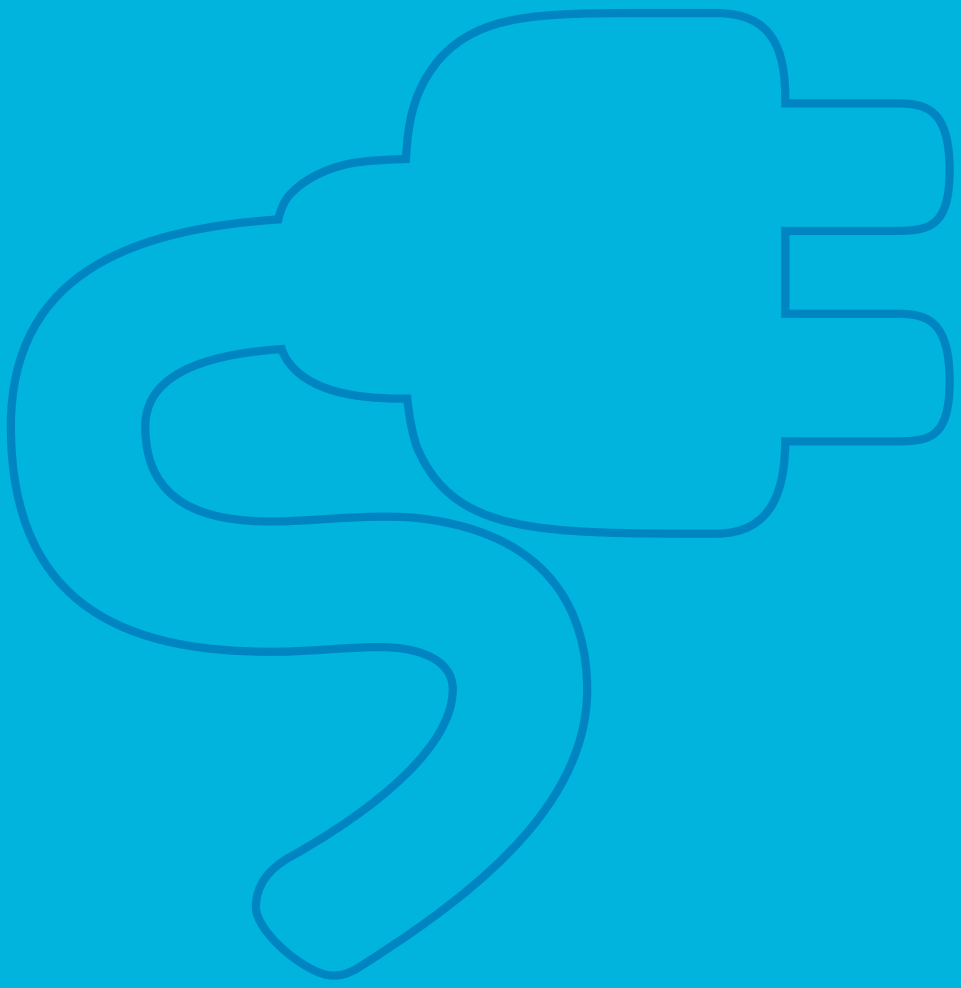
Cybersecuritymonitor 2018

Een verkenning van dreigingen, incidenten en maatregelen



Cybersecuritymonitor 2018

Een verkenning van dreigingen, incidenten en maatregelen

Verklaring van tekens

.	Gegevens ontbreken
*	Voorlopig cijfer
**	Nader voorlopig cijfer
x	Geheim
–	Nihil
–	(Indien voorkomend tussen twee getallen) tot en met
0 (0,0)	Het getal is kleiner dan de helft van de gekozen eenheid
Niets (blank)	Een cijfer kan op logische gronden niet voorkomen
2017–2018	2017 tot en met 2018
2017/2018	Het gemiddelde over de jaren 2017 tot en met 2018
2017/'18	Oogstjaar, boekjaar, schooljaar enz., beginnend in 2017 en eindigend in 2018
2015/'16–2017/'18	Oogstjaar, boekjaar, enz., 2015/'16 tot en met 2017/'18

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: Textcetera, Den Haag en CCN Creatie, Den Haag
Ontwerp: Edenspiekermann

Inlichtingen
Tel. 088 570 70 70, fax 070 337 59 94
Via contactformulier: www.cbs.nl/infoservice

ISBN 978-90-357-2630-7

Inhoud

Samenvatting

In deze publicatie is een aantal indicatoren samengebracht die iets zeggen over de verschillende aspecten van cybersecurity. In een samenleving waar in toenemende mate via informatie- en communicatietechnologie (ICT) wordt gecommuniceerd is het waarborgen van de privacy en de veiligheid van deze communicatie en de opslag van de bijbehorende gegevens een serieuze voorwaarde. Als het vertrouwen van de gebruikers hierin ontbreekt dan kan dit een belemmering zijn voor de verdere ontwikkeling van het gebruik van internet en ICT. In deze tweede publicatie over cybersecurity van het CBS wordt aan de hand van een twintigtal indicatoren een beeld geschetst van de cyberdelicten en incidenten waarmee mensen, bedrijven en organisaties worden geconfronteerd en de preventieve maatregelen die ze ertegen nemen. De publicatie geeft hiermee nog geen volledig beeld van de incidenten en bedreigingen en ook niet van alle maatregelen die getroffen zijn om deze bedreigingen het hoofd te bieden. De ambitie is op termijn te komen tot een volledige *Cybersecuritymonitor* die een evenwichtig beeld geeft van de situatie in Nederland.

Cybersecuritymaatregelen

- Bij 86 procent van de bedrijven met 10 of meer werkzame personen was in 2016 sprake van werkzaamheden op het terrein van ICT-beveiliging. Twee derde van deze bedrijven (67 procent) liet deze werkzaamheden voornamelijk door derden verzorgen. Voor bedrijven met 2 tot 10 werkzame personen waren deze percentages respectievelijk 64 en 60 procent.
- Ruim een derde van de bedrijven (35 procent) met 10 of meer werkzame personen maakte in 2016 gebruik van betaalde clouddiensten. De helft van deze bedrijven (49 procent) gebruikte hierbij een apart voor het bedrijf gereserveerde server. In 2014 waren deze percentages respectievelijk 28 procent en39 procent.
- Acht op de tien (81 procent) bedrijven met 10 of meer werkzame personen had in 2017 drie of meer ICT-beveiligingsmaatregelen genomen. Voor de bedrijven met 2 tot 10 werkzame personen gold dit voor zes op de tien (60 procent) bedrijven.
- Bij 84 procent van de bedrijven met 10 of meer werkzame bedrijven was in 2017 sprake van het uitvoeren van software-updates (security-patches). Bij de bedrijven met 2 tot 10 werkzame personen gold dit voor 71 procent van de bedrijven. Bij beide groepen werden deze updates meestal volledig automatisch doorgevoerd.
- Eind juni 2018 maakte 52 procent van de .nl-domeinnamen gebruik van DNSSEC; een beveiligingsstandaard die o.a. *phishing* en *pharming* bemoeilijkt. Eind juni 2014 was dit nog 32 procent.
- In 2017 gaf 89 procent van de personen van 12 jaar of ouder met een computer aan dat deze was voorzien van beveiligingssoftware; 7 procent gaf aan dit eigenlijk niet te weten. Van de bezitters van mobiele telefoons en smartphones gaf 52 procent aan dat hun mobiele telefoon was voorzien van beveiligingssoftware. Hier gaf echter bijna een kwart (24 procent) van de personen aan dit niet te weten.
- In 2017 maakte 46 procent van de personen van 12 jaar of ouder gebruik van clouddiensten voor de opslag van gegevens (31 procent in 2014).
- Een op de drie Nederlanders (34 procent) veranderde in 2016 weleens de instellingen van de browser om cookies te voorkomen of te beperken.

Cybersecurityincidenten

- In 2016 had 50 procent van de bedrijven met 10 of meer werkzame personen een ICT-veiligheidsincident gehad. Voor de bedrijven met 2 tot 10 werkzame personen was dit

26 procent. ICT-veiligheidsincidenten betreffen hier zowel onbedoelde uitval van ICT als uitval veroorzaakt door een aanval van buitenaf.

- Voor de bedrijven met 10 of meer werkzame personen die een ICT-veiligheidsincident hadden, vloeide hier voor 49 procent van de bedrijven ook kosten uit voort. Voor de bedrijven met 2 tot 10 werkzame personen was dit aandeel 44 procent.
- 9 procent van de bedrijven met 10 of meer werkzame personen met een ICT-veiligheidsincident heeft hier melding van gedaan bij bijvoorbeeld de politie, de bank of de Autoriteit Persoonsgegevens. Voor de bedrijven met 2 tot 10 werkzame personen was dit 6 procent. Overigens hoeven lang niet alle ICT-veiligheidsincidenten (ergens) te worden gemeld.
- In 2017 had 3 procent van de Nederlanders bij het online bestellen van goederen en diensten te maken met fraude. Dit was in 2016 ook zo.
- In 2017 ontving de Autoriteit Persoonsgegevens 10 009 meldingen van datalekken; 5 617 in 2016. Dit zijn incidenten waarbij privacygevoelige informatie in handen van derden terecht is gekomen. Dit kan onbedoeld zijn gebeurd door bijvoorbeeld slordigheid van medewerkers van de betreffende organisatie, maar ook moedwillig door kwaadwillende (een hack). In 2017 werd 6 procent van deze datalekken veroorzaakt door hacking.
- In 2017 waren er 50 meldingen van verstoringen van de continuïteit van openbare telecomdiensten bij het Agentschap Telecom. In 2016 waren dit er 57. Ook hier geldt dat dit onbedoeld gebeurd kan zijn (bijvoorbeeld een defecte zendmast) of door moedwillige sabotage.
- Van alle DDoS-aanvallen (al dan niet verijdeld) in 2017 had 12 procent een omvang van meer dan 10 gbps. Dit percentage is ongeveer gelijk aan dat in 2016 (13 procent). Ruim een op de vijf DDoS-aanvallen (21 procent) duurde langer dan een uur. Dit aandeel is kleiner dan in 2016 (36 procent).Het gaat hier om DDoS-aanvallen die liepen via de internetproviders die gebruikmaken van de Nationale anti-DDoS Wasstraat van de Stichting Nationale Beheerorganisatie Internet Providers.

