk te zien dat grote bedrijven meer maatregelen nemen ten opzichte van kleine bedrijven. Voor kleine bedrijven is het percentage van bedrijven dat twee maatregelen neemt het grootst, bijna 19 procent. Kleine bedrijven die alle twaalf maatregelen nemen komen daarentegen niet veel voor: slechts 1,4 procent. Aan de andere kant neemt Ruim 30 procent van de grote bedrijven alle twaalf gevraagde maatregelen . Daarnaast zien we in figuur 2.1.4 weer dat het aantal maatregelen ook afhangt van de bedrijfstak: ICT-bedrijven scoren bijvoorbeeld beter dan horecabedrijven.

2.1.3 Verdeling van het aantal cybersecuritymaatregelen N per bedrijfsgrootteklasse, 2018



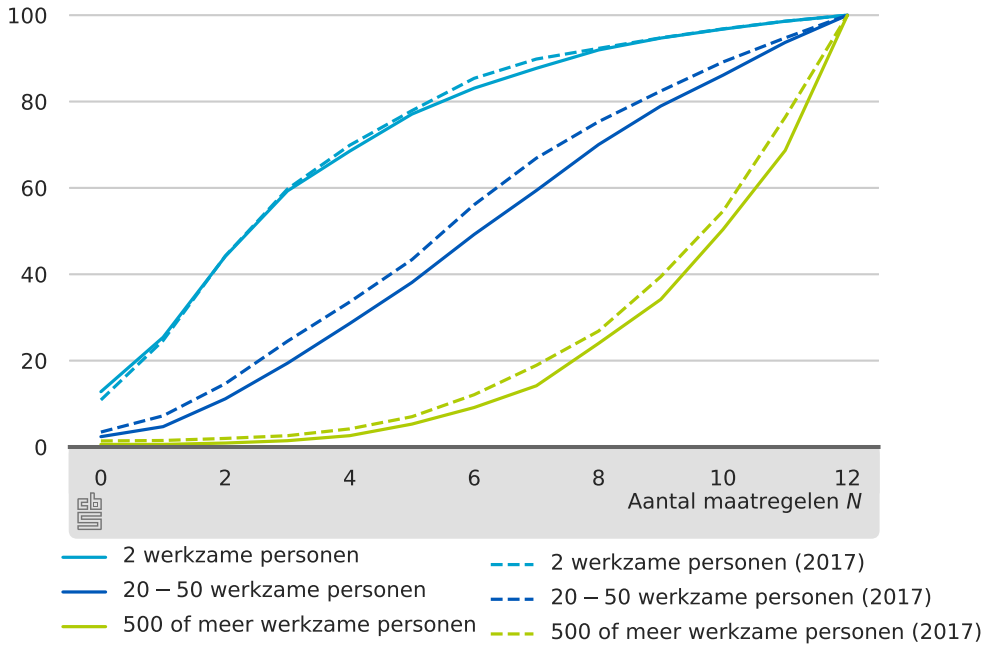
Bron: CBS, 2018a

2.1.4 Verdeling van het aantal cybersecuritymaatregelen *N* per bedrijfstak, 2018



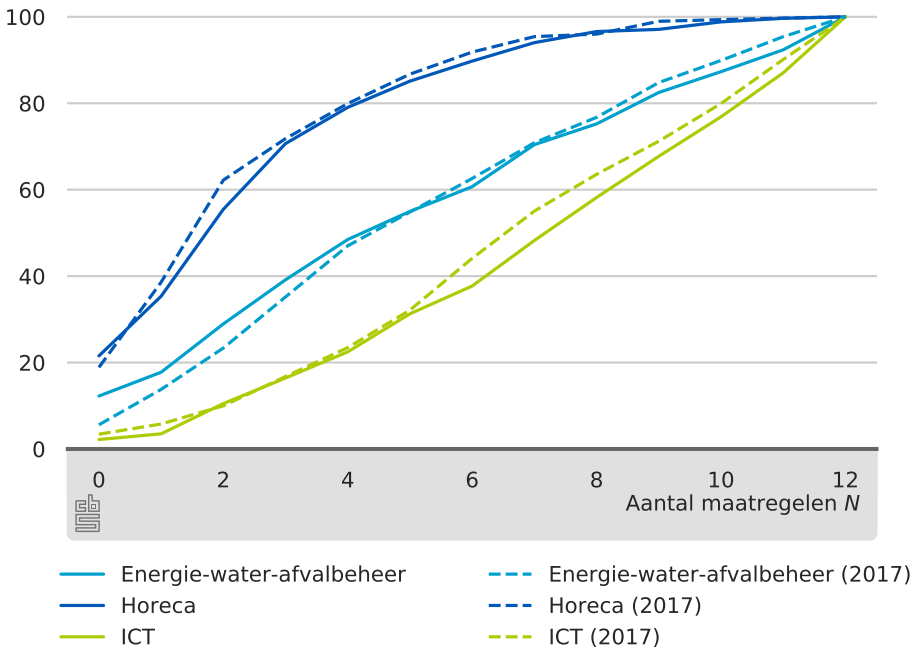
Bron: CBS, 2018b

2.1.5 Cumulatieve verdeling van het aantal cybersecuritymaatregelen *N* per bedrijfsgrootteklasse, 2018



Bron: CBS, 2018a

2.1.6 Cumulatieve verdeling van het aantal cybersecuritymaatregelen N per bedrijfstak, 2018



Bron: CBS, 2018b

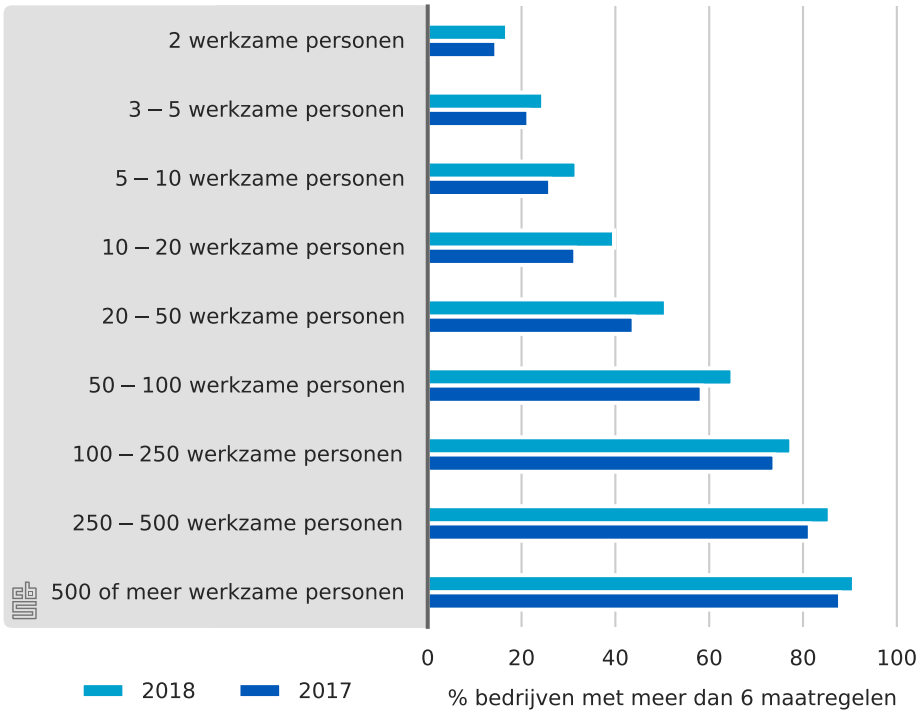
Een kwart van de bedrijven neemt meer dan zes maatregelen

We kunnen ook naar de cumulatieve verdeling kijken, zoals we voor verschillende bedrijfsgrootteklasses en bedrijfstakken in respectievelijk figuren 2.1.5 en 2.1.6 laten zien. Deze grafieken geven het percentage bedrijven dat N of minder maatregelen neemt.[3)] Op deze manier kunnen we bijvoorbeeld direct aflezen dat 9 procent van de grote bedrijven zes maatregelen of minder neemt, wat impliceert dat 91 procent van de grote bedrijven meer dan zes maatregelen neemt. Bij kleine bedrijven is het beeld precies andersom: we lezen af dat 83 procent van de kleine bedrijven zes of minder maatregelen neemt, wat inhoudt dat slechts 17 procent van de kleine bedrijven meer dan zes maatregelen neemt. Overigens kan je je natuurlijk afvragen of het zinnig is voor kleine bedrijven om al deze twaalf maatregelen te nemen: een maatregel als bijvoorbeeld data-encryptie hoeft voor een klein bedrijf niet per se van meerwaarde zijn om het cybersecurityniveau te verhogen.

Als we de getallen per bedrijfsklasse bekijken in figuur 2.1.6 dan zien de dat de bedrijven uit de ICT-branche de meeste cybersecuritymaatregelen nemen: 38 procent van de ICT-bedrijven neemt zes of minder maatregelen, waaruit volgt dat dus 62 procent meer dan zes maatregelen neemt. Als hekkensluiter vinden we de Horeca, waar 90 procent zes of minder maatregelen neemt en dus neemt slechts 10 procent van de horeca meer dan zes cybersecuritymaatregelen. Een volledig overzicht voor de andere bedrijfsklassen en bedrijfsgroottes is te vinden in tabellen A.5, A.6, A.7 en A.8.

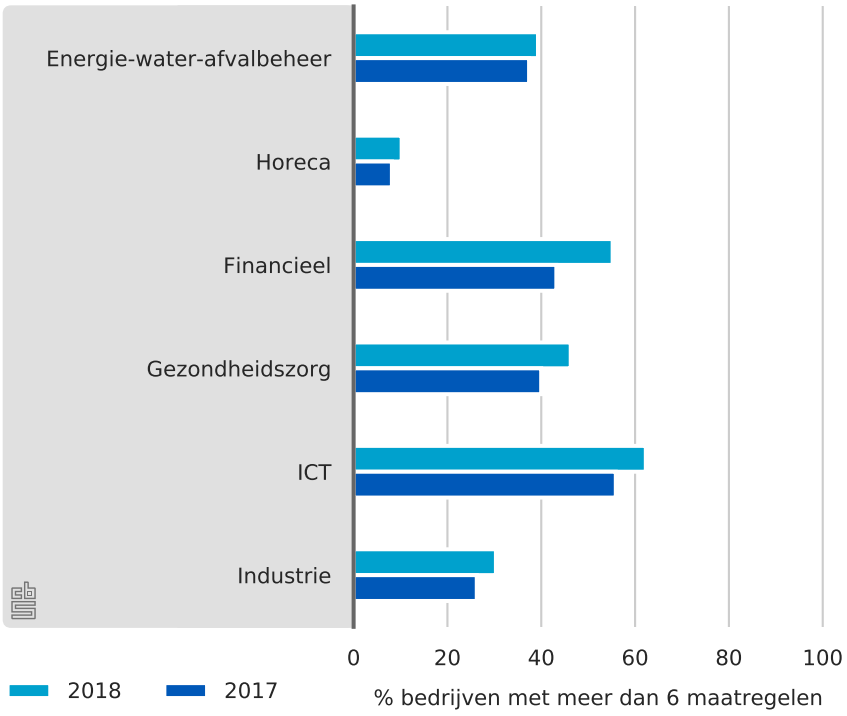
3) De cumulatieve verdeling volgt uit de gewone verdeling door alle voorgaande staafjes bij de staaf van N op te tellen.