Cybercrime

- In 2017 was een op de negen Nederlanders (11 procent) slachtoffer van een of meer van de volgende cyberdelicten: identiteitsfraude, koop- en verkoopfraude, hacken of cyberpesten. Ruim een kwart (27 procent) van deze delicten werd gemeld bij een officiële instantie waarvan 13 procent van de gevallen (ook) bij de politie.
- In 2017 is 0,4 procent van de Nederlanders slachtoffer geworden van identiteitsfraude. In 86 procent van de gevallen werd dit gemeld bij een officiële instantie, in 70 procent van de gevallen was dit een bank of financiële instelling en in 21 procent van de gevallen betrof dit (ook) de politie.
- 3,9 procent van de 15-plussers werd opgelicht bij het online shoppen. In 40 procent van de gevallen werd dit gemeld bij een officiële instantie, in 24 procent van de gevallen (ook) bij de politie.
- In 2017 is 4,9 procent van de 15-plussers gehackt. In 5 procent van de gevallen werd dit gemeld bij de politie, in 16 procent van de gevallen (ook) bij een andere instantie. In het merendeel van de gevallen betrof hacken het inbreken op een e-mailaccount, web- of profielsite.
- Van online pestgedrag had 3,1 procent van de Nederlanders last. Met name jongeren worden vaak gepest. In bijna een kwart (23 procent) van de gevallen werd het incident gemeld bij de politie of een andere instantie.
- In 2017 werd 2 300 keer aangifte gedaan van computervredebreuk. Hiervan werd 4,6 procent opgehelderd.

Het Nederlandse 'Internet of Things' volgens Censys

Bij het zoeken naar relevante data over cybersecurity is het CBS naast het verbeteren van zijn eigen enquêtes op dit punt, ook nadrukkelijk op zoek naar andere manieren en bronnen van onderzoek. Er is immers een grens aan wat je personen en bedrijven kan vragen op het punt van cybersecurity. Het langs andere weg (objectiever) vaststellen van kwetsbaarheden in onze ICT-infrastructuur is een belangrijke complementaire aanpak. Een moeilijk punt bij het exploiteren van andere bronnen van gegevens is het vellen van een oordeel over de kwaliteit en representativiteit van deze gegevens (zie ook hoofdstuk 2). Desalniettemin worden in bijlage 1 enkele bevindingen gedeeld uit een eerste exploratief onderzoek met publiek beschikbare data met informatie over apparatuur die was aangesloten op ruim 150 miljoen IP4-adressen wereldwijd zoals verzameld en beschikbaar gesteld door Censys.
Hieruit komt o.a. naar voren dat software met erkende kwetsbaarheden nog lang niet altijd compleet verdwenen is uit de ICT-infrastructuur in Nederland.

Kerntabel indicatoren cybersecurity

Indicator	2014	2015	2016	2017	Eenheid	Bron
Cybersecurity, maatregelen						
ICT-beveiliging en bescherming van data door bedrijven	88	85	86	.	**% bedrijven met 10 of meer werkzame personen**	CBS
	.	.	64		**% bedrijven met 2 tot 10 werkzame personen**	
voornamelijk uitgevoerd door eigen personeel	26	26	33	.	**% bedrijven met 10 of meer werkzame personen met ICT-beveiliging**	
	.	.	40		**% bedrijven met 2 tot 10 werkzame personen met ICT-beveiliging**	
voornamelijk uitgevoerd door externe leverancier(s)	74	74	67	.	**% bedrijven met 10 of meer werkzame personen met ICT-beveiliging**	
	.	.	60		**% bedrijven met 2 tot 10 werkzame personen met ICT-beveiliging**	
Bedrijven die gebruikmaken van betaalde clouddiensten	28	.	35	.	**% bedrijven met 10 of meer werkzame personen**	CBS
op gedeelde servers en/of	64	.	74	.	**% bedrijven met clouddiensten**	
servers uitsluitend gereserveerd voor het bedrijf	39	.	49	.	**% bedrijven met clouddiensten**	
Bedrijven die om veiligheidsredenen niet of maar beperkt via een website/app verkopen	.	.	19	.	**% bedrijven met 10 of meer werkzame personen**	CBS
Bedrijven met drie of meer ICT-veiligheidsmaatregelen[1)]						CBS
	.	.	.	81	**% bedrijven met 10 of meer werkzame personen**	
	.	.	.	60	**% bedrijven met 2 tot 10 werkzame personen**	
Uitvoeren van software-updates (security-patches) door bedrijven						
meestal volledig automatisch	.	.	.	51	**% bedrijven met 10 of meer werkzame personen**	CBS
	.	.	.	47	**% bedrijven met 2 tot 10 werkzame personen**	
meestal (deels) handmatig	.	.	.	33	**% bedrijven met 10 of meer werkzame personen**	
	.	.	.	24	**% bedrijven met 2 tot 10 werkzame personen**	
niet van toepassing	.	.	.	17	**% bedrijven met 10 of meer werkzame personen**	
	.	.	.	29	**% bedrijven met 2 tot 10 werkzame personen**	
Verandert instellingen browser om cookies tegen te gaan of te verminderen	.	36	34	.	**% personen vanaf 12 jaar**	CBS
Mijn computer is voorzien van beveiligingssoftware[2]						CBS
ja				89	**% personen vanaf 12 jaar met een computer**	
Weet niet				7		

Kerntabel indicatoren cybersecurity (vervolg)

Indicator	2014	2015	2016	2017	Eenheid	Bron
Mijn smartphone of mobiele telefoon is voorzien van beveiligingssoftware[2]						
ja				52	**% personen vanaf 12 jaar met een**	
weet niet				24	**smartphone of mobiele telefoon**	
Maakt gebruik van clouddiensten voor opslag van bestanden[3]	31	34	40	46	**% personen vanaf 12 jaar**	CBS
Maakt gebruik van betaalde clouddiensten voor opslag van bestanden[3]	3	4	6	8	**% personen vanaf 12 jaar**	
Websites in het .nl-domein die gebruikmaken van DNS-SEC[4]	32	44	44	47	**% van .nl domeinnamen**	SIDN
Cybersecurity, incidenten						
Bedrijven met ICT-veiligheidsincidenten						CBS
			50		**% bedrijven met 10 of meer werkzame personen**	
			26		**% bedrijven met 2 tot 10 werkzame personen**	
Bedrijven met kosten als gevolg van ICT-veiligheids-incidenten						CBS
			49		**% bedrijven met 10 of meer werkzame personen met ICT-veiligheidsincidenten**	
			44		**% bedrijven met 2 tot 10 werkzame personen met ICT-veiligheidsincidenten**	
Bedrijven die melding hebben gedaan van ICT-veiligheidsincidenten[5]						CBS
			9		**% bedrijven met 10 of meer werkzame personen met ICT-veiligheidsincidenten**	
			6		**% bedrijven met 2 tot 10 werkzame personen met ICT-veiligheidsincidenten**	
Fraude bij online aankopen (bijvoorbeeld geen levering of misbruik van creditcardgegevens)	.	2	3	3	**% personen vanaf 12 jaar**	CBS
Meldingen in het kader van de meldplicht datalekken zoals opgenomen in de Wet bescherming persoonsgegevens	.	.	5617	10009	**aantal meldingen (excl. ingetrokken meldingen)**	Autoriteit Persoonsgegevens
Meldingen in het kader van de zorg- en meldplicht van aanbieders van openbare telecommunicatienetwerken of -diensten zoals opgenomen in de Telecommunicatiewet	41	39	57	50	**aantal incidenten**	Agentschap Telecom
Verstoringen in de continuïteit van de dienstverlening	.	.	112	114	**aantal verstoringen**	
Omvang en duur (verijdelde) DDoS-aanvallen[6]						NBIP
waarvan > 10 gbps			13	12	**% van totaal**	
> 1 uur			36	21	**% van totaal**	
Cybercrime						
Ondervonden delicten cybercrime[7]	18,8	18,7	17,9	18,6	**per 100 inwoners**	CBS
Slachtofferschap cybercrime[7]	11,2	11,1	10,7	11,0	**% personen vanaf 15 jaar**	CBS
Meldingen cybercrime[7]	27,7	26,9	26,9	27,0	**% van ondervonden delicten**	CBS
Meldingen bij politie[7]	12,7	12,7	13,1	13,1	**% van ondervonden delicten**	CBS
Aangifte totaal[7]	7,3	7,8	7,6	8,0	**% van ondervonden delicten**	CBS
identiteitsfraude totaal	0,7	0,6	0,4	0,4	**per 100 inwoners**	
slachtoffers	0,8	0,6	0,4	0,4	**% personen vanaf 15 jaar**	
melding totaal	87,6	84,0	81,9	86,0	**% van ondervonden delicten**	
melding bij politie	14,4	20,4	23,1	20,6	**% van ondervonden delicten**	
aangifte totaal	11,6	13,1	16,9	16,0	**% van ondervonden delicten**	

Kerntabel indicatoren cybersecurity (slot)

Indicator	2014	2015	2016	2017	Eenheid	Bron
koop- en verkoopfraude totaal	4,1	4,2	4,1	4,6	**per 100 inwoners**	
slachtoffers	3,5	3,5	3,4	3,9	**% personen vanaf 15 jaar**	
melding totaal	40,9	39,1	39,8	39,7	**% van ondervonden delicten**	
melding bij politie	24,2	23,4	23,6	23,5	**% van ondervonden delicten**	
aangifte totaal	20,1	20,0	20,2	19,0	**% van ondervonden delicten**	
hacken totaal	7,9	7,6	7,4	7,5	**per 100 inwoners**	
slachtoffers	5,2	5,1	4,9	4,9	**% personen vanaf 15 jaar**	
melding totaal	18,8	18,4	20,4	20,0	**% van ondervonden delicten**	
melding bij politie	4,9	4,3	5,3	5,1	**% van ondervonden delicten**	
aangifte totaal	1,8	1,8	2,3	2,7	**% van ondervonden delicten**	
cyberpesten totaal	6,0	6,3	6,0	6,1	**per 100 inwoners**	
slachtoffers	3,1	3,2	3,2	3,1	**% personen vanaf 15 jaar**	
melding totaal	23,1	23,9	22,1	22,6	**% van ondervonden delicten**	
melding bij politie	15,1	15,2	14,8	14,5	**% van ondervonden delicten**	
aangifte totaal	5,4	6,4	4,9	5,7	**% van ondervonden delicten**	
Computervredebreuk						
Geregistreerde misdrijven	2045	2225	1875	2300	**aantal**	CBS
Geregistreerde misdrijven, relatief	0,2	0,2	0,2	0,3	**% van totaal geregistreerde misdrijven**	
Geregistreerde misdrijven per 1 000 inwoners	0,1	0,1	0,1	0,1	**per 1 000 inwoners**	
Opgehelderde misdrijven	195	165	160	105	**aantal**	CBS
Opgehelderde misdrijven, relatief	9,5	7,4	8,6	4,6	**% van geregistreerde misdrijven**	
Registraties van verdachten	235	195	210	220	**aantal**	CBS

[1] Antivirussoftware, Sterke wachtwoorden, Identificatie en authenticatie gebruikers, Encryptie (opslag), Encryptie (versturen), Offsite data-back-up, Network access control, VPN, Log-bestanden, Veiligheidstests, Risocoanalyses, Andere maatregelen.

[2] Computer (PC, desktop, laptop, notebook, tablet) of smartphone of mobiele telefoon voor privé-doeleinden met bijv. antivirus- of anti-spamprogramma's en/of firewall.

[3] Bestanden voor privé-gebruik zoals foto's, video's, privé-documenten of andere bestanden.

[4] Per 30-6. 52 procent per 30-6-2018.

[5] Bij de Autoriteit Persoonsgegevens, een financiële instelling, de politie (aangifte) of een sectoraal, nationaal of ander securityteam.

[6] Heeft betrekking op de bij de NBIP aangesloten internetproviders die gebruikmaken van de Nationale anti-DDoS Wasstraat (NaWas). 2016: periode 1-7 tot en met 14-12.

[7] In het onderzoek is naar een gelimiteerd aantal typen cybercrimedelicten gevraagd (identiteitsfraude, hacken, koop- en verkoopfraude, cyberpesten).

1. Waarom een cybersecuritymonitor?

Anno 2018 leven we in een informatiesamenleving: een samenleving waar in toenemende mate via informatie- en communicatietechnologie (ICT) wordt gecommuniceerd en grote hoeveelheden informatie[1] – al dan niet bedoeld – digitaal worden vastgelegd. Het is een samenleving waarin plan B ook niet altijd meer beschikbaar is. Als er ICT-systemen om wat voor reden dan ook uitvallen kan er niet altijd zo maar overgeschakeld worden op de oude manier van doen. ICT is daarvoor inmiddels te alom aanwezig en te cruciaal.

Privacy en veiligheid van elektronisch dataverkeer en -opslag en alles wat daarbij hoort, is de laatste jaren erkend als een potentiële bedreiging voor de ontwikkelingsmogelijkheden van de informatiesamenleving. Veel activiteiten van bedrijven, overheden en personen laten digitale sporen na. Is dit altijd bekend? Worden deze gegevens wel zorgvuldig behandeld? Is alle dataverkeer beveiligd? En zijn bedrijfsgegevens wel voldoende beschermd, en onbereikbaar voor derden? Kortom: zijn de vertrouwelijkheid en de integriteit van de informatie en de authenticiteit en beschikbaarheid van de ICT-systemen wel voldoende gewaarborgd?

Ook in de media wordt regelmatig aandacht besteed aan cybersecurity. Staten blijken elkaar te bespioneren via internet. Bedrijven zijn slachtoffer van *ransomware*. Personen worden opgelicht via internet. Kinderen pesten elkaar via internet. Er verschijnt 'nepnieuws' op internet. Er ontstaat zelfs een heuse bedrijfstak cybercrime die op bestelling cybercrimediensten levert (DDoS-aanvallen, *exploitkits*[2]). Het speelveld is mondiaal. Een ouderwetse inbreker moet nog fysiek in Nederland zijn om in Nederland te kunnen inbreken. Voor een hacker geldt dit niet.

Dit soort praktijken, van het plegen van strafbare feiten tot zaken die niet per se strafbaar zijn maar wel het vertrouwen in bijvoorbeeld internet ondergraven, kunnen ertoe leiden dat bedrijven, overheden en burgers internet de rug toekeren of het maar beperkt gebruiken. Daartegenover staan nieuwe wettelijke maatregelen om de internetgebruiker meer rechtsbescherming te geven, en de politie meer opsporingsmogelijkheden te bieden én de ICT-middelen en procedures om het gebruik van ICT-systemen zo veilig mogelijk te maken. Ook dit soort maatregelen kunnen de gebruiksmogelijkheden of het gebruiksgemak van bijvoorbeeld internet beperken en daardoor een belemmering vormen om optimaal gebruik te kunnen maken van de (technische) mogelijkheden van internet en ICT in het algemeen. Het is een delicate balans tussen vrijheid in het ICT-gebruik en bescherming van gebruikers en informatie.

Tegen deze achtergrond is bij het CBS de wens ontstaan om cybersecurity in nauwe samenwerking met andere partijen te definiëren en te meten. Hoe erg is het nu? Hoeveel bedrijven, overheden en burgers zijn slachtoffer van cybercrime? Wat zijn dan de dreigingen? En wat doen we er eigenlijk tegen? Deze publicatie is een tweede proeve van een cybersecuritymonitor. Er is een aantal indicatoren samengebracht die iets zeggen over de verschillende aspecten van cybersecurity. De monitor geeft zeker nog geen volledig en evenwichtig beeld, maar moet gezien worden als een eerste stap.

[1] De term informatie wordt hier in ruime zin gehanteerd. In principe is alles wat in gedigitaliseerde vorm opgeslagen, verwerkt en verspreid kan worden informatie (Shapiro en Varian, 2000).

[2] Hulpmiddel om een aanval op te zetten door te kiezen uit kant- en klare *exploits*, in combinatie met gewenste gevolgen en besmettingsmethode. Een *exploit* is software, gegevens of opeenvolging van commando's die gebruikmaken van een kwetsbaarheid in software of hardware om ongewenste functies en/of gedrag te veroorzaken.

2. Hoe te komen tot een cybersecuritymonitor?

Er is niet een eensluidende definitie van cybersecurity en aanverwante begrippen. Het CBS heeft ook niet de ambitie om de standaarden op dit terrein op dit moment te zetten. Er is gekozen voor een praktische benadering: het bieden van een raamwerk waarin de verschillende aspecten van cybersecurity gepositioneerd kunnen worden. Met behulp van dit raamwerk kunnen geselecteerde indicatoren gecategoriseerd worden en kan gerichter gezocht worden naar nieuwe indicatoren op terreinen waarvoor het aantal indicatoren nog te gering is.
Er is gekozen voor abstracte en (dus) veelomvattende begrippen die naar verwachting hun houdbaarheid zullen behouden. Wat er wel en niet onder valt kan met behulp van actuele – dus wisselende – voorbeelden worden geïllustreerd. De omgekeerde weg zou zijn om van onderop een uitputtende opsomming te geven van alle mogelijke cybercrimedelicten, cybersecuritymaatregelen en -dreigingen voor zover we die nu kennen, en deze vervolgens te categoriseren. Dit lijkt een moeizamere en tijdrovender weg. Daar komt bij dat het niet zo eenvoudig zal zijn om het 'totaal aan cybercrime' of het 'totaal aan cybersecuritymaatregelen' te kwantificeren. Bijvoorbeeld omdat de verschillende cybersecuritymaatregelen niet optelbaar zijn. Vergelijk het met de omzet van een bedrijf: voor hoeveel euro heeft uw bedrijf goederen en diensten verkocht aan derden? Deze vraag is voor elk bedrijf te beantwoorden, ongeacht om welke goederen en diensten het gaat. Een dergelijk equivalent van een begrip als omzet lijkt er voor cybercrime of cybersecurity vooralsnog niet te zijn; hoewel er wel vraag is naar de totale schade van cybercrime uitgedrukt in geld en bijvoorbeeld de totale uitgaven aan cybersecurity door bedrijven.
De gekozen werkwijze om te komen tot relevante indicatoren is het bijvoorbeeld in een enquête formuleren van een delict op het terrein van cybercrime – zoals oplichting via internet – en het geven van actuele voorbeelden daarbij (oplichting door webwinkels, via online handelsplaatsen, datingsites). De verwachting is dat oplichting via internet voorlopig nog wel zal blijven bestaan, maar dat de manier waarop dat gebeurt, kan veranderen. Dit laatste wordt dan ondervangen door het aanpassen van de voorbeelden. Een ander voorbeeld is het kwantificeren van een erkende beveiligingsmaatregel op het terrein van cybersecurity, bijvoorbeeld het aantal websites in het .nl-domein dat gebruikmaakt van DNSSEC[1]. Het gebruik hiervan wordt op dit moment door de overheid gestimuleerd, maar kan op enig moment bijna honderd procent zijn of worden ingehaald door een beter alternatief. In beide gevallen moet dan overwogen worden over te stappen op een andere – relevantere – indicator.
Het punt is hier dat het uit de aard van de zaak – namelijk snel veranderende cybercrimedelicten, dreigingen en maatregelen – moeilijk zal zijn over een langere periode te kunnen volstaan met een vaste set van indicatoren. Dit ondergraaft enigszins het karakter van een monitor, maar dit lijkt vooralsnog onvermijdelijk. Het monitoren heeft dus deels betrekking op het in de tijd kwantitatief beschrijven van het fenomeen cybersecurity aan de hand van wisselende indicatoren. Desalniettemin zal geprobeerd worden een beperkte set kernindicatoren te definiëren die door de jaren heen relevant blijft en op consistente wijze kan worden waargenomen.
In het vervolg zal de geschetste werkwijze concreter worden toegelicht en uitgewerkt.

[1] DNS Security Extensions (DNSSEC) is een uitbreiding op DNS met een extra authenticiteits- en integriteitscontrole. DNS is het Domain Name System dat internetdomeinnamen koppelt aan IP-adressen en omgekeerd.