2.1.7 Percentage van bedrijven per bedrijfsgrootteklasse dat meer dan 6 van de 12 gevraagde cybersecuritymaatregelen genomen heeft, 2018



Bron: CBS, 2018a

2.1.8 Percentage van bedrijven per bedrijfstak dat meer dan 6 van de 12 gevraagde cybersecuritymaatregelen genomen heeft, 2018

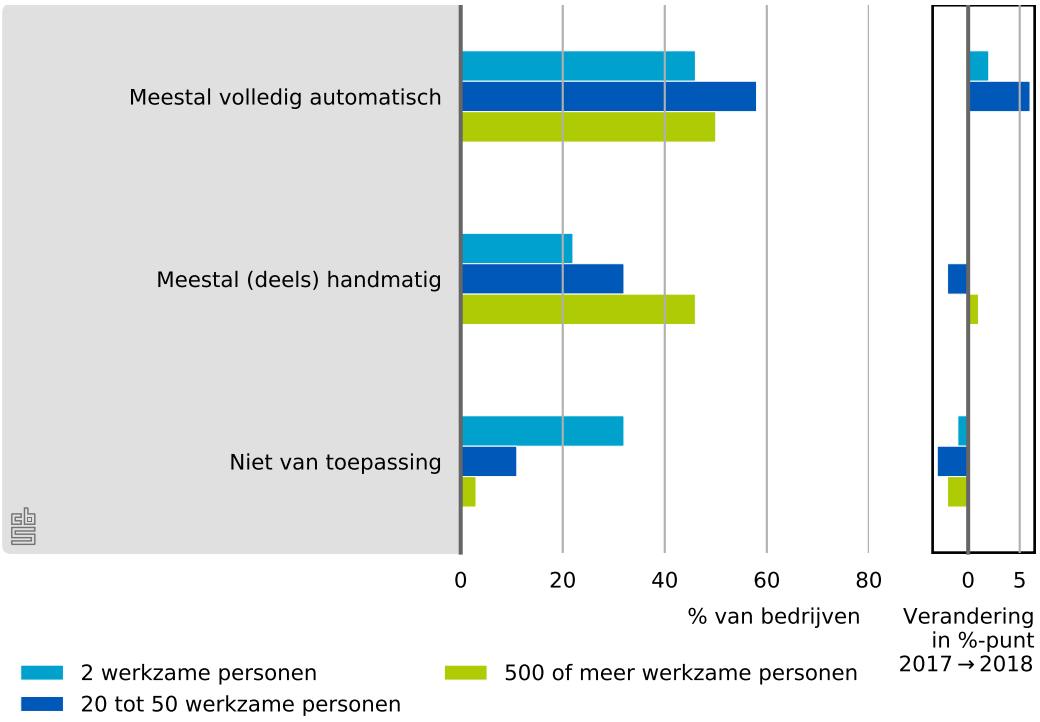


Bron: CBS, 2018b

Om de toename van het aantal cybersecuritymaatregelen dat bedrijven nemen nog verder samen te vatten kunnen we ook simpelweg naar het percentage van bedrijven kijken dat meer dan zes maatregelen neemt. Dit wordt in figuren 2.1.7 en 2.1.8 voor respectievelijk verschillende bedrijfsgrootteklasses en bedrijfstakken getoond voor zowel 2017 en 2018. Het percentage van bedrijven dat meer dan zes maatregelen neemt is gemiddeld met 5 procentpunt toegenomen. De grootste toename is te zien bij bedrijven met tien tot twintig werkzame personen. Bijna 40 procent gaf in 2018 aan meer dan zes cybersecuritymaatregelen te gebruiken. Een jaar eerder was dat nog 31 procent.

Uitvoering security-updates

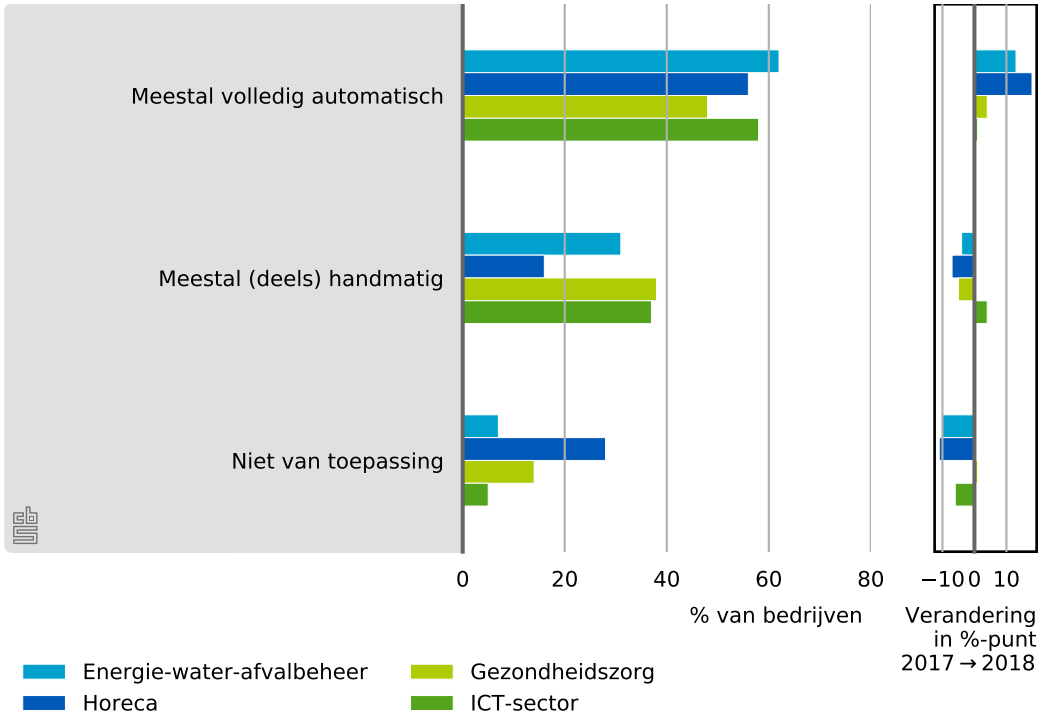
2.1.9 Uitvoering security-updates per bedrijfsgrootteklasse, 2018



Bron: CBS, 2018a

De organisatie van de ICT-beveiliging wordt in figuur 2.1.9 en 2.1.10 onder de loep genomen. De eerste drie items slaan op de manier waarop bedrijven hun security-updates uitvoeren. Het tijdig uitvoeren van security-updates binnen een bedrijf is een goede indicator van het cybersecurityniveau van een bedrijf. We kunnen zien dat de meeste van de medium en grote bedrijven een security-updatebeleid hebben. Het is opvallend dat grote bedrijven dit relatief vaker handmatig uitvoeren, terwijl medium bedrijven kiezen om dit automatisch te doen. Dit zou te maken kunnen hebben met het feit dat bij grote bedrijven vaak meer ICT-experts werken die een security-update wellicht liever handmatig doen om meer controle over het proces te hebben. Daarnaast hebben grote bedrijven vaak een meer complexe ICT-infrastructuur dat wellicht meer handmatig onderhoud behoeft. Bij kleine bedrijven worden security-updates minder vaak toegepast (rond de 70 procent heeft een security-updatebeleid). Van de kleine bedrijven die wel security-updates toepassen doet de meerderheid dat automatisch. In tabellen A.9 en A.10 kan het overzicht voor alle bedrijfsgrootteklasse en bedrijfstak gevonden worden.

2.1.10 Uitvoering security-updates per bedrijfstak, 2018

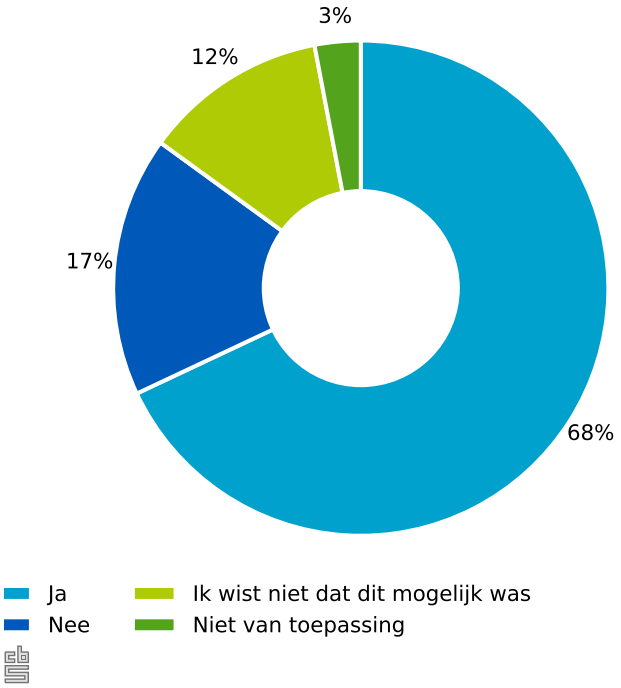


Bron: CBS, 2018b

2.2 Personen

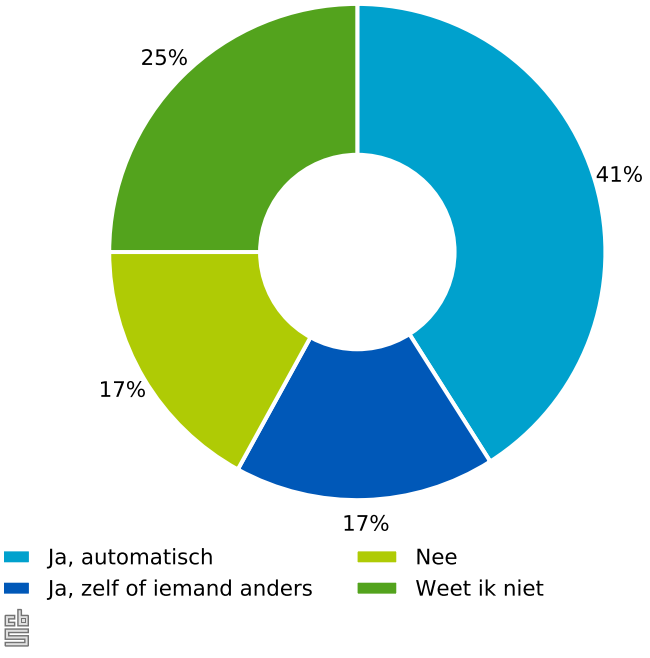
Net als bedrijven kunnen personen maatregelen nemen om zichzelf meer cyberweerbaar te maken. In figuur 2.2.1 wordt het percentage van de Nederlandse bevolking tussen 16 en 75 jaar geplot dat in 2018 de toegang tot Apps beperkte of weigerde. Het laat zien dat 68 procent inderdaad toegang tot een App heeft beperkt of geweigerd, wat welbeschouwd een vorm van bewustzijn van cyberweerbaarheid aangeeft. In figuur 2.2.2 zien we dat 58 procent van de Nederlandse bevolking tussen de 16 en 75 jaar al dan niet automatisch enige vorm van beveiligingssoftware geïnstalleerd heeft. Ook dit geeft aan dat bijna twee derde deel van de bevolking bewust bezig is het cybersecurityniveau van hun smartphone te verbeteren.