2.1 Begripsvorming rondom cybersecurity

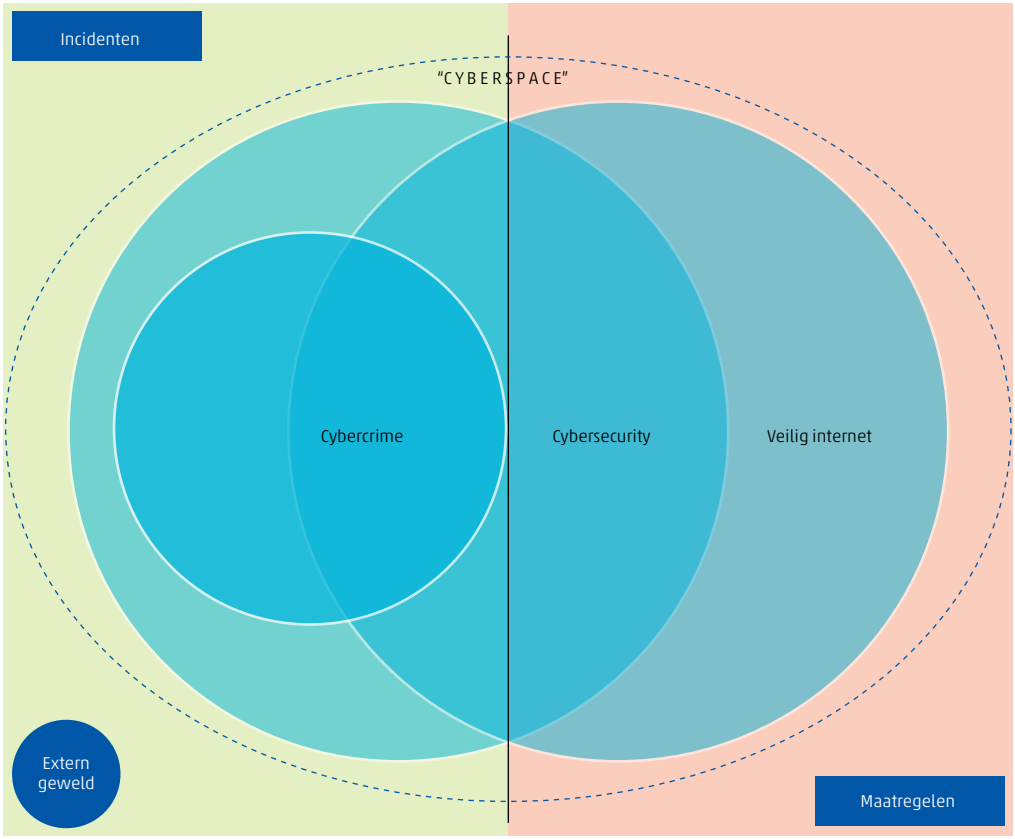
In schema 2.1.1 is met een aantal domeinen getracht structuur aan te brengen in de wereld van de cybersecurity. Zoals gezegd is het doel vooral de verschillende begrippen ten opzichte van elkaar te positioneren en de geselecteerde en nog te selecteren indicatoren op die manier onder te kunnen brengen in een van de onderscheiden domeinen. Het bereik van hetgeen in schema 2.1.1 is weergegeven is redelijk groot. Cybercrime is eigenlijk het kleinste domein, namelijk alle strafbare en moedwillig gepleegde cyberdelicten. Cybercrime is hiermee een deelverzameling van cybersecurity. Er vinden immers ook incidenten plaats die onbedoeld zijn en ook niet per se strafbaar, zoals het tijdelijk uitvallen van een systeem door een verkeerde software-installatie of het onbedoeld lekken van vertrouwelijke gegevens door het laten slingeren van een USB-stick. Daarnaast omvat cybersecurity ook uitdrukkelijk alle preventieve maatregelen van burgers, bedrijven en organisaties om hun ICT-systemen minder kwetsbaar te maken. Dit kunnen ICT-technische maatregelen zijn maar even zo goed organisatorische, procedurele en personele maatregelen.
Ten slotte is er ook nog zoiets als veilig internet. Niet alles wat via internet tot ons komt, is ons altijd even welgevallig. Iedereen kan zich op internet uiten. Hier gaat het om het sentiment dat er om internet heen hangt en dat er soms voor zorgt dat burgers, bedrijven en organisaties hun internetgebruik beperken of het zelfs de rug toekeren. Denk bijvoorbeeld aan de inspanningen van ouders om hun kinderen te vrijwaren van onwelgevallige content, en de systematische wijze waarop 'ons' internetgebruik door bepaalde partijen wordt gevolgd en vastgelegd.
In het volgende zijn in de boxjes in de tekst de kernbegrippen gedefinieerd en toegelicht. Dit is met name bedoeld om enige structuur in de indicatoren aan te kunnen brengen en een idee te geven van wat er in deze publicatie onder de genoemde begrippen moet worden verstaan. Het is zeker niet zo dat hier het laatste woord over is gezegd. Zowel op het terrein van dataverzameling als op het terrein van definities en classificaties is cybersecurity nog een nieuw vakgebied.

Wat is 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 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.

2.1.1 Contextdiagram cybersecurity en gerelateerde begrippen



Cybercrime bevindt zich in schema 2.1.1 letterlijk en figuurlijk aan de verkeerde kant van de streep. Het kwaad is al geschied. De preventieve maatregelen hebben hun doel gemist. Daarnaast heeft cybercrime een juridische dimensie. Het betreft in aanleg strafbare feiten (delicten). Het plegen van cybercrime gebeurt dan ook doelbewust. Voorbeelden van cybercrime zijn: het schenden van de integriteit (hacken, *malware* verspreiden e.d.) en het tijdelijk onklaar maken of het overnemen van de controle van ICT-systemen. Vaak is zo'n delict ook een eerste stap naar een vervolgdelict. Door hacken verkrijg je iemands identiteits- of inloggegevens waarmee vervolgens een ander delict wordt gepleegd, bijvoorbeeld onrechtmatige (financiële) transacties. Uiteindelijk zijn het wel altijd personen, bedrijven en organisaties die slachtoffer zijn van cybercrime. Oplichting, fraude, chantage en bedreiging via internet of andere ICT-systemen zijn andere voorbeelden van cybercrime. Dit zijn niet zo zeer nieuwe delicten maar ze hebben door internet en sociale media een nieuw platform gekregen met een enorm bereik en dus een grotere potentiële impact. Deze laatste groep delicten is in de door de politie geregistreerde criminaliteit maar ook in de door het CBS gehanteerde classificatie nog niet altijd apart terug te vinden. Kinderporno via internet wordt bijvoorbeeld nog vaak geregistreerd als zedendelict, terwijl onvermeld blijft dat het delict via internet is gepleegd.

Wat is cyber secure?

Het vrij zijn van gevaar of schade veroorzaakt door verstoring of uitval van ICT of door misbruik van ICT. Het gevaar of de schade door misbruik, verstoring of uitval kan bestaan uit beperking van de beschikbaarheid en betrouwbaarheid van de ICT, schending van de vertrouwelijkheid van in ICT opgeslagen informatie of schade aan de integriteit van die informatie (Bron: NCSC, 2016).

Cyber secure zoals hier gedefinieerd is in feite de ideale situatie. In deze publicatie wordt onder cybersecurity verstaan: het streven naar deze ideale situatie. Dit betekent dat cybersecurity alle maatregelen omvat die bijdragen aan het bereiken van de ideale situatie. Cybersecurity – of eigenlijk het ontbreken ervan – omvat echter ook het tekortschieten van deze maatregelen of het ontbreken van maatregelen. Deze laatste twee situaties kunnen zich manifesteren in de vorm van incidenten.

Bij cybersecurity ligt de focus op de ICT-systemen zelf: het beschermen van de ICT-systemen en de daarin opgeslagen informatie tegen misbruik. In tegenstelling tot cybercrime gaat het hier vooral over de te treffen maatregelen om misbruik tegen te gaan en de kans op onbedoelde incidenten te verkleinen. Dit zijn deels ICT-technische maatregelen, zoals *firewalls*, antivirussoftware en het gebruik van erkende beveiligingsprotocollen bij elektronisch dataverkeer (DNSSEC, TLS). Deels zijn dit ICT-organisatorische maatregelen, bijvoorbeeld de doorlooptijd van het repareren van kwetsbaarheden in de software (een *patch*), het gebruik van wachtwoorden en andere procedures om toegang te krijgen tot een ICT-systeem. Ten slotte zijn dit ook maatregelen die erop gericht zijn om burgers en werknemers van bedrijven en organisaties alerter te maken op misbruik, zoals het vergroten van de kennis en de bewustwording op het terrein van cybersecurity en het aanreiken van makkelijk te implementeren maatregelen of gedragingen. Niet zelden blijkt de mens immers nog de (zwakke) schakel in de keten om tot een ICT-systeem door te dringen (*social engineering*).

Wat is cyberspace?

Cyber security shall refer to security of cyberspace, where cyberspace itself refers to the set of links and relationships between objects that are accessible through a generalised telecommunications network, and to the set of objects themselves where they present interfaces allowing their remote control, remote access to data, or their participation in control actions within that cyberspace.

Bron: ENISA, *Definition of Cybersecurity, V1.0*, December 2015.

Het begrip cyberspace wordt gehanteerd om aan te geven dat het speelveld van cybercrime en cybersecurity meer is dan het 'zichtbare' internet. Uiteindelijk zullen apparaten in toenemende mate met elkaar verbonden zijn en wordt het dus ook mogelijk ICT-systemen vanuit talloze aangesloten *devices* binnen te dringen. Een voorbeeld is *skimming* waarbij een pinpas wordt uitgelezen, de bijbehorende inlogcode wordt bemachtigd en vervolgens onrechtmatige financiële transacties worden verricht. Uiteindelijk zullen kwaadwillende via thermostaten, koelkasten en auto's toegang kunnen krijgen tot ICT-systemen én andersom (*Internet of Things*).
In verschillende beschouwingen over cybersecurity (o.a. ENISA, 2016) wordt ook expliciet de aandacht gevestigd op dreigingen van buiten cyberspace. Niet alle mogelijke dreigingen komen vanuit cyberspace of zijn te kwader trouw. Met name de beschikbaarheid van ICT-systemen kan ook verstoord worden door bijvoorbeeld elektriciteitsuitval of omgewaaide zendmasten. Uiteindelijk hebben deze verstoringen eenzelfde effect als een hack of een DDoS-aanval, namelijk het tijdelijk niet beschikbaar zijn van de dienst, met alle gevolgen van dien.

Het voorgaande beoogt te illustreren dat het nogal wat tijd zal vergen om voor alle begrippen uitputtend vast te stellen wat er wel en niet toe gerekend moet worden. Terwijl we aan de andere kant weten dat we er niet direct in zullen slagen het totaal aan cybersecurity te meten. In deze tweede CBS-publicatie over cybersecurity wordt voor de verschillende domeinen een handvol indicatoren gepresenteerd. Die zeggen dan wel niet alles, maar in ieder geval iets over cybersecurity.

2.2 Op zoek naar indicatoren

Bij het zoeken naar indicatoren wordt in eerste instantie gekeken naar de relevantie van de indicator: zegt de indicator iets over het te beschrijven fenomeen? Daarna is gekeken naar een aantal aanvullende (statistische) criteria:

1. Validiteit: meet een indicator wat deze moet meten?
2. Objectiviteit: is een indicator gebaseerd op feiten?
3. Tijdigheid: hoe snel is een indicator beschikbaar na afloop van de meetperiode?
4. Beschikbaarheid van tijdreeksen: is een indicator periodiek voorhanden?
5. Transparantie: is het duidelijk hoe een indicator tot stand is gekomen?
6. Onafhankelijkheid: heeft de samensteller van de indicator geen belangen bij de uitkomsten?

Een deel van de indicatoren komt uit bestaande CBS-statistieken. Dit zijn met name statistieken over personen en bedrijven. Daarnaast zijn er op het terrein van de ICT-technische cybersecuritymaatregelen en -dreigingen indicatoren geselecteerd die door andere partijen dan het CBS worden samengesteld. Hierbij wordt aansluiting gezocht bij partijen die een duidelijke rol vervullen in het faciliteren van de ICT-infrastructuur van Nederland en de werking ervan, die geen uitgesproken belang hebben, én over concrete data (kunnen) beschikken. SIDN is hier een voorbeeld van, maar ook de Autoriteit Persoonsgegevens.
Op internet en in rapporten van verschillende bedrijven en onderzoeksinstellingen zijn wel gegevens te vinden over cybersecurity. Deze informatie is echter veelal op mondiaal niveau (niet apart voor Nederland bijvoorbeeld), komt vaak van ICT-beveiligingsbedrijven en is zelden transparant. In algemene zin is het moeilijk een oordeel te vellen over de kwaliteit en representativiteit van deze gegevens (zie ook de box aan het eind van deze paragraaf).
Daarnaast ligt het voor de hand dat het CBS een toegevoegde waarde heeft bij het verzamelen en presenteren van data over cybersecurity. Alleen het samenbrengen van bestaande data is weliswaar nuttig, maar niet genoeg. Op de eerste plaats beschikt het CBS over eigen statistieken waarin aan cybersecurity gerelateerde zaken zijn opgenomen. Er zijn altijd zaken die niet op een andere wijze kunnen worden verkregen dan via een klassieke enquête. Ten tweede beschikt het CBS over de (wettelijke) mogelijkheid data van derden op te vragen die bewerkt kunnen worden en vaak ook gekoppeld kunnen worden aan andere gegevens van het CBS, waardoor meer of gedetailleerdere informatie beschikbaar komt. Ten slotte worden de verkregen gegevens uitsluitend voor statistische doeleinden gebruikt en alleen in geaggregeerde vorm gepubliceerd. Het CBS kan dus zeker een rol vervullen bij het verzamelen en ontsluiten van data over cybersecurity.

Om te illustreren dat er nog een lange weg te gaan is om te komen tot eenduidige begrippen en transparante gegevens op het terrein van cybersecurity is in onderstaande box een conclusie overgenomen uit een onderzoek naar de beschikbaarheid van gegevens over cybersecurity. Deze inventarisatie is in opdracht van The Hague Centre for Strategic Studies samengesteld (HCSS, 2015). Hiertoe zijn 70 rapporten vanuit verschillende sectoren van de samenleving bestudeerd.

General recommendations

The picture that emerges from our meta-assessment of cyber threat analyses is one where it has become difficult to see the forest for the trees. There clearly are a lot of reports around, but these are based on definitions and methods that are difficult to compare. In addition, these reports (and we may add: at least parts of this meta-assessment) require a level of expertise not available to the layman. We close our report with four recommendations. If we want to provide a more encompassing and comparable assessment of cyber threats, and increase awareness thereof, we should:

- **In line with emerging efforts on the international level, develop shared, commonly agreed definitions, metrics, and reporting standards to enhance threat assessments, allowing for more targeted investments in cyber security, on both company and government level.**
- **Anticipate trends and developments at an early stage to include potential new threats.**
- **Develop evidence based cyber security policies in line with evidence obtained via data and indicators, rather than subjective perceptions.**
- **Consider setting up a mechanism to harmonize the collection and reporting of cyber statistics.**

Source: The Hague Centre for Strategic Studies, 2015. *Assessing cyber security, A meta-analysis of threats, trends, and responses to cyber attacks*

Zeker voor een eerste verkenning van de mogelijkheden om te komen tot een statistische beschrijving van cybersecurity is er ook sprake van enig pragmatisme; er kan alleen maar gekozen worden uit bestaande indicatoren. De selectie van indicatoren voor deze publicatie heeft geleid tot 24 indicatoren waarvan 20 afkomstig van het CBS en 4 van andere partijen. Deze indicatoren worden in drie hoofdstukken gepresenteerd. Zestien indicatoren in het domein cybersecurity waarvan negen betreffende de preventieve maatregelen (hoofdstuk 3) en zeven met betrekking tot incidenten (hoofdstuk 4). De resterende acht indicatoren vallen in het domein cybercrime en worden in hoofdstuk 5 gepresenteerd.

3. Cybersecurity, maatregelen

3.1.1 Cybersecurity, maatregelen

Indicator	2014	2015	2016	2017	Eenheid	Bron
ICT-beveiliging en bescherming van data door bedrijven	88	85	86	.	**% bedrijven met 10 of meer werkzame personen**	CBS
	.	.	64		**% bedrijven met 2 tot 10 werkzame personen**	
voornamelijk uitgevoerd door eigen personeel	26	26	33	.	**% bedrijven met 10 of meer werkzame personen met ICT-beveiliging**	
	.	.	40		**% bedrijven met 2 tot 10 werkzame personen met ICT-beveiliging**	
voornamelijk uitgevoerd door externe leverancier(s)	74	74	67	.	**% bedrijven met 10 of meer werkzame personen met ICT-beveiliging**	
	.	.	60		**% bedrijven met 2 tot 10 werkzame personen met ICT-beveiliging**	
Bedrijven die gebruikmaken van betaalde clouddiensten	28	.	35	.	**% bedrijven met 10 of meer werkzame personen**	CBS
op gedeelde servers en/of	64	.	74	.	**% bedrijven met clouddiensten**	
servers uitsluitend gereserveerd voor het bedrijf	39	.	49	.	**% bedrijven met clouddiensten**	
Bedrijven die om veiligheidsredenen niet of maar beperkt via een website/app verkopen	.	.	19	.	**% bedrijven met 10 of meer werkzame personen**	CBS
Bedrijven met drie of meer ICT-veiligheidsmaatregelen[1]						CBS
	.	.	.	81	**% bedrijven met 10 of meer werkzame personen**	
	.	.	.	60	**% bedrijven met 2 tot 10 werkzame personen**	
Uitvoeren van software-updates (security-patches) door bedrijven						
meestal volledig automatisch	.	.	.	51	**% bedrijven met 10 of meer werkzame personen**	CBS
	.	.	.	47	**% bedrijven met 2 tot 10 werkzame personen**	
meestal (deels) handmatig	.	.	.	33	**% bedrijven met 10 of meer werkzame personen**	
	.	.	.	24	**% bedrijven met 2 tot 10 werkzame personen**	
niet van toepassing	.	.	.	17	**% bedrijven met 10 of meer werkzame personen**	
	.	.	.	29	**% bedrijven met 2 tot 10 werkzame personen**	
Verandert instellingen browser om cookies tegen te gaan of te verminderen	.	36	34	.	**% personen vanaf 12 jaar**	CBS
Mijn computer is voorzien van beveiligingssoftware[2]						CBS
ja				89	**% personen vanaf 12 jaar met een computer**	
weet niet				7		
Mijn smartphone of mobiele telefoon is voorzien van beveiligingssoftware[2]						
ja				52	**% personen vanaf 12 jaar met een smartphone of mobiele telefoon**	
weet niet				24		
Maakt gebruik van clouddiensten voor opslag van bestanden[3]	31	34	40	46	**% personen vanaf 12 jaar**	CBS
Maakt gebruik van betaalde clouddiensten voor opslag van bestanden[3]	3	4	6	8	**% personen vanaf 12 jaar**	
Websites in het .nl-domein die gebruikmaken van DNSSEC[4]	32	44	44	47	**% van .nl domeinnamen**	SIDN

[1] Antivirussoftware, Sterke wachtwoorden, Identificatie en authenticatie gebruikers, Encryptie (opslag), Encryptie (versturen), Offsite data-back-up, Network access control, VPN, Log-bestanden, Veiligheidstests, Risocoanalyses, Andere maatregelen.

[2] Computer (PC, desktop, laptop, notebook, tablet) of smartphone of mobiele telefoon voor privé-doeleinden met bijv. antivirus- of anti-spamprogramma's en/of firewall.

[3] Bestanden voor privé-gebruik zoals foto's, video's, privé-documenten of andere bestanden.

[4] Per 30-6. 52 procent per 30-6-2018.

In tabel 3.1.1 zijn maatregelen opgesomd die bedrijven en personen nemen om incidenten op het terrein van cybersecurity te voorkomen. Deze maatregelen variëren van het nemen van ICT-beveiligingsmaatregelen tot het aanpassen van het internetgedrag omdat men zaken niet vertrouwd. Ook het gebruik van clouddiensten door bedrijven en personen is opgenomen onder het domein cybersecuritymaatregelen.

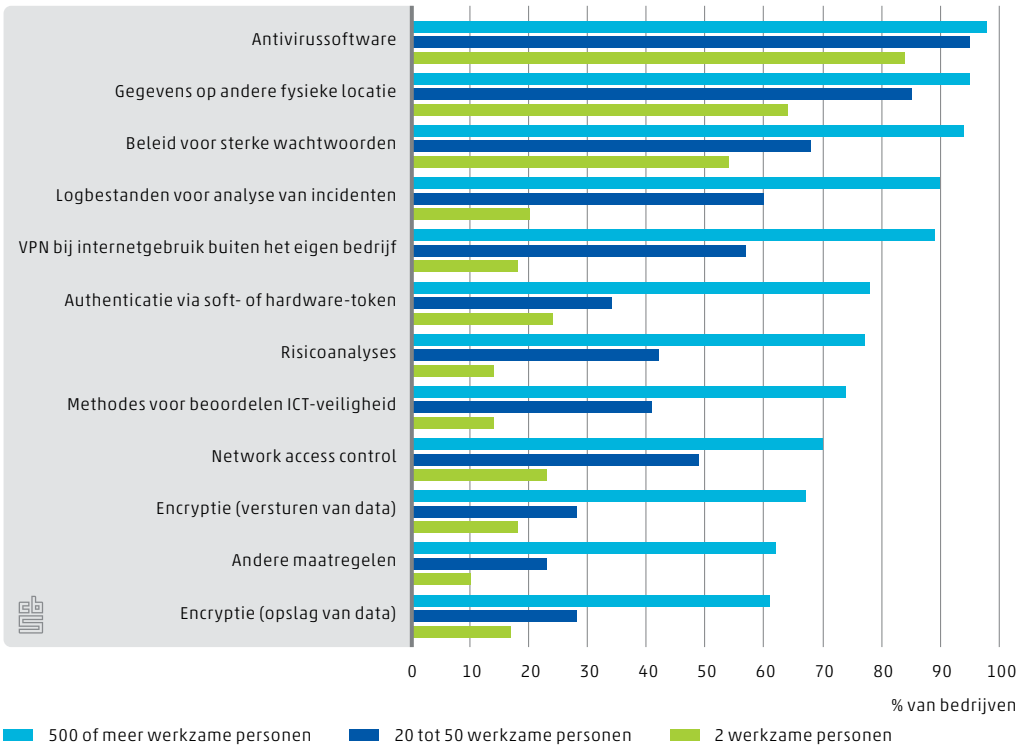
3.1 Bedrijven

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.