2.2.1 Percentage van de bevolking van 16 tot 75 jaar dat datatoegang van hun smartphone heeft beperkt of geweigerd, 2018



Bron: CBS, 2018h

2.2.2 Percentage van de bevolking van 16 tot 75 jaar dat beveiligingssoftware zoals virusscanner, anti-spam of firewall op de telefoon geïnstalleerd heeft, 2018



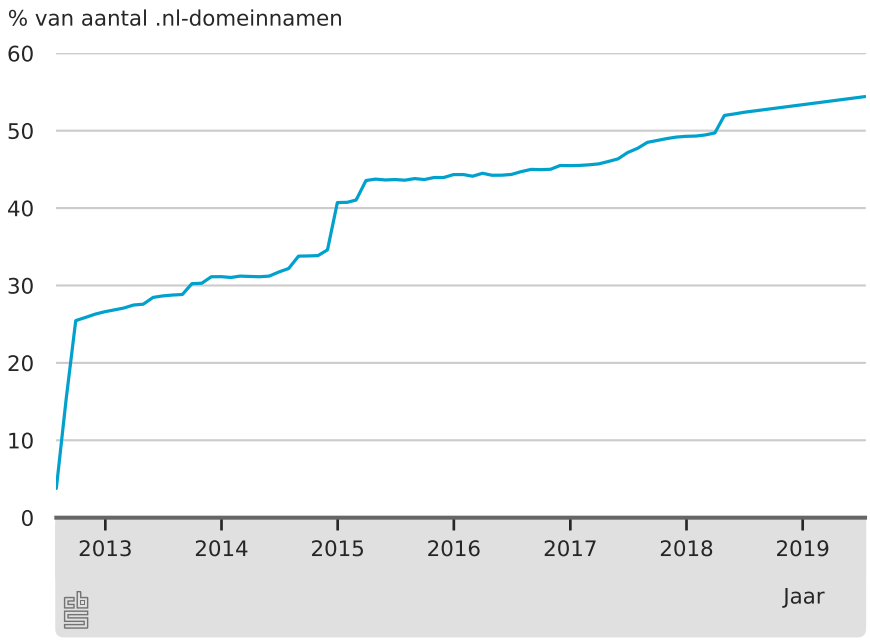
Bron: CBS, 2018h

2.3 Internetstandaarden voor websites

Een laatste indicator op het terrein van maatregelen om de cybersecurity te verhogen is het aantal .nl-domeinnamen dat gebruikmaakt van DNSSEC. DNSSEC is een beveiligingssysteem voor DNS, het internet-telefoonboek 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. Op die manier kunnen wachtwoorden of andere gevoelige informatie worden onderschept. 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. Het op deze wijze misleiden van een internetgebruiker is een beproefde methode om iemand vertrouwelijke gegevens of zelfs geld te ontfutselen. 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 2.3.1 is te zien dat het percentage van .nl bedrijven met een domeinnaam met DNSSEC gestaag toeneemt. Deze domeinnaamregistratie wordt door SIDN, 2018 uitgevoerd. We kunnen zien dat nu ruim de helft van de .nl domein namen met een DNSSEC beveiligd is.

2.3.1 Percentage nl-domeinnamen met DNSSEC



Bron: SIDN, 2018

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.

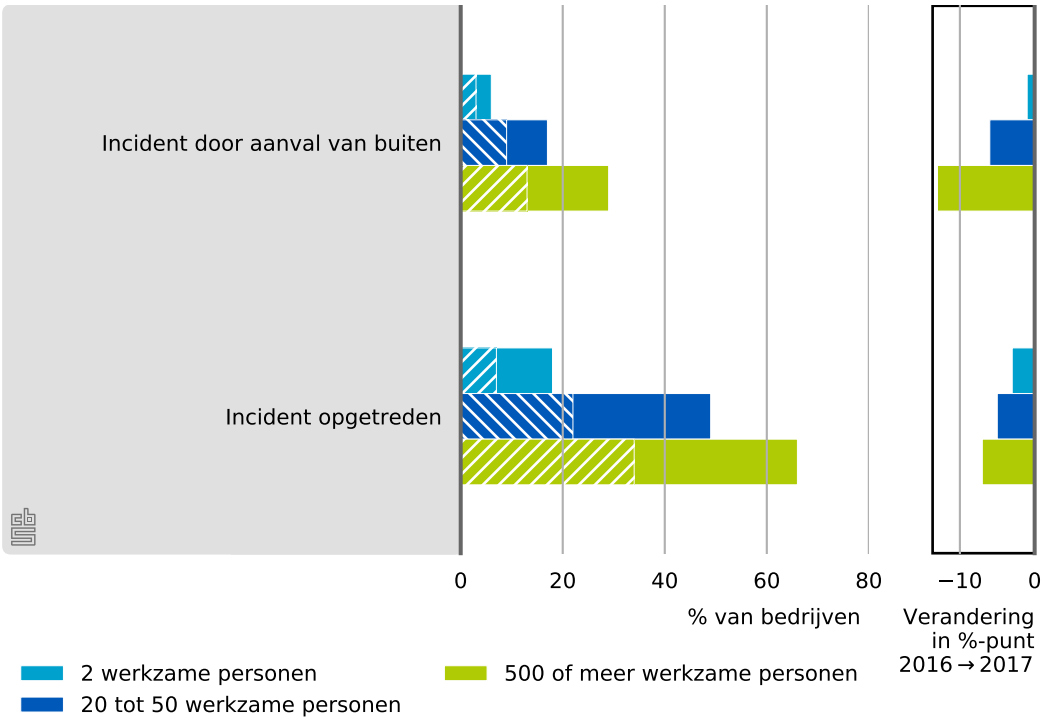
3.1 Bedrijven

In deze paragraaf nemen we de incidenten bij bedrijven onder de loep. Hierna komen de incidenten bij personen aan bod.

Cybersecurityincidenten per bedrijfsgrootte en -tak

Uit de resultaten van de ICT-enquête kunnen we de uitkomsten per bedrijfsgrootte en bedrijfstak opsplitsen. We bekijken hier de cybersecurityincidenten achtereenvolgens per bedrijfsgrootte en -tak.

3.1.1 Oorzaken en kosten (gearceerd) van ICT-veiligheidsincidenten per bedrijfsgrootteklasse, 2017

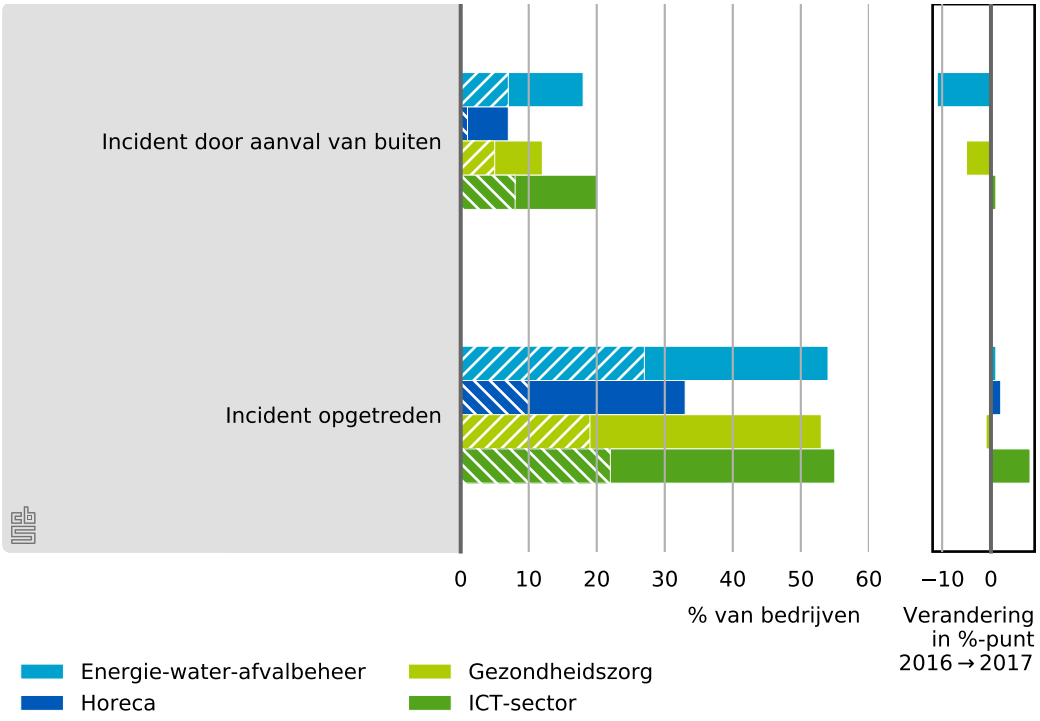


Bron: CBS, 2018a

Grote bedrijven hebben vaker incidenten

In figuur 3.1.1 kunnen we zien dat beide soorten incidenten toenemen naarmate bedrijven groter worden. Van de grote bedrijven meldt 66 procent in 2017 een cybersecurityincident

3.1.2 Oorzaken en kosten (gearceerd) van ICT-veiligheidsincidenten per bedrijfstak, 2017



Bron: CBS, 2018b

gehad te hebben. Bij 34 procent van de grote bedrijven ging dit met kosten gepaard. Voor kleine bedrijven is dit aanzienlijk minder: maar 18 procent van de bedrijven met 2 werknemers meldt dat ze een incident in 2017 hebben gehad waarbij dit voor 7 procent van de bedrijven leidde tot kosten.

Als we kijken naar de cybersecurityincidenten door een aanval van buitenaf is de trend hetzelfde: grote bedrijven melden meer incidenten door een aanval van buitenaf dan kleine bedrijven. Wederom zijn bij ongeveer de helft van deze incidenten hiermee kosten gemoeid: 29 procent van de grote bedrijven meldt een cybersecurityincident door een aanval van buitenaf waarbij 13 procent aangeeft dat hier kosten mee gemoeid waren. Voor kleine bedrijven zijn deze cijfers respectievelijk 6 en 3 procent. Het totale overzicht van de andere bedrijfsgrootteklasses en bedrijfstakken wordt in tabellen A.11 en A.12 gegeven.

Dat grote bedrijven meer incidenten rapporteren, kan meerdere oorzaken hebben. Allereerst hebben grote bedrijven vaker een grotere, meer complexe ICT-infrastructuur met meer computers die aan het netwerk aangesloten zijn; dit maakt de kans op een incident uiteraard groter. Als je kijkt naar incidenten door een aanval van buiten kunnen we aannemen dat grote bedrijven vaak interessanter voor cybercriminelen zijn omdat er meer te halen valt of de (publiciteits)schade groter is.

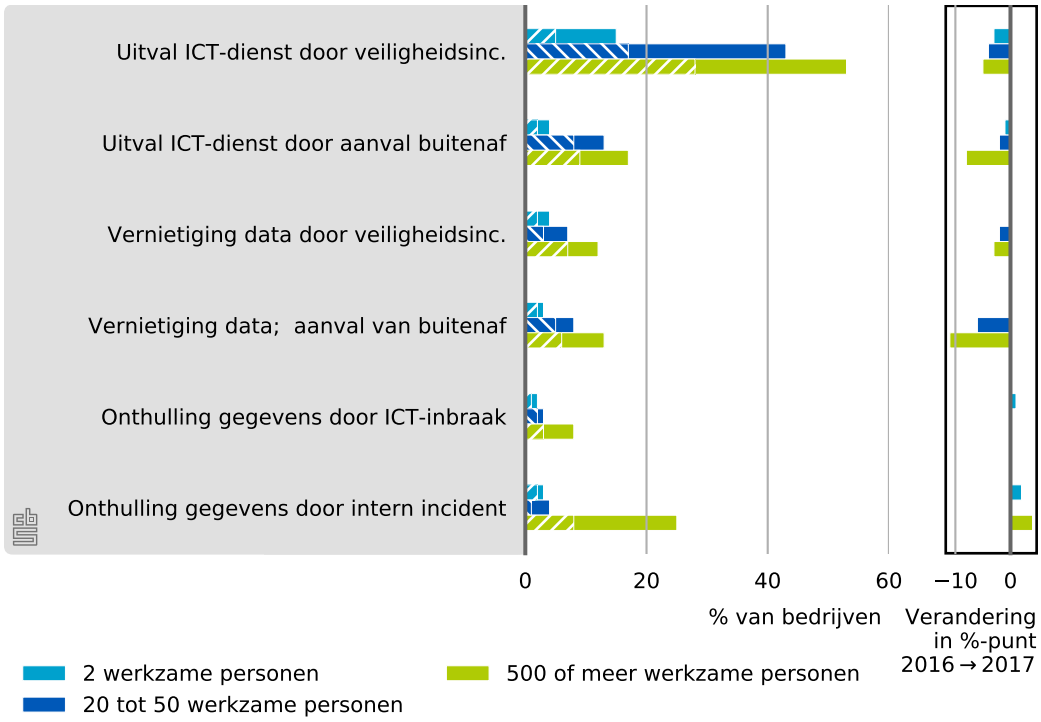
Opvallend genoeg hangt het aantal incidenten niet zozeer samen met de bedrijfstak. Voor de bedrijfstakken die we in figuur 3.1.2 bekijken, vinden we dat ongeveer de helft van de bedrijven een incident heeft gehad, waarvan weer ongeveer de helft kosten met zich meebracht. Alleen de horeca meldt aanzienlijk minder incidenten: ongeveer 30 procent van de horecabedrijven heeft een incident in 2017 gehad, waarvan ongeveer een derde (10 procent) met kosten gepaard ging.