Grotere bedrijven nemen meer ICT-veiligheidsmaatregelen

In figuur 3.1.2 wordt gekeken naar het type beveiligingsmaatregelen dat door de bedrijven genomen is. In het algemeen geldt dat het ICT-beveiligingsniveau van een bedrijf hoger is naarmate er meer maatregelen tegelijkertijd genomen worden. Het is duidelijk te zien dat voor alle maatregelen grote bedrijven beter scoren dan kleine bedrijven. Deze trend is consistent voor alle grootteklassen (zie tabel A3.1 achterin de publicatie). Uiteraard hebben grotere bedrijven vaak ook een grotere en complexere ICT-infrastructuur en derhalve is er een breder scala aan beveiligingsmaatregelen nodig om het bedrijf cybersecure te houden. Antivirussoftware en het opslaan van gegevens op een andere fysieke locatie (offsite data-backup) zijn de meest voorkomende maatregelen. Het gebruik van dataencryptie bij zowel de opslag van data als het versturen van data, komt nog maar bij een minderheid van de bedrijven voor (zie tabel A3.1 in de annex).
In tabel 3.1.1 is te zien dat 60 procent van de bedrijven met 2 tot 10 werkzame personen drie of meer van de genoemde ICT-veiligheidsmaatregelen heeft genomen. Voor de bedrijven met 10 of meer werkzame personen geldt dit voor 81 procent.

3.1.2 Gebruikte ICT-veiligheidsmaatregelen bedrijven, 2017



Verschillen tussen bedrijfstakken

Per bedrijfstak bekeken nemen bedrijven in de horeca, de bouw en de handel en verhuur van onroerend goed wat minder ICT-veiligheidsmaatregelen en de bedrijven in de informatie- en communicatiesector en de financiële sector wat meer (zie ook tabel A3.1). Dit lijkt een plausibel beeld. Bedrijfstakken waarvan verwacht mag worden dat informatiebeveiliging en beveiliging van de ICT-systemen een grote rol spelen, scoren ook het hoogst op de hier genoemde maatregelen. Bedrijven maken overigens verschillende afwegingen bij de vraag welke maatregelen genomen moeten worden. Net als voor ICT-gebruik in het algemeen geldt ook voor ICT-beveiliging dat de lat niet voor elk bedrijf even hoog gelegd hoeft te worden. Intuïtief lijkt het rationeel dat financiële instellingen meer werk maken van ICT-beveiliging dan bijvoorbeeld een horecaonderneming. Hetzelfde geldt voor kleinere bedrijven ten opzichte van grotere bedrijven.

Meeste bedrijven besteden ICT-beveiligingswerk uit

In 2016 was er bij 86 procent van de bedrijven met 10 of meer werkzame personen sprake van aanwijsbare werkzaamheden op het terrein van ICT-beveiliging en de bescherming van data. In twee derde (67 procent) van de gevallen werd dit werk voornamelijk uitgevoerd door externe leveranciers. Bij bedrijven met 2 tot 10 werkzame personen was er bij 64 procent van de bedrijven sprake van ICT-beveiligingswerk. Dit werd in 60 procent van de gevallen voornamelijk uitgevoerd door externe leveranciers. Hoewel een bedrijf formeel verantwoordelijk blijft voor zijn eigen ICT-beveiliging

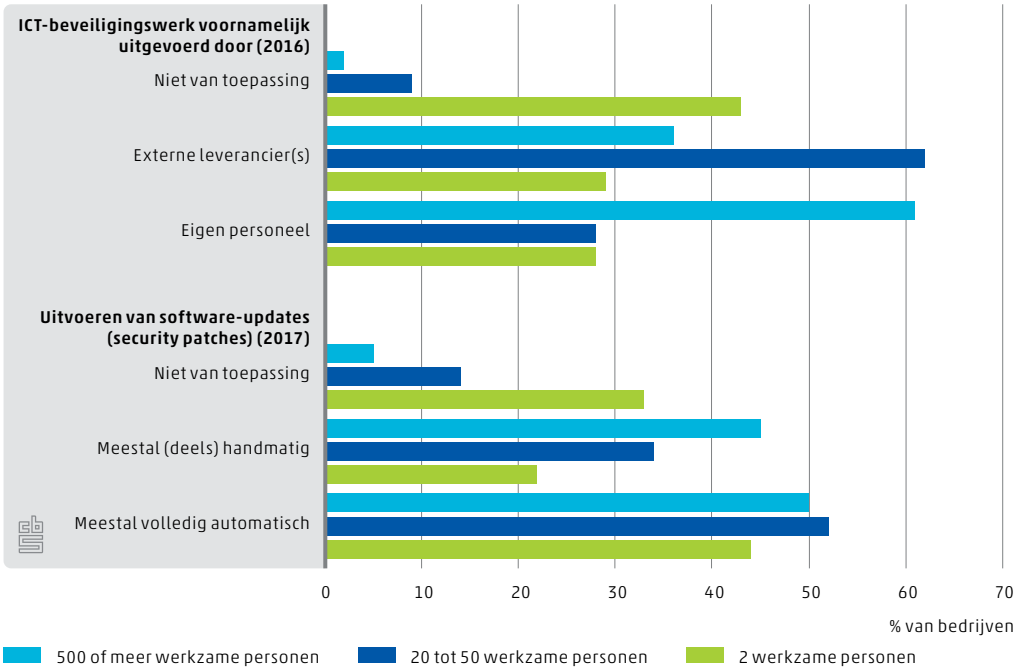
legt deze grootschalige uitbesteding ook een verantwoordelijkheid bij de bedrijven aan wie dit werk is uitbesteed (zie ook tabel A3.2 achter in deze publicatie).
In figuur 3.1.3 is voor de kleinste, middelgrote en grootste bedrijven te zien wie de ICT-beveiliging uitvoert: eigen personeel of een externe leverancier. Weer is te zien dat het overgrote deel van de middelgrote en grote bedrijven een vorm van ICT-beveiliging heeft. Van de grootste bedrijven kiest 63 procent ervoor om dit werk voornamelijk zelf te doen, terwijl de meeste (69 procent) middelgrote bedrijven dit juist uitbesteden aan externe leveranciers. Ook dit hangt waarschijnlijk weer samen met het feit dat grote bedrijven vaker eigen ICT-experts in dienst zullen hebben die de beveiliging grotendeels ook zelf uit kunnen voeren.
Bij de kleinste bedrijven geeft een relatief groot percentage van de bedrijven aan geen uitgesproken ICT-beveiligingswerk te kennen (43 procent van de bedrijven).
Voor de kleinste bedrijven die wel een vorm van ICT-beveiliging hebben doet de helft (49 procent) het zelf en de andere helft (51 procent) besteedt het uit. Middelgrote bedrijven besteden het ICT-beveiligingswerk dus vaker uit dan kleine bedrijven. Bij het merendeel van de kleinere bedrijven beperkt de ICT-beveiliging zich tot het installeren van een virusscanner en het gebruik van veilige wachtwoorden; dit kan inderdaad vaak zelf gedaan worden. Kennelijk is er een omslagpunt van vaker zelf doen (weinig ICT-beveiligingswerk, niet te complex, geen financiële middelen om het uit te besteden) naar relatief vaker uitbesteden (meer ICT-beveiligingswerk, complexer, wel financiële middelen). Dit omslagpunt lijkt te liggen bij bedrijven met 10 tot 20 werkzame personen (zie tabel A3.2 in de annex).
Overigens geldt alleen voor de bedrijven vanaf 100 of meer werkzame personen dat de meerderheid het ICT-beveiligingswerk zelf doet. Per bedrijfstak bekeken geldt dit alleen voor de informatie- en communicatiesector (76 procent) (zie tabel A3.2).
Bij de organisatie van het ICT-beveiligingswerk komt de belangrijke rol van externe leveranciers van ICT-beveiligingssoftware en aanverwante kennis en kunde voor de (kleinere) bedrijven naar voren. Het overgrote deel van de bedrijven heeft dit werk uitbesteed aan derden. Dit kan een voordeel zijn. Als de bedrijven die deze ICT-beveiliging verzorgen dit goed doen, dan is het – via hen – voor een groot aantal bedrijven ook goed geregeld.

Security-patches meestal automatisch

Een tweede onderdeel van de organisatie van ICT-beveiligingswerk is het uitvoeren van software-updates (security-patches). Het updaten van software betreft zeker niet alleen beveiligingssoftware. Het komt maar al te vaak voor dat er kwetsbaarheden voorkomen in besturingssoftware of andere operationele software waar cybercriminelen misbruik van zouden kunnen maken. Het tijdig uitvoeren van security updates binnen een bedrijf is een goede indicator van het cybersecurityniveau van een bedrijf. Figuur 3.1.3 laat zien dat de meeste van middelgrote en grote bedrijven een security update-beleid hebben. Het valt op dat grote bedrijven dit relatief vaker handmatig uitvoeren (47 procent). Middelgrote bedrijven kiezen er vaker voor om dit automatisch te doen (60 procent). 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. Bij de kleinste bedrijven worden security updates minder vaak toegepast (67 procent heeft een security update-beleid). Van de kleinste bedrijven die wel security updates toepassen doet de meerderheid dat automatisch (67 procent).

Per bedrijfstak bekeken voeren de bedrijven in de informatie- en communicatiesector security-patches het vaakste deels handmatig uit (45 procent). Voor alle bedrijfstakken en -grootteklassen geldt echter dat de meerderheid van de bedrijven met een security update-beleid deze updates automatisch doorvoert (zie tabel A3.2).

3.1.3 Organisatie ICT-beveiliging; security patches (2017) en ICT-beveiligingswerk (2016)



Bron: CBS, ICT-gebruik bedrijven.

Gebruik van clouddiensten

In 2016 maakte een op de drie (35 procent) bedrijven met 10 of meer werkzame personen gebruik van betaalde clouddiensten. Driekwart (74 procent) van deze bedrijven maakte hierbij gebruik van gedeelde servers. De helft (49 procent) maakte hierbij (ook) gebruik van servers uitsluitend gereserveerd voor het bedrijf. Bedrijven kunnen gebruikmaken van beide opties afhankelijk van de dienst die ze afnemen. Zo kan een bedrijf voor e-mailverkeer en dataopslag gebruikmaken van een eigen server, maar voor het gebruik van *office software* van een gedeelde server. In 2014 maakte nog maar 28 procent van de bedrijven gebruik van clouddiensten waarvan 39 procent (ook) van een eigen server. Beide percentages zijn dus toegenomen.

Aanpassen gedrag

Een bijzondere cybersecuritymaatregel is het aanpassen van het gedrag onder invloed van ICT-beveiligingsrisico's. In 2016 gaf 19 procent van de bedrijven met 10 of meer werkzame personen aan niet of beperkt online te verkopen via een website of app vanwege problemen met ICT-beveiliging of gegevensbescherming.

3.2 Personen

Net zo goed als bedrijven nemen ook personen maatregelen om zo veilig mogelijk te internetten. Het CBS heeft informatie over het aanpassen van het internetgedrag vanwege zorgen om de veiligheid, het daadwerkelijk handelend optreden om cookies te verwijderen en/of de instellingen van de browser op dat punt te wijzigen of computer en smartphone te voorzien van beveiligingssoftware. Ook zijn er gegevens over het gebruik van clouddiensten voor de opslag van privé-bestanden.

Aanpassen gedrag

Een extreme vorm van het nemen van maatregelen is gewoonweg afzien van het gebruik van internet of bepaalde activiteiten op internet. Zo is er in Nederland in 2017 nog een procent van de huishoudens die aangeeft niet over internet te (willen) beschikken vanwege zorgen over de veiligheid en privacy. In 2017 gaf bijna twee procent van de personen van 12 jaar of ouder aan niet langs elektronische weg gegevens te hebben verstrekt aan overheidsinstanties vanwege zorgen over de bescherming en veiligheid van deze te verstrekken gegevens; bijna zes procent van de personen van 12 jaar of ouder gaf aan niet online te hebben gekocht vanwege zorgen over de veiligheid en privacy.[1)] Meer in zijn algemeenheid gaf in 2015 meer dan de helft van de personen van 12 jaar of ouder aan internetactiviteiten weleens afgebroken of vermeden te hebben omdat hij of zij het niet vertrouwde. Het ging hier om een beperkt aantal gemeten activiteiten (CBS, 2017). Op zich is het een goede reflex van gebruikers om bepaalde activiteiten af te breken omdat men zaken niet vertrouwd. Idealiter zouden zorgen over veiligheid en privacy echter geen belemmering moeten vormen voor het gebruik van internet.

Nederlander steeds bekender met term cookies

Steeds meer Nederlanders zijn bekend met cookies. In 2016 wist 80 procent van de mensen wat cookies zijn, in 2015 was dat 74 procent. Cookies zijn kleine bestanden die worden gebruikt om internetgedrag van gebruikers in kaart te brengen, om hen te identificeren en hen gericht advertenties te kunnen aanbieden of om het gebruik van websites te veraangenamen. Hoewel 55 procent van de personen van 12 jaar of ouder bezorgd is dat activiteiten op internet op deze manier bijgehouden worden, verandert slechts een derde de instelling van de internetbrowser om cookies te voorkomen of het aantal cookies te beperken. Het aantal personen dat zich *erg* zorgen maakt over het gebruik van cookies is overigens maar 11 procent (CBS, 2017).

Bijna helft personen maakt gebruik van clouddiensten

Bijna de helft (46 procent) van de personen van 12 jaar of ouder maakt in 2017 gebruik van clouddiensten voor het opslaan van privé-bestanden. In 2014 was dit nog 31 procent. Over het algemeen betreft het clouddiensten waar niet (apart) voor betaald hoeft te worden. Echter, het aantal personen dat gebruik maakt van betaalde clouddiensten is

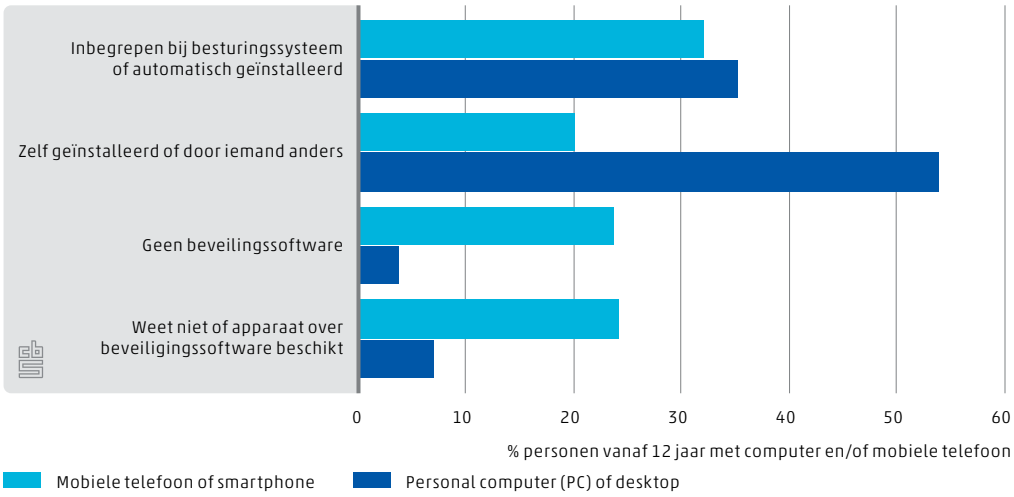
[1)] Bron: CBS, ICT-gebruik huishoudens en personen.

in de periode 2014 tot en met 2017 toegenomen van 3 naar 8 procent. Clouddiensten kunnen gezien worden als een vorm van ICT-beveiliging. Op de eerste plaats voor de gebruiker zelf; als de eigen computer beschadigd raakt zijn de bestanden nog veilig opgeslagen in de cloud. Daarnaast zal de beveiliging van de bestanden tegen beschadiging en ongeautoriseerde toegang in de cloud anders (beter) geregeld zijn dan in de gemiddelde privé-situatie.
Foto's zijn de meest voorkomende bestanden die in de cloud worden opgeslagen. Daarnaast maken mannen iets vaker gebruik van clouddiensten dan vrouwen, hoogopgeleiden iets vaker dan laagopgeleiden en jongeren veel vaker dan ouderen (zie ook tabel A3.3 achter in de publicatie).

Computers beter beveiligd dan mobiele telefoons

In 2017 is aan personen van 12 jaar of ouder gevraagd in hoeverre hun computer en mobiele telefoon voorzien zijn van beveiligingssoftware zoals antivirusprogramma's of een firewall. Voor de computer geeft 89 procent van de personen aan dat deze is voorzien van beveiligingssoftware. In het merendeel van de gevallen is deze software ook zelf geïnstalleerd. Slechts een kleine minderheid geeft aan het niet te weten (7 procent) of geen beveiligingssoftware geïnstalleerd te hebben (4 procent).
Voor de mobiele telefoon of smartphone liggen deze verhoudingen heel anders. Van de groep die zegt dat zijn of haar telefoon is voorzien van beveiligingssoftware (52 procent) zegt de meerderheid te denken dat dit inbegrepen is in het besturingssysteem of automatisch geïnstalleerd. Daarnaast geeft een kwart van de personen (24 procent) aan eigenlijk niet te weten of zijn of haar mobiele telefoon is voorzien van beveiligingssoftware. De bekendheid met of de informatie over beveiligingssoftware voor mobiele telefoons lijkt dus achter te blijven bij die met betrekking tot de (vaste) computer (zie ook tabel A3.4 achter in deze publicatie).

3.2.1 Beveiligingssoftware op computer en mobiele telefoon, 2017

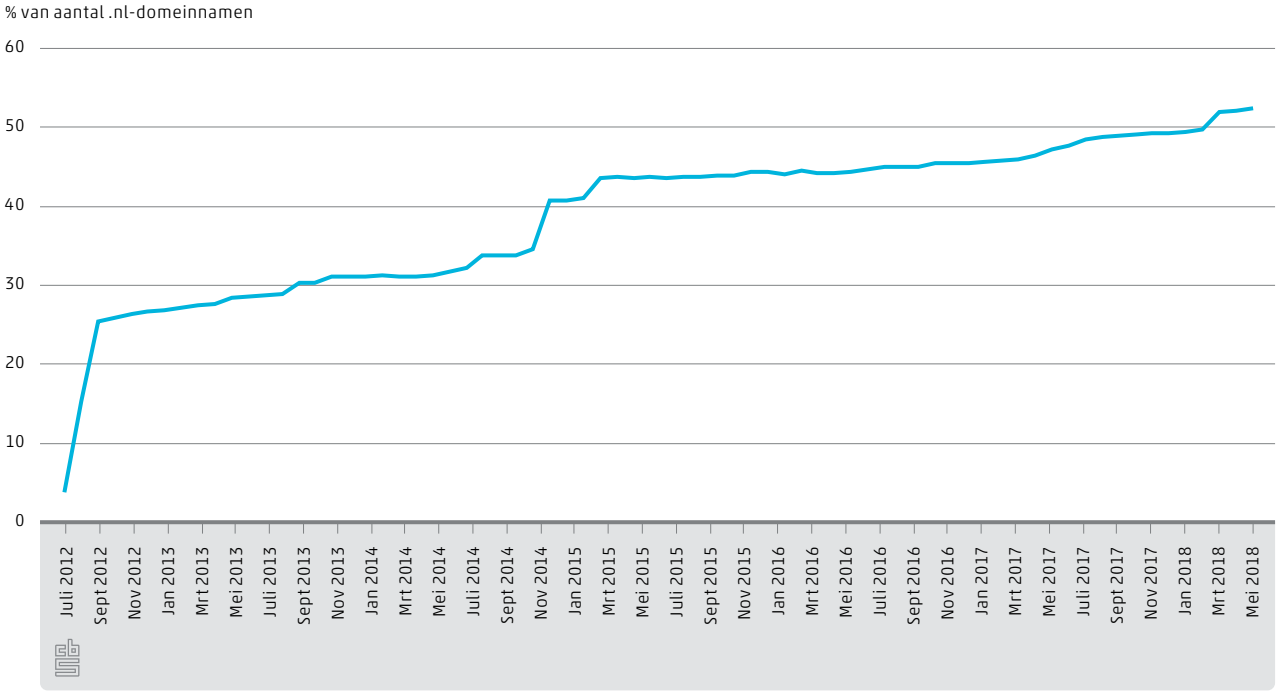


Bron: CBS, ICT-gebruik huishoudens en personen.

3.3 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 te ontfutselen of zelfs rechtstreeks 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.

3.3.1 Aantal .nl-domeinnamen dat gebruikmaakt van DNSSEC



Bron: SIDN.

Meer dan helft .nl-domeinnamen maakt gebruik van DNSSEC

Eind juni 2018 waren er 5,8 miljoen .nl-domeinnamen geregistreerd bij de Stichting Internet Domeinregistratie Nederland (SIDN). Ruim 3,0 miljoen van deze domeinnamen (52 procent) maakten gebruik van DNSSEC. Eind juni 2014 was dit nog 32 procent.
De 5,8 miljoen geregistreerde .nl-domeinnamen omvatten allerlei websites. Van niet of nauwelijks actieve websites van personen, tot websites van bedrijven en instellingen die duizenden keren per dag worden bezocht. Het aantal websites dat gebruikmaakt van DNSSEC zou dan ook informatiever zijn als het gedetailleerd zou kunnen worden naar personen en bedrijven (en daarbinnen bedrijfstakken) of bijvoorbeeld gewogen zou kunnen worden met het aantal bezoeken. Het is immers nuttiger als een veel bezochte website van bijvoorbeeld een bank gebruikmaakt van DNSSEC dan een website van een individuele persoon waar alleen maar recepten op staan. Het gebruik van DNSSEC is overigens niet een keuze van de houders van websites zelf, maar van de hostingbedrijven die deze techniek moeten aanbieden. Naast DNSSEC zijn er nog andere internetstandaarden waarvan het gebruik wordt aanbevolen, zoals DKIM, SPF en DMARC. Dit zijn standaarden die het onder andere moeilijker maken om e-mailverkeer te misleiden ('verkeerd te bezorgen'). Het gebruik van deze standaarden is wel een individuele keuze van de houder van de website.