Ook incidenten door een aanval van buitenaf vinden ongeveer gelijk plaats voor alle bedrijfstakken: tussen de 12 en 20 procent van de bedrijven heeft in 2017 te maken gehad met een incident door een aanval van buitenaf. Wederom vinden de minste aanvallen van buiten plaats in de horeca: 7 procent van de horecabedrijven geeft aan een incident door een aanval van buitenaf gehad te hebben waarvan bij 1 procent sprake was van kosten door deze aanval.

Afname van aantal cybersecurityincidenten in 2017

Ten slotte wordt aan de rechter zijde in figuren 3.1.1 en 3.1.2 ook nog de verandering van het aantal incidenten in procentpunten ten opzichte van 2016 weergegeven voor respectievelijke verschillende bedrijfsgrootteklasses en bedrijfstakken. Meest opvallend is dat het aantal incidenten bij de meeste categorieën afgenomen is. Als we ons beperken tot de incidenten door een aanval van buitenaf kunnen we zien dat grote bedrijven 13 procentpunt minder incidenten door een aanval van buitenaf melden: een afname van 42 procent naar 29 procent, oftewel 30 procent minder aanvallen van buitenaf. Ook de energiesector heeft zo'n 10 procentpunt minder incidenten. Alhoewel we het verband waarschijnlijk niet direct zo kunnen leggen, is het toch interessant te constateren dat we in het vorige hoofdstuk juist gezien hebben dat het aantal cybersecuritymaatregelen over de hele linie in 2018 ook toegenomen was. In appendix A wordt in tabellen A.11 en A.12 het overzicht gegeven van alle grootteklassen en bedrijfstakken.

3.1.3 Oorzaken en kosten (gearceerde deel) van ICT-veiligheidsincidenten per grootteklasse, 2017

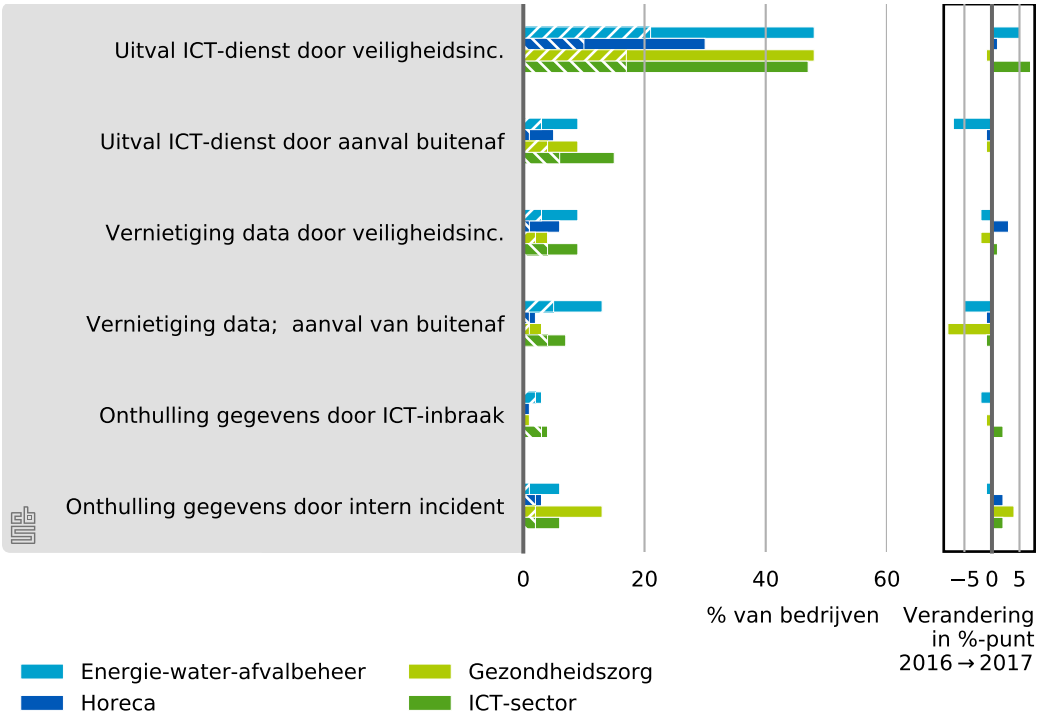


Bron: CBS, 2018a

Cybersecurityincidenten per type

We kunnen de cybersecurityincidenten ook nog uitsplitsen naar het type incident. In figuren 3.1.3 en 3.1.4 vinden we de volgende categorieën: uitval ICT-dienst, vernietiging data en

3.1.4 Oorzaken en kosten (gearceerde deel) van ICT-veiligheidsincidenten per bedrijfstak, 2017



Bron: CBS, 2018a

onthulling gegevens. Voor ieder van deze categorieën onderscheiden we weer op welke wijze dit incident tot stand gekomen is: door eigen toedoen of door een aanval van buitenaf. Alleen de laatste wordt als een cybersecurityincident beschouwd en is in feite een vorm van cybercrime.

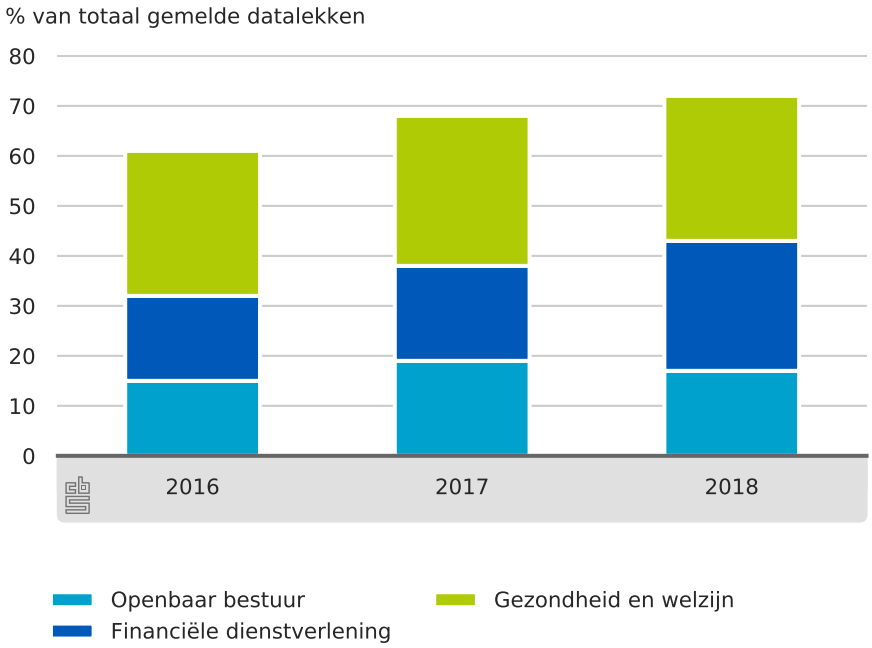
Datalekken en verstoringen telecomdiensten

Voorbeelden van incidenten die niet per se strafbaar zijn en zich eerder onbedoeld dan willens en wetens voordoen, zijn de uitval van telecomdiensten door een defecte zendmast of het lekken van privacygevoelige gegevens door het achterlaten van een laptop in het openbaar vervoer. Belangrijke storingen van openbare telecomdiensten moeten de aanbieders van deze diensten melden bij het Agentschap Telecom. Belangrijk betekent hier dat er een groot aantal klanten (gedupeerden) bij betrokken moet zijn. In 2018 zijn 57 van dit soort meldingen gedaan (50 in 2017). Een melding kan gepaard gaan met meerdere verstoringen van telecomdiensten. In 2018 leidden de 57 meldingen tot 133 verstoringen (114 in 2017). In sommige gevallen is de storing overigens wel doelbewust veroorzaakt door een kwaadwillende. Vaak ook is de oorzaak de genoemde defecte zendmast of verkeerd geïnstalleerde software en/of defecte hardware. De oorzaken kunnen dus uiteenlopen, het effect is hetzelfde, namelijk tijdelijke uitval van de dienst. En dit is ook het hoofddoel van de meldplicht: het meten van de betrouwbaarheid of stabiliteit van de aangeboden dienst. Kunnen de gebruikers erop rekenen dat die dienst praktisch altijd beschikbaar is? Een belangrijk issue hier is de permanente bereikbaarheid van het alarmnummer 112.

21 duizend meldingen van datalekken

Een ander voorbeeld van incidenten die niet altijd doelbewust en strafbaar zijn, zijn de 20 881 datalekken zoals die in 2018 zijn gemeld bij de Autoriteit Persoonsgegevens. Over 2017 waren dit er 1 009 (5 617 in 2016). De meldplicht datalekken geldt in Nederland al sinds 2016. Deze meldplicht is in EU-verband verder geformaliseerd en gepreciseerd middels 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 toe hebben kunnen 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. In 2018 was 4 procent van de datalekken veroorzaakt door het hacken en/of via malware en phishing toegang krijgen tot de betreffende gegevens. In 2017 was dit nog 6 procent.

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



Bron: Autoriteit Persoonsgegevens, 2019

Meeste meldingen uit gezondheidssector

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.). Het aandeel van ieder van deze instanties aan het totaal aantal lekken wordt in figuur 3.1.5 weergegeven. In 2016 waren deze drie sectoren goed voor 61 procent van alle gemelde datalekken, in 2017 was dit opgelopen tot 68 procent en in 2018 tot bijna drie kwart (72 procent). Dit zijn ook voorbeelden van sectoren waar veel en 'gevoelige' persoonsgegevens worden verwerkt en opgeslagen. Aan de andere kant zegt het ook weer niet alles dat de meeste meldingen uit de gezondheidssector 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 ca. 3 500 meldingen. In 2018 was de genoemde 72 procent goed voor 15 duizend meldingen.

Type gelekte gegevens

De meest gelekte gegevens zijn naam, geslacht en contactgegevens. Daarnaast zijn in 2018 ruim zes duizend meldingen ontvangen over gelekte medische gegevens (6 526) en het burgerservicenummer (6 056). Een datalek met het burgerservicenummer komt met name voor in de zorg (37 procent) en in de sector openbaar bestuur (33 procent).

Omvang datalekken en hacken

In de ruime meerderheid van de gevallen, namelijk 58 procent in 2018, raakt het datalek één persoon. Het gaat in deze gevallen veelal (77 procent) om het versturen of afgeven van persoonsgegevens aan een verkeerde ontvanger. In mindere mate (3 procent) treft het datalek een zeer groot aantal betrokkenen. Datalekken die meer dan 5 000 personen raken, worden vaak veroorzaakt door hacking, malware en/of phishing. In 2018 werd 4 procent van alle datalekken veroorzaakt door hacking, malware en/of phishing (6 procent in 2017). Datalekken door hacking en phishing komen met name voor in de zorg (18 procent). Ook hier geldt dat er in absolute aantallen wel degelijk sprake is van een toename van het aantal gemelde datalekken als gevolg van hacking, malware en/of phishing. In 2018 komt 4 procent van alle datalekken overeen met ruim 800 datalekken terwijl de 6 procent in 2017 overeenkomt met 600 gemelde datalekken door hacking, malware en/of phishing. De voorgaande voorbeelden van incidenten illustreren dat niet alles wat er mis kan gaan met ICT kwade opzet is. Ook geldt dat de primaire oorzaak van een incident niet altijd uit ‘cyberspace’ hoeft te komen maar ook gewoon een natuurlijke oorzaak kan hebben (omgewaaide zendmast) of voortkomt uit menselijke tekortkomingen (slordigheid, vergeetachtigheid, onbekwaamheid e.d.).

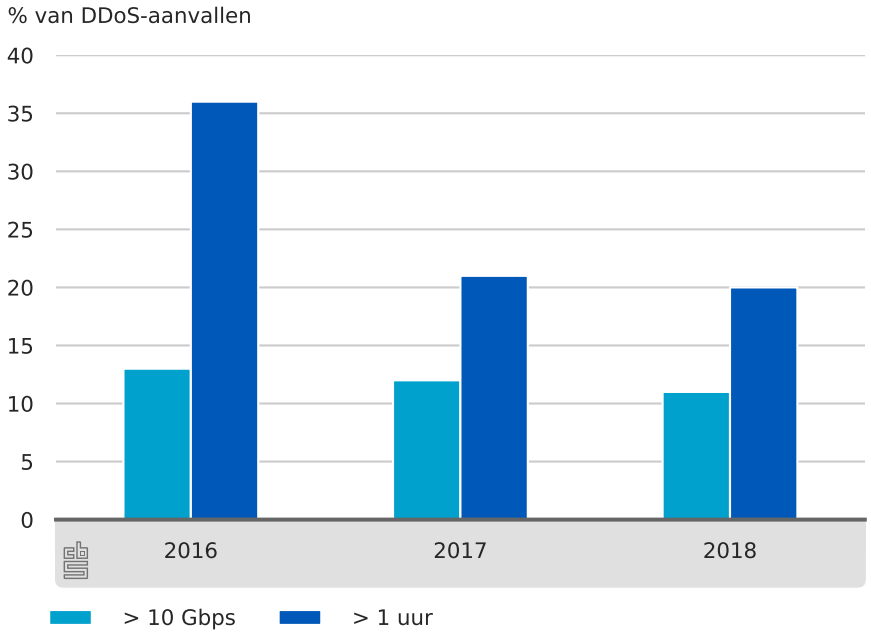
DDoS-aanvallen

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 meer netwerkverkeer dan de server van de website aan kan. De in figuur 3.1.6 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 lang niet alle DDoS-aanvallen waar Nederlandse websites mee te maken hebben, maar wel een groot deel daarvan. Het absolute aantal DDoS-aanvallen is daardoor minder veelzeggend dan de karakteristieken van de DDoS-aanvallen, ook omdat het aantal deelnemers van deze dienst gestaag toeneemt (68 in 2018; 56 in 2017; 53 in 2016).

Kenmerken van DDoS-aanvallen zijn de omvang (Gbps) en de duur (tijd). In figuur 3.1.6 wordt het aandeel van relatief intensere of langere aanvallen geplot, namelijk de aanvallen groter dan 10 Gbps (Gigabit per seconde) of langer dan één uur. In 2018 had 11 procent van de DDoS-aanvallen een omvang van meer dan 10 Gbps. Dit was in 2017 het geval bij 12 procent van de aanvallen. Een vijfde (20 procent) van de aanvallen duurde in 2018 langer dan een uur (21 procent in 2017). In 2016 was dit aandeel met 36 procent veel hoger. Hierbij moet

opgemerkt worden dat de grootte van een DDoS-aanval niet per se maatgevend is voor de schade die een DDoS 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 tegen te gaan. Daarnaast is het soort DDoS-aanval waar websites mee geconfronteerd worden in ontwikkeling. Het aantal soorten DDoS-aanvallen in 2018 bedroeg 56 tegen 46 in 2017; het mitigeren van een DDoS-aanvallen vergt dus een continue inspanning met betrekking tot het up-to-date houden van de software van de NaWas.

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



Bron: NBIP en SIDN, 2018
[1)] Het gaat hier alleen om de DDoS-aanvallen van bij de NaWas aangesloten internetproviders.

In een studie samen met SIDN heeft de NBIP voor de periode 1 juli 2017–30 juni 2018 geanalyseerd welke websites doelwit van een DDoS-aanval waren (NBIP en SIDN, 2018). Op basis van de tekst op de websites zijn deze websites ingedeeld in categorieën. Websites van evenementen en festivals waren het vaakst doelwit van DDoS-aanvallen gevolgd door websites van onderwijsinstellingen. Uit het onderzoek kwam ook naar voren dat er regelmatig websites uit de lucht gaan, niet omdat ze doelbewust worden aangevallen maar omdat ze toevallig achter hetzelfde IP-adres schuil gaan als het voorziene doelwit (collateral attacks); shared-hosting brengt dus risico's met zich mee.

4. Cybercrime

We presenteren in dit hoofdstuk enkele cijfers uit de bij de politie geregistreerde misdrijven waar cybercrime in is opgenomen. Voor de statistische informatie over cybercrime is dit jaar dankbaar gebruikgemaakt van de recente publicatie Digitale Veiligheid en Criminaliteit (DVC), zie (CBS, 2018h). De cijfers uit de DVC-publicatie hangen vaak samen met cybersecurity, maar zijn breder dan dat. Er wordt namelijk gekeken naar alle vormen van criminaliteit die online plaatsvinden; ook vormen waarbij niet per se sprake is geweest van criminaliteit ten gevolge van cybersecurityincidenten. Zo wordt bijvoorbeeld ook gekeken of mensen last hebben gehad van vervelende mailtjes, of online pesten. Dit zijn zaken die niet direct ontstaan door een tekort aan beveiliging. We zullen in deze monitor daarom alleen een selectie van wat getallen meenemen om een beeld te krijgen. Voor het hele verhaal verwijzen we naar de DVC-publicatie.

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 reeds 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.

8,5 procent van de Nederlanders slachtoffer cybercrime

Van de Nederlanders van 12 jaar en ouder maakt 97,7 procent gebruik van internet, waarvan 92,6 procent dagelijks voor privédoeleinden online is. Door de intrede van smartphone en tablet is het gebruik van internet zeer toegankelijk geworden, dus zulke hoge scores zijn niet vreemd meer. Van deze doelgroep zegt 8,5 procent in 2018 de afgelopen 12 maanden slachtoffer te zijn geweest van één of meerdere vormen van digitale criminaliteit. Dit is dus inclusief incidenten waarbij cybersecurity geen rol speelt, zoals interpersoonlijke incidenten. De verschillen tussen mannen en vrouwen zijn hierin verwaarloosbaar. Alleen bij vermogensdelicten zijn mannen vaker slachtoffer: 5,1 procent tegen 4 procent.

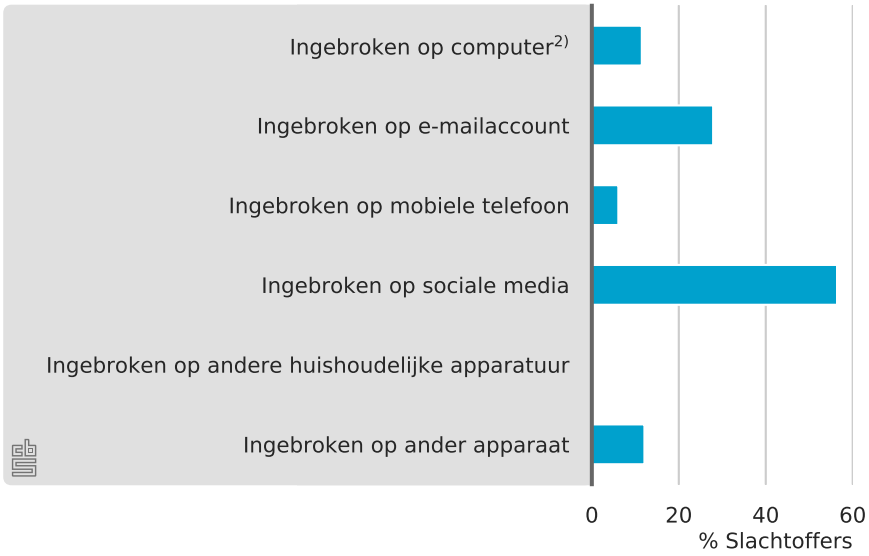
4.1 Computervredebreuk

Een van de cybercrimeincidenten 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. Eerst gaan we in op de niet-geregistreerde hackincidenten zoals ze uit de DVC-publicatie(CBS, 2018h) volgen, vervolgens publiceren we de bij de politie geregistreerde hackincidenten.

Gemelde en onvermelde computervredebreuk

De data in deze sectie is verkregen uit de DVC-publicatie van dit jaar (CBS, 2018h). De doelgroep van dit onderzoek zijn de personen in Nederland ouder dan 12 jaar. Uit deze doelgroep zijn 100 duizend personen in 2018 benaderd waarvan er ruim 38 duizend gereageerd hebben.

4.1.1 Het soort apparaat of account dat gehackt is, 2018[1)]



Bron: Digitale veiligheid en criminaliteit (CBS, 2018h)
[1)] Meerdere antwoorden mogelijk
[2)] Desktop, laptop of tablet

Meer dan de helft van de hacks betreft sociale media

In 2018 zegt 1,8 procent van de personen boven de 12 jaar de afgelopen 12 maanden gehackt te zijn (CBS, 2018h). Hierbij zijn alleen de incidenten meegenomen waarbij hacken geen ander geregistreerd doel had, zoals bijvoorbeeld het stelen van geld door te hacken. In dat geval wordt het niet als hacken geregistreerd, maar als vermogensdelict. Als deze delicten waarbij hacken toegepast wordt ook meegeteld worden, dan is 2,1 procent van de personen in 2018 de afgelopen 12 maanden gehackt.[1)]

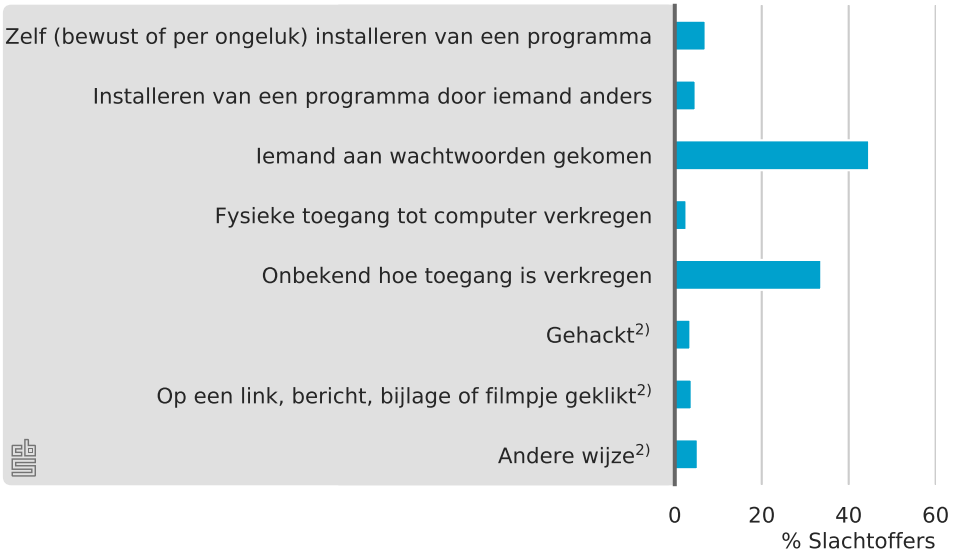
Het soort apparaat of account dat gehackt is, wordt in figuur 4.1.1 gegeven. Een ruime meerderheid (56 procent) betreft het hacken van sociale media, gevolgd door het hacken van een e-mailaccount met ruim een kwart van de gevallen. Hacken van andere huishoudelijke apparaten komt eigenlijk niet voor (0,1 procent).

Hacken in bijna de helft van gevallen door verkregen wachtwoorden

In figuur 4.1.2 wordt een overzicht van de oorzaken van de hack getoond. Het is de zien dat in bijna de helft van de gevallen (45 procent) als oorzaak van de hack aangegeven wordt dat wachtwoorden verkregen zijn. Dit benadrukt het belang van het veilig gebruik van wachtwoorden. Door de veelheid van inlogaccounts gebruiken veel mensen nu vaak hetzelfde wachtwoord voor meerdere sites. Mocht je wachtwoord op de ene website gestolen worden dan kan een cybercrimineel vrij eenvoudig ook al je andere accounts met hetzelfde wachtwoord uitproberen. Gelukkig bieden steeds meer browsers wachtwoordmanagers aan

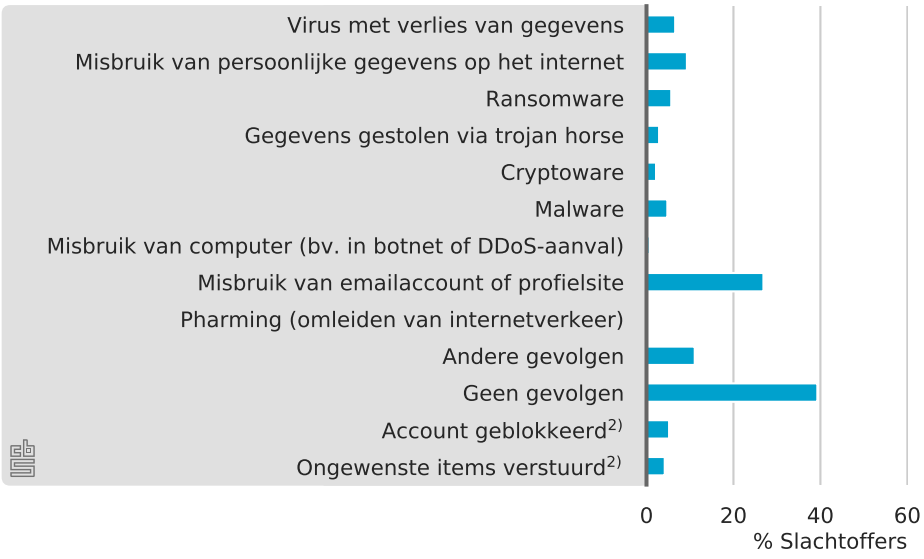
[1)] In de Cybersecuritymonitor 2018 (CBS, 2018g) meldden we nog dat het percentage personen ouder dan 15 jaar dat gehackt was rond de 7,5 procent lag, waar we hier maximaal 2,1 procent rapporteren (als we hacken met vermogensdelicten meenemen). De cijfers zijn echter niet goed te vergelijken omdat deze uit een ander CBS-onderzoek komen, namelijk uit 'De Veiligheidsmonitor'CBS, 2017b. Het cijfer dat we hier gebruiken komt uit het nieuwe CBS-onderzoek Digitale Veiligheid & en CriminaliteitCBS, 2018h. In laatstgenoemde onderzoek zijn de vragen verbeterd en aangescherpt, waardoor de uitkomsten lager uitvallen dan voorgaande jaren. In de DVC-publicatie wordt uitgebreid ingegaan op de oorzaken van de verschillen tussen beide onderzoeken.

4.1.2 Oorzaken hacken bij personen boven de 12 jaar, 2018[1)]



Bron: Digitale veiligheid en criminaliteit (CBS, 2018h)
1) Meerdere antwoorden mogelijk
2) Genoemd bij open antwoordcategorie

4.1.3 Gevolgen hacken bij personen boven de 12 jaar, 2018[1)]



Bron: Digitale veiligheid en criminaliteit (CBS, 2018h)
1) Meerdere antwoorden zijn mogelijk
2) Genoemd bij open antwoordcategorie

4.1.4 Melding en aangiftes van hacken, 2018

	% slachtoffers
Gemeld bij minstens één van de volgende instanties	5,1
Politie	4,8
Centraal Meldpunt Nederland (meld.nl)	0,3
Meld Misdaad Anoniem	0,2
Aangifte bij de politie	2,8

Bron: CBS, 2018h

4.1.5 Bij de politie geregistreerde computervredebreuk

	2013	2014	2015	2016	2017	2018	Eenheid
Totaal geregistreerde misdrijven	2535	2045	2225	1875	2310	2885	*aantal*
Geregistreerde misdrijven, relatief	0,23	0,2	0,23	0,2	0,28	0,37	*% van totaal*
Geregistreerde misdrijven per 100 000 inw.	15	12	13	11	14	17	*per 100 000 inw.*
Totaal opgehelderde misdrijven	255	195	165	170	170	240	*aantal*
Opgehelderde misdrijven, relatief	10	9,5	7,4	9	7,4	8,3	*% van totaal*
Registraties van verdachten	295	235	195	215	250	400	*aantal*

Bron: CBS

(om je wachtwoorden veilig op te slaan zodat je voor iedere site eenvoudig een nieuw moeilijk wachtwoord kan kiezen). Ook wordt op steeds meer websites en platformen two-factor-authentication aangeboden, zodat je naast je wachtwoord ook een code moet invoeren die je via een sms of met behulp van een hardware- of softwarekey kan ontvangen. Dit verhoogt het cyberveiligheidsniveau van je account aanzienlijk. Bij middelgrote bedrijven zagen we in hoofdstuk 3 dat het gebruik van hardware- en softwarekeys in 2018 met 24 procent toegenomen is. Het is te hopen dat in navolging van bedrijven ook bij personen het gebruik van veilige inlogmethodes toeneemt, om zo het aantal hacks waarbij een onderschept wachtwoord de oorzaak is, terug te dringen.

Misbruik email of profielsite meest voorkomend

De gevolgen van de hack zijn te vinden in figuur 4.1.3 Na de bijna 40 procent van de internetgebruikers die aangeeft dat de hack geen gevolgen had, is misbruik van het emailaccount of de profielwebsite het meest voorkomende gevolg van een hack. Dit is consistent met onze eerdere constatering dat in meer dan de helft van de hackincidenten het een socialemedia-account betreft.

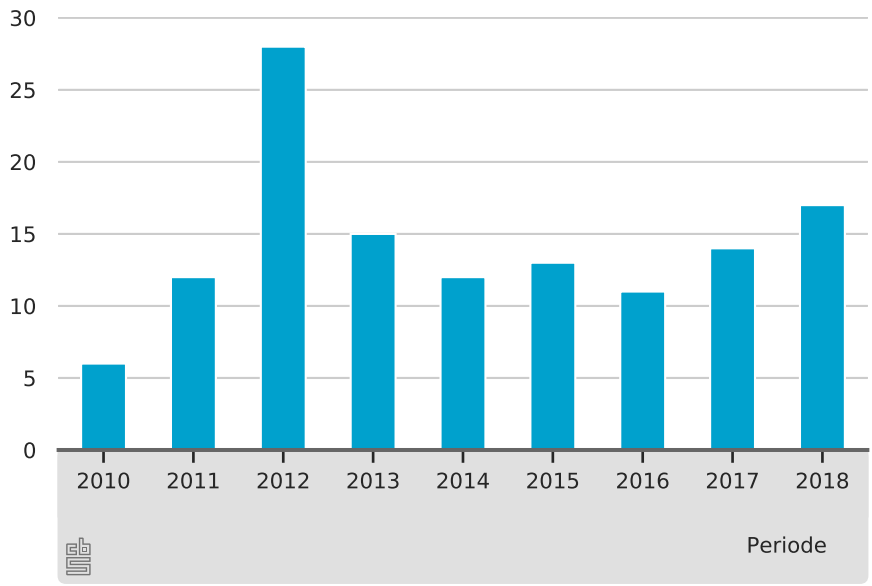
Één op de twintig hackincidenten gemeld

In tabel 4.1.4 is terug te vinden dat slechts 1 op de 20 (5,1 procent) incidenten van hacken bij een instantie gemeld wordt. Aangifte bij de politie vindt slechts in 2,8 procent van de gevallen plaats. Uitgaande van de 1,8 procent van de bevolking die gehackt is, komt dit neer op 50 aangiftes per 100 duizend inwoners.

Geregistreerde computervredebreuk

Hierboven hebben we de niet-geregistreerde hackincidenten besproken zoals ze uit de DVC-publicatie CBS, (2018h) volgen. In deze paragraaf gaan we in op de bij de politie geregistreerde cybercrime. We kijken eerst naar de hackincidenten omdat deze met een eigen 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.

4.1.6 Aantal geregistreerde computervredebreuken per jaar per 100 duizend inwoners



Bron: CBS

Aantal geregistreerde aangifte van hacken blijft constant

De bij de politie geregistreerde computervredebreuk wordt in tabel 4.1.5 samengevat. Figuur 4.1.6 licht van deze tabel het aantal geregistreerde hackincidenten uit. In 2018 zijn 17 hackincidenten per 100 duizend inwoners geregistreerd. Hiervoor meldden we dat uit het DVC-rapport 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 gek. 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. Het aantal bij de politie geregistreerde aangiftes ligt zo tussen de 10 en 50 per 100 duizend inwoners en dit is de laatste jaren redelijk constant gebleven. Daarnaast hadden we al eerder geconstateerd dat het aantal daadwerkelijke hacks waarbij geen aangifte gedaan is een stuk hoger ligt: van slechts 1 op de 20 hacks wordt bij de politie aangifte gedaan.

Cybercrime achterhalen in aangiften

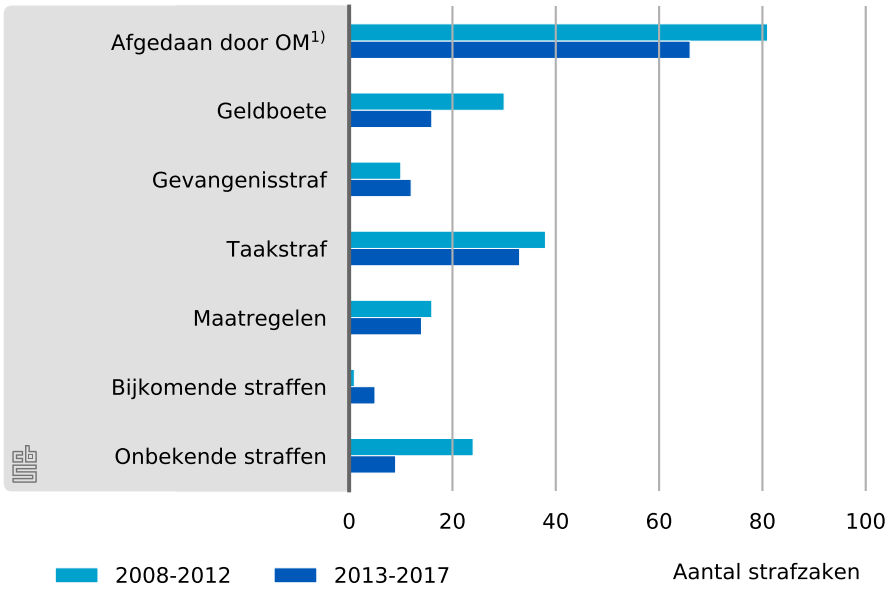
Naast de hierboven genoemde categorieën, komen ook in andere delicttypen cybercrime-aspecten voor. Het CBS heeft tekstanalyse toegepast bij het onderzoeken van processen-verbaal uit 2016 om te achterhalen bij welke geregistreerde misdrijven cybercrime een rol speelt (CBS, 2018f). Daarbij is cybercrime 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

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



Bron: CBS

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

In figuur 4.1.7 is weergegeven welke sancties het Openbaar Ministerie en de rechter hebben opgelegd aan verdachten van computervredebreuk. In een deel van de gevallen deelt het

4.1.8 Aantal computervredebreuk zaken afgehandeld door de rechter of het OM

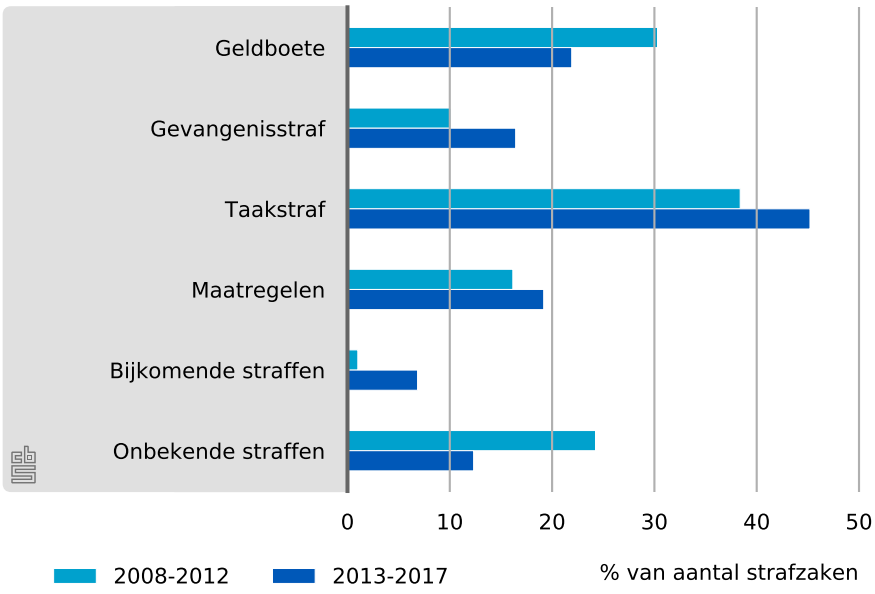
		2008–2012	2013–2017
Totaal door OM genomen beslissingen		439	354
Waarvan:	- Transactie OM[1)]	81	66
	- Schuldig verklaard door rechter	99	73

Bron: CBS

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

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 deze uit een taakstraf of een geldboete of het vergoeden van de schade. 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 4.1.8 aflezen dat het OM in de periodes 2008–2012 en 2013–2017 respectievelijk 18 en 19 procent van de zaken zelf afdeed met een transactie, strafbeschikking of voorwaardelijke beleidssepot. Het totaal aantal zaken is bovendien van 439 naar 354 afgenomen.

4.1.9 Door de rechter opgelegde straffen en maatregelen voor computervredebreuk per strafzaak[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.

De percentages van de soorten door de rechter opgelegde straffen en maatregelen per periode worden in figuur 4.1.9 gegeven. Het totaal door de rechter afgehandelde strafzaken was 99 voor de periode 2008–2012 en 73 voor de periode 2013–2017. In de periode 2013–2017 bestonden de opgelegde straffen voor het grootste gedeelte uit taakstraffen (45 procent). Het aandeel taakstraffen en gevangenisstraffen is gegroeid van respectievelijk 38 en 10 procent in de periode 2008–2012 naar 45 en 16 procent in de periode 2013–2017. Het aandeel door de rechter opgelegde geldboetes is gedaald van 30 naar 22 procent.

Bijlagen

Tabellen

Definities

A.1 Overzicht van de bedrijfstakken

Code	Bedrijfsklasse
C	Industrie
D-E	Energie, water, afvalbeheer
F	Bouwnijverheid
G	Handel
H	Vervoer en opslag
I	Horeca
J	Informatie en communicatie
K	Financiële dienstverlening
L	Verhuur en handel van onroerend goed
M	Specialistische zakelijke diensten
N	Verhuur en overige zakelijke diensten
Q	Gezondheids- en welzijnszorg
ICT	ICT-sector

A.2 Overzicht 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.3 Gebruikte ICT-maatregelen voor alle grootteklassen als percentage van het aantal bedrijven, 2018

	Antivirussoftware	Beleid voor sterke wachtwoorden	Authenticatie via soft- of hardwaretoken	Encryptie voor het opslaan van data	Encryptie voor het versturen van data	Gegevens op andere fysieke locatie	Network access control	VPN bij internetgebruik buiten het eigen bedrijf	Logbestanden voor analyse incidenten	Methodes voor beoordelen ICT-veiligheid	Risicoanalyses	Andere maatregelen
	% van bedrijven											
Totaal	87	62	31	25	25	68	34	32	34	25	25	15
Bedrijfsgrootte												
2 tot 250 werkzame personen	87	62	31	24	25	68	33	32	33	25	25	15
2 werkzame personen	82	56	24	19	20	57	22	19	20	14	15	9
3 tot 5 werkzame personen	86	60	29	24	25	66	34	28	27	21	21	13
5 tot 10 werkzame personen	90	65	34	25	26	73	38	37	39	30	29	17
10 tot 20 werkzame personen	94	68	36	28	29	80	44	45	49	37	36	19
20 tot 50 werkzame personen	96	74	43	33	32	86	51	59	64	46	47	27
50 tot 100 werkzame personen	98	82	52	42	42	90	59	72	77	57	59	32
100 tot 250 werkzame personen	99	89	62	51	50	91	63	80	83	68	71	45
250 tot 500 werkzame personen	98	94	71	62	61	91	65	87	87	72	73	52
500 of meer werkzame personen	99	95	82	69	72	95	72	88	91	79	80	65

Bron: CBS, 2018a

A.4 Gebruikte ICT-maatregelen voor alle bedrijfstakken als percentage van het aantal bedrijven, 2018

	Antivirussoftware	Beleid voor sterke wachtwoorden	Authenticatie via soft- of hardwaretoken	Encryptie voor het opslaan van data	Encryptie voor het verstuuren van data	Gegevens op andere fysieke locatie	Network access control	VPN bij internetgebruik buiten het eigen bedrijf	Logbestanden voor analyse incidenten	Methodes voor beoordelen ICT-veiligheid	Risicoanalyses	Andere maatregelen
	% van bedrijven											
Totaal, C-N en Q	96	74	43	34	34	84	50	56	60	45	46	26
Bedrijfstak												
Voedings-, genotm. industrie	93	64	38	26	23	80	40	51	51	34	39	21
Textiel-, kleding-, lederindustrie	98	73	36	31	30	83	47	56	60	47	43	28
Hout-, papier-, grafische industr.	98	68	38	29	27	87	50	63	60	44	47	21
Raffinaderijen en chemie	99	86	53	46	42	92	60	76	81	60	60	34
Kunststof- en bouwm. industr	98	71	47	32	29	89	53	65	68	51	51	27
Basismetaal, metaalprod. -ind.	96	66	35	23	23	89	42	52	58	46	40	16
Elektrische en elektron. ind.	99	76	45	37	34	93	54	77	70	61	51	28
Machine-industrie	99	79	41	38	33	91	60	76	72	46	48	32
Transportmiddelenindustrie	99	65	40	28	31	90	44	58	61	48	49	30
Overige industrie en reparatie	98	74	41	33	33	90	49	65	63	49	43	26
Energie, water, afvalbeheer	97	78	48	33	35	90	59	67	68	58	49	31
B&U en wegenbouw	97	67	40	20	25	86	38	47	54	39	38	25
Vervoer en opslag	94	72	41	29	29	84	45	49	56	38	42	23
Logiesverstrekking	99	81	29	25	26	77	46	48	41	34	41	21
Eet- en drinkgelegenheden	82	54	15	14	15	56	26	18	24	18	18	5
Uitgeverijen, film, radio en t.v.	98	78	44	40	44	90	54	65	70	51	54	39
Telecommunicatie	96	95	69	64	50	89	70	88	83	67	73	53
IT- en informatiedienstverlening	97	92	68	73	67	90	71	78	85	73	73	54
Banken	96	91	78	76	70	94	81	88	90	79	78	67
Verzekeringen	100	100	83	67	75	100	79	90	98	90	99	65
Financiële advisering	100	100	82	72	68	91	72	86	92	78	81	52
Verhuur/handel onroerend goed	94	84	63	34	28	85	54	68	75	63	63	35
Juridisch en managementadvies	98	86	59	44	44	90	55	63	69	54	54	34
Architecten-, ingenieursbureaus	98	81	44	38	33	93	62	80	80	50	56	30
Research	99	81	51	49	47	91	64	73	79	61	57	40
Reclamewezen/marktonderzoek	95	75	52	45	49	85	55	72	69	54	50	36
Uitzendbureaus en arb.bemidd.	90	72	41	32	31	79	48	45	52	42	41	21
Reisbureaus, reisorganisaties	97	86	53	51	48	80	66	77	63	57	51	33
Gezondheidszorg	98	88	63	49	70	91	56	63	63	55	62	28
Verzorging en welzijn	98	76	45	38	44	86	42	46	56	41	47	31
ICT-sector	98	91	65	69	60	91	71	80	84	65	67	50

Bron: CBS, 2018b

A.5 Percentage van bedrijven met *N* ICT-maatregelen per grootteklasse, 2018

Aantal maatregelen *N*	0	1	2	3	4	5	6	7	8	9	10	11	12
Totaal	8,5	9,0	14,3	13,2	9,6	8,9	8 ,1	7,0	6,1	4,6	4,1	3,6	3,0
Bedrijfsgrootte													
2 werkzame personen	12,8	12,6	18,7	15,2	9,2	8,6	6,0	4,6	4,2	2,8	2,1	1,8	1,4
3 tot 5 werkzame personen	8,9	9,8	15,8	13,1	10,4	8,4	9,0	7,3	5,5	4,0	3,2	2,8	1,8
5 tot 10 werkzame personen	6,3	7,0	11,4	13,6	10,7	10,2	9,0	7,9	6,3	5,4	5,0	3,9	3,2
10 tot 20 werkzame personen	3,5	5,8	9,7	12,3	9,6	9,7	9,7	10,1	8,2	5,5	6,2	5,3	4,5
20 tot 50 werkzame personen	2,4	2,3	6,4	8,3	9,2	9,5	11,1	10,2	0,6	8,9	7,1	7,6	6,3
50 tot 100 werkzame personen	1,4	1,2	3,5	5,3	6,7	6,9	10,2	9,0	13,0	12,2	10,1	9,8	10,8
100 tot 250 werkzame personen	0,8	0,8	1,0	2,9	4,1	5,2	7,7	10,3	2,4	12,1	13,6	13,0	16,2
250 tot 500 werkzame personen	1,0	0,1	0,5	1,2	2,1	4,1	5,3	8,1	10,1	16,1	16,0	18,8	16,7
500 en meer werkzame personen	0,6	0,0	0,3	0,5	1,2	2,7	3,8	5,0	9,8	10,2	16,2	18,3	31,3

Bron: CBS, 2018a

A.6 Percentage van bedrijven met *N* ICT-maatregelen per bedrijfstak, 2018

Aantal maatregelen *N*	0	1	2	3	4	5	6	7	8	9	10	11	12
Totaal	8,5	9,0	14,3	13,2	9,6	8,9	8,1	7,0	6,1	4,6	4,1	3,6	3,0
Bedrijfstak													
Industrie	5,1	6,9	13,9	14,5	10,3	9,7	9,3	7,1	6,8	4,2	4,7	4,4	3,1
Specialistische zakelijke diensten	3,3	5,8	10,8	12,7	11,2	10,5	10,7	9,5	7,5	5,2	4,5	4,5	3,7
Verhuur en overige diensten	9,1	9,5	14,3	11,2	11,0	9,3	7,9	5,9	5,3	4,4	3,7	3,7	4,5
Gezondheids- en welzijnszorg	2,6	2,7	7,3	8,4	9,0	12,1	11,6	9,6	11,5	9,4	8,5	3,8	3,5
Energievoorziening en afvalbeheer	12,2	5,5	11,2	10,2	9,3	6,5	5,7	9,7	4,8	7,3	4,8	5,1	7,6
Bouwnijverheid	10,9	11,5	18,2	16,6	9,7	7,5	5,0	5,1	4,4	4,7	1,5	3,2	1,7
Handel	8,7	11,2	16,0	14,0	9,4	9,0	7,7	6,5	5,5	3,3	3,7	2,8	2,1
Vervoer en opslag	10,1	12,5	14,5	17,9	9,6	6,6	6,2	4,8	4,1	4,4	3,1	4,1	2,1
Horeca	21,5	13,8	20,1	15,2	8,4	6,1	4,6	4,3	2,6	0,5	1,7	0,8	0,3
Informatie en communicatie	2,9	2,4	9,0	6,2	7,0	7,8	7,8	7,8	8,3	9,6	7,8	10,4	12,9
Financ, dienstverl, beperkt	3,3	2,4	5,8	11,1	5,1	6,7	10,4	11,2	3,3	12,8	6,7	9,5	11,8
Verhuur/handel onroerend goed	14,0	10,9	13,3	7,9	11,3	8,0	10,0	9,0	5,9	6,0	1,7	1,6	0,5
ICT	2,2	1,3	7,0	5,9	6,0	8,8	6,4	10,5	9,9	9,5	9,1	10,2	13,0

Bron: CBS, 2018b

A.7 Percentage van bedrijven met *N* of minder ICT-maatregelen per grootteklasse, 2018

Aantal maatregelen *N*	0	1	2	3	4	5	6	7	8	9	10	11	12
Totaal	8,5	17,6	31,9	45,0	54,6	63,5	71,6	78,6	84,7	89,3	93,3	97,0	100
Bedrijfsgrootte													
2 werkzame personen	12,8	25,4	44,1	59,3	68,5	77,1	83,1	87,7	91,9	94,7	96,8	98,6	100
3 tot 5 werkzame personen	8,9	18,7	34,6	47,6	58,0	66,4	75,4	82,7	88,2	92,2	95,4	98,2	100
5 tot 10 werkzame personen	6,3	13,4	24,8	38,4	49,1	59,3	68,3	76,2	82,5	87,9	92,9	96,8	100
10 tot 20 werkzame personen	3,5	9,3	19,0	31,3	40,9	50,6	60,3	70,4	78,6	84,1	90,2	95,5	100
20 tot 50 werkzame personen	2,4	4,7	11,2	19,4	28,6	38,1	49,2	59,4	70,0	79,0	86,1	93,7	100
50 tot 100 werkzame personen	1,4	2,5	6,0	11,3	18,0	24,9	35,0	44,0	57,0	69,2	79,4	89,2	100
100 tot 250 werkzame personen	0,8	1,6	2,6	5,5	9,6	14,8	22,5	32,8	45,1	57,2	70,8	83,8	100
250 tot 500 werkzame personen	1,0	1,1	1,6	2,8	4,9	9,0	14,3	22,4	32,5	48,5	64,5	83,3	100
500 en meer werkzame personen	0,6	0,6	0,9	1,5	2,6	5,3	9,1	14,2	24,0	34,2	50,4	68,7	100

Bron: CBS, 2018a

A.8 Percentage van bedrijven met *N* of minder ICT-maatregelen per bedrijfstak, 2018

Aantal maatregelen *N*	0	1	2	3	4	5	6	7	8	9	10	11	12
Totaal	8,5	17,6	31,9	45,0	54,6	63,5	71,6	78,6	84,7	89,3	93,3	97,0	100
Bedrijfstak													
Industrie	5,1	12,0	25,9	40,4	50,6	60,3	69,7	76,7	83,6	87,8	92,5	96,9	100
Specialistische zakelijke diensten	3,3	9,1	19,9	32,6	43,8	54,3	65,1	74,5	82,0	87,2	91,7	96,3	100
Verhuur en overige diensten	9,1	18,6	32,9	44,1	55,2	64,5	72,4	78,3	83,7	88,1	91,8	95,5	100
Gezondheids- en welzijnszorg	2,6	5,3	12,6	21,0	30,0	42,1	53,7	63,4	74,9	84,3	92,7	96,5	100
Energievoorziening en afvalbeheer	12,2	17,8	28,9	39,2	48,5	55,0	60,7	70,4	75,2	82,5	87,3	92,4	100
Bouwnijverheid	10,9	22,3	40,6	57,2	66,9	74,4	79,4	84,6	88,9	93,6	95,1	98,3	100
Handel	8,7	19,9	36,0	50,0	59,4	68,3	76,1	82,6	88,1	91,4	95,1	97,9	100
Vervoer en opslag	10,1	22,6	37,0	54,9	64,5	71,1	77,4	82,2	86,3	90,7	93,8	97,9	100
Horeca	21,5	35,3	55,5	70,7	79,0	85,1	89,8	94,0	96,6	97,1	98,8	99,7	100
Informatie en communicatie	2,9	5,3	14,3	20,5	27,5	35,3	43,1	50,9	59,2	68,8	76,6	87,1	100
Financ. dienstverl, beperkt	3,3	5,8	11,5	22,6	27,7	34,3	44,8	56,0	59,3	72,1	78,8	88,2	100
Verhuur/handel onroerend goed	14,0	24,9	38,2	46,1	57,4	65,4	75,4	84,4	90,3	96,3	97,9	99,5	100
ICT	2,2	3,5	10,5	16,4	22,5	31,3	37,7	48,2	58,2	67,7	76,9	87,0	100

Bron: CBS, 2018b

A.9 Organisatie ICT-beveiliging per bedrijfsgrootteklasse, 2018

	Meestal volledig automatisch	Meestal (deels) handmatig	Niet van toepassing
Totaal	50	25	25
Bedrijfsgrootte			
2 tot 250 werkzame personen	50	25	25
2 werkzame personen	46	22	32
3 tot 5 werkzame personen	48	25	27
5 tot 10 werkzame personen	54	25	21
10 tot 20 werkzame personen	58	26	16
20 tot 50 werkzame personen	58	32	11
50 tot 100 werkzame personen	58	35	8
100 tot 250 werkzame personen	56	39	5
250 tot 500 werkzame personen	54	41	5
500 of meer werkzame personen	50	46	3

Bron: CBS, 2018a

A.10 Organisatie ICT-beveiliging per bedrijfstak, 2018

	Meestal volledig automatisch	Meestal (deels) handmatig	Niet van toepassing
Totaal, C-N en Q	58	30	12
Bedrijfstakken			
Voedings-, genotm. industrie	51	27	22
Textiel-, kleding-, lederindustrie	68	30	2
Hout-, papier-, grafische industr.	47	40	12
Raffinaderijen en chemie	64	33	3
Kunststof- en bouwm. industr	55	37	8
Basismetaal, metaalprod. ind.	51	40	9
Elektrische en elektron. ind.	54	41	6
Machine-industrie	55	37	8
Transportmiddelenindustrie	51	36	13
Overige industrie en reparatie	52	41	6
Energie, water, afvalbeheer	62	31	7
B&U en wegenbouw	51	34	14
Vervoer en opslag	58	25	17
Logiesverstrekking	72	17	11
Eet- en drinkgelegenheden	56	16	28
Uitgeverijen, film,radio en t.v.	53	38	9
Telecommunicatie	62	37	1
IT- en informatiedienstverlening	57	37	6
Banken	69	30	1
Verzekeringen	57	41	1
Financiële advisering	57	23	20
Verhuur/handel onroerend goed	60	29	11
Juridisch en managementadvies	62	31	8
Architecten-, ingenieursbureaus	59	34	7
Research	59	34	7
Reclamewezen/marktonderzoek	64	28	8
Uitzendbureaus en arb.bemidd.	59	22	18
Reisbureaus, reisorganisatie	55	35	10
Gezondheidszorg	48	38	14
Verzorging en welzijn	59	28	13
Management- en tech. advies	61	32	7
Reclame, design, overige dnst.	60	33	7
ICT-sector	58	37	5

Bron: CBS, 2018b

A.11 Incidenten en kosten per grootteklasse als percentage van het aantal bedrijven, 2017

	Uitval ICT-dienst door veilig-heidsinc.	Uitval ICT-dienst door aanval buitenaf	Vernieti-ging data door veilig-heidsinc.	Vernieti-ging data; aanval van buitenaf	Onthul-ling gegevens door ICT-inbraak	Onthul-ling gegevens door in-tern incident
Totaal	25	7	5	5	3	3
Bedrijfsgrootte						
2 tot 250 werkzame personen	25	7	5	5	3	3
2 werkzame personen	15	4	4	3	2	3
3 tot 5 werkzame personen	23	7	5	4	3	4
5 tot 10 werkzame personen	29	8	6	5	2	3
10 tot 20 werkzame personen	38	10	7	5	2	3
20 tot 50 werkzame personen	43	13	7	8	3	4
50 tot 100 werkzame personen	48	12	8	10	3	6
100 tot 250 werkzame personen	49	12	8	12	3	9
250 tot 500 werkzame personen	49	15	9	13	6	14
500 of meer werkzame personen	53	17	12	13	8	25

Bron: CBS, 2018a

A.12 Incidenten per bedrijfstak als percentage van het aantal bedrijven, 2017

	Uitval ICT-dienst door veilig-heidsinc.	Uitval ICT-dienst door aanval buitenaf	Vernieti-ging data door veilig-heidsinc.	Vernieti-ging data; aanval van buitenaf	Onthul-ling gegevens door ICT-inbraak	Onthul-ling gegevens door in-tern incident
Totaal, C-N en Q	42	11	7	7	3	5
Bedrijfstak						
Voedings-, genotm.ndustrie	43	14	10	14	7	7
Textiel-, kleding-, lederindustrie	46	15	9	8	6	0
Hout-, papier-, grafische industr.	30	10	4	4	1	6
Raffinaderijen en chemie	51	16	8	6	7	9
Kunststof- en bouwmateriaalind.	37	12	8	10	3	2
Basismetaal, metaalprod.-ind.	37	5	4	7	3	2
Elektrische en elektron. ind.	48	12	8	7	1	3
Machine-industrie	37	10	3	9	2	2
Transportmiddelenindustrie	40	10	7	11	2	2
Overige industrie en reparatie	41	12	7	7	3	4
Energie, water, afvalbeheer	48	9	9	13	3	6
B&U en wegenbouw	42	14	7	14	2	3
Vervoer en opslag	40	15	5	9	2	3
Logiesverstrekking	30	3	4	3	2	2
Eet- en drinkgelegenheden	30	5	6	2	1	3
Uitgeverijen, film,radio en t.v.	43	15	8	6	2	2
Telecommunicatie	45	30	7	7	1	4
IT- en informatiedienstverlening	45	15	9	6	5	5
Banken	56	15	8	11	2	6
Verzekeringen	57	16	10	13	7	24
Financiële advisering	52	15	9	5	5	5
Verhuur/handel onroerend goed	51	13	12	7	1	7
Juridisch en managementadvies	45	11	7	8	2	8
Architecten-, ingenieursbureaus	47	12	9	10	3	7
Research	52	14	14	10	10	9
Reclamewezen/marktonderzoek	36	9	8	6	5	5
Uitzendbureaus en arb.bemidd.	38	9	7	8	2	4
Reisbureaus, reisorganisatie	42	8	1	3	1	3
Gezondheidszorg	48	9	4	3	1	13
Verzorging en welzijn	42	7	6	6	3	10
Management- en tech. advies	46	11	8	9	3	8
Reclame, design, overige dnst.	41	10	9	5	5	5
ICT-sector	47	15	9	7	4	6

Bron: CBS, 2018b

Literatuur

Autoriteit Persoonsgegevens (2019). *Datalekregistraties*.

CBS (2017a). *Cybersecuritymonitor 2017*.

CBS (2017b). *Veiligheidsmonitor 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 (2019). *CBS StatLine*.

NBIP en SIDN (2018). *The impact of DDOS attacks on Dutch enterprises*.

SIDN (2018). *SIDN Labs: .nl stats en data*.

Uitgave 2019