4. Cybersecurity, incidenten

Als het misgaat bij elektronisch dataverkeer is dat soms onbedoeld, en incidenten zijn niet altijd meteen strafbare feiten. Ook het voorkómen van dit soort incidenten valt onder cybersecurity. Werken met ICT vergt een zekere discipline en procedures die de kans op incidenten verkleinen. Cybersecurity is niet alleen het wapenen tegen kwaadwillende maar ook tegen 'jezelf'. De belangrijkste indicatoren in dit hoofdstuk zijn de ICT-veiligheidsincidenten bij bedrijven en het aantal gemelde datalekken bij de Autoriteit Persoonsgegevens.

4.1 Cybersecurity, incidenten

Indicator	2014	2015	2016	2017	Eenheid	Bron
Bedrijven met ICT-veiligheidsincidenten						CBS
			50		**% bedrijven met 10 of meer werkzame personen**	
			26		**% bedrijven met 2 tot 10 werkzame personen**	
Bedrijven met kosten als gevolg van ICT-veiligheidsincidenten						CBS
			49		**% bedrijven met 10 of meer werkzame personen met ICT-veiligheidsincidenten**	
			44		**% bedrijven met 2 tot 10 werkzame personen met ICT-veiligheidsincidenten**	
Bedrijven die melding hebben gedaan van ICT-veiligheidsincidenten[1]						CBS
			9		**% bedrijven met 10 of meer werkzame personen met ICT-veiligheidsincidenten**	
			6		**% bedrijven met 2 tot 10 werkzame personen met ICT-veiligheidsincidenten**	
Fraude bij online aankopen (bijvoorbeeld geen levering of misbruik van creditcardgegevens)	.	2	3	3	**% personen vanaf 12 jaar**	CBS
Meldingen in het kader van de meldplicht datalekken zoals opgenomen in de Wet bescherming persoonsgegevens	.	.	5617	10009	**aantal meldingen (excl. ingetrokken meldingen)**	Autoriteit Persoonsgegevens
Meldingen in het kader van de zorg- en meldplicht van aanbieders van openbare telecommunicatienetwerken of -diensten zoals opgenomen in de Telecommunicatiewet	41	39	57	50	**aantal incidenten**	Agentschap Telecom
Verstoringen in de continuïteit van de dienstverlening	.	.	112	114	**aantal verstoringen**	
Omvang en duur (verijdelde) DDoS-aanvallen[2]						NBIP
waarvan > 10 gbps			13	12	**% van totaal**	
> 1 uur			36	21	**% van totaal**	

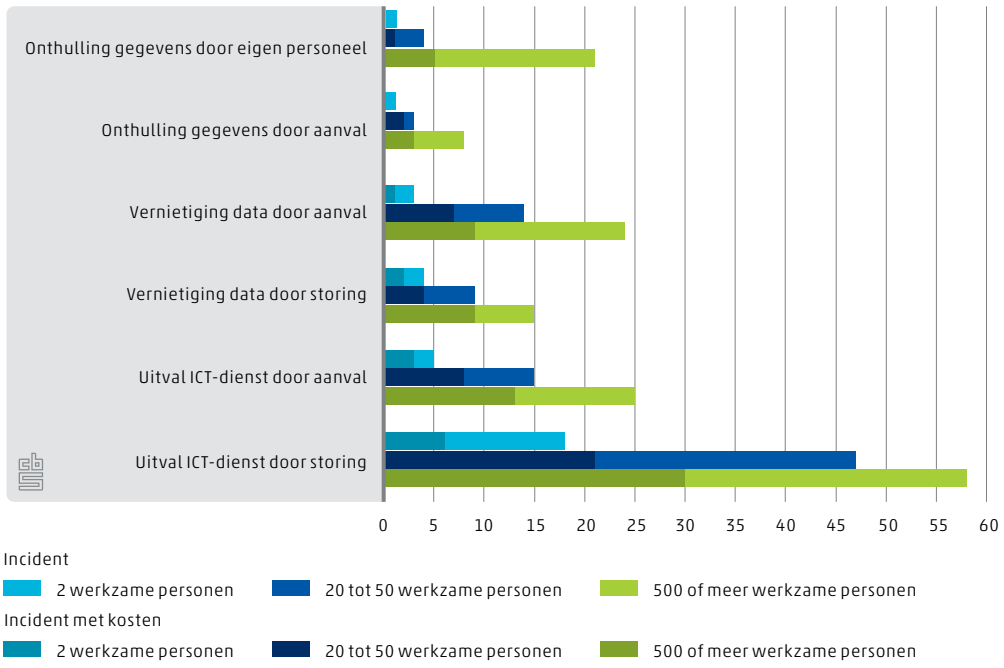
[1] Bij de Autoriteit Persoonsgegevens, een financiële instelling, de politie (aangifte) of een sectoraal, nationaal of ander securityteam.

[2] Heeft betrekking op de bij de NBIP aangesloten internetproviders die gebruikmaken van de Nationale anti-DDoS Wasstraat (NaWas). 2016: periode 1-7 tot en met 14-12.

Grotere bedrijven hebben vaker incidenten

Tot nu toe kwam naar voren dat over het algemeen grote bedrijven een hogere standaard van ICT-beveiliging hebben: er worden meer maatregelen toegepast, software-updates worden vaker handmatig doorgevoerd en het ICT-beveiligingswerk wordt vaker door het eigen personeel gedaan. Toch resulteert dit hogere cybersecurityniveau niet in minder incidenten ten opzichte van de kleinere bedrijven. Dit is te zien in figuur 4.2, waarin voor verschillende interne en externe incidenten aangegeven wordt welk percentage van de bedrijven daar mee te maken heeft gehad.
De grootste bedrijven hebben naar verhouding meer met incidenten te maken; 73 procent van de bedrijven met 500 of meer werkzame personen had in 2016 te maken met een ICT-veiligheidsincident tegen 21 procent van de bedrijven met 2 werkzame personen. Het relatief grote aantal incidenten binnen grote bedrijven kan verschillende oorzaken hebben. Allereerst hebben grote bedrijven over het algemeen meer mensen die met een computer werken, wat de kans groter maakt dat er ook een keer ergens iets mis gaat. De ICT-infrastructuur zal daarnaast ook complexer zijn dan bij een klein bedrijf. Het lijkt er minder toe te doen in welke bedrijfstak een bedrijf actief is. Het is bijvoorbeeld niet zo dat de financiële instellingen (37 procent) veel vaker een ICT-beveiligingsincident hebben dan een bedrijf in de industrie (36 procent). De horeca kent overigens wel verreweg het minste aantal incidenten (17 procent). Dit kan te maken hebben met het minder grootschalige en complexe ICT-gebruik binnen deze bedrijfstak. Voor alle bedrijfsgroottes en bedrijfstakken geldt overigens dat het overgrote deel van de ICT-veiligheidsincidenten veroorzaakt werd door een niet moedwillig veroorzaakte storing, bijvoorbeeld verkeerd geïnstalleerde software en in veel mindere mate door een kwaadwillende aanval van buitenaf (zie tabel A4.1 in de annex).

4.2 ICT-veiligheidsincidenten en daaruit voortvloeiende kosten, 2016



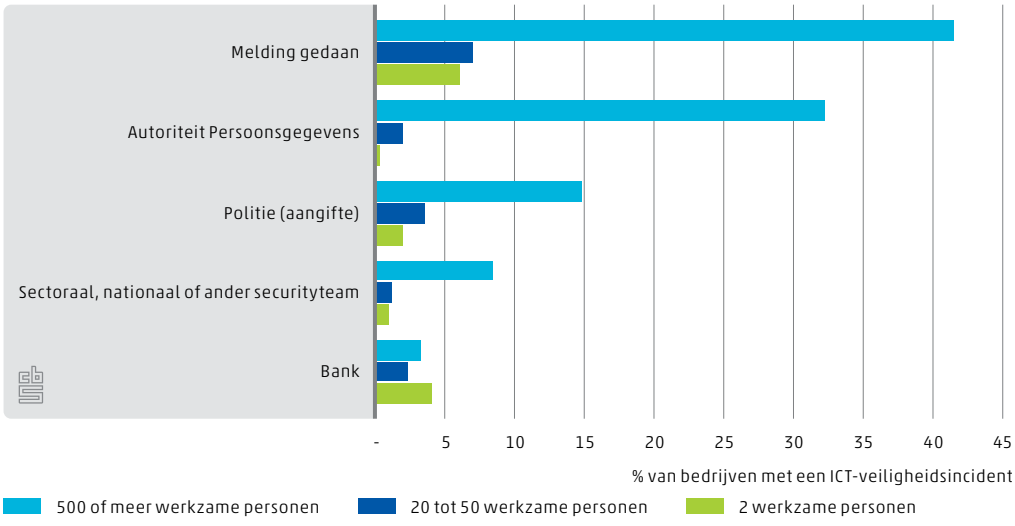
Bijna helft ICT-veiligheidsincidenten kost geld

Van de bedrijven met 2 of meer werkzame personen die in 2016 te maken hebben gehad met een ICT-veiligheidsincident gaf 46 procent aan dat hier ook kosten uit voortgevloeid waren. Dit percentage varieerde van 41 procent voor de kleinste bedrijven (2 werkzame personen) tot 52 procent voor de grootste bedrijven (500 of meer werkzame personen). Voor de bedrijven in de horeca (34 procent), de informatie- en communicatiesector (38 procent) en de financiële sector (40 procent) vloeiden er het minst vaak kosten voort uit een ICT-veiligheidsincident terwijl dit heel verschillende bedrijfstakken zijn. Misschien leiden de incidenten in de horeca inderdaad niet zo vaak tot kosten en zijn bedrijven in de informatie- en communicatiesector en de financiële sector beter in staat de gevolgen van een incident te controleren (zie tabel A4.1 in de annex).

7 procent bedrijven meldt ICT-veiligheidsincident

Van alle bedrijven met 2 of meer werkzame personen die in 2016 een ICT-veiligheidsincident hebben gehad, heeft 7 procent hiervan melding gedaan bij een officiële instantie. Van de bedrijven met 2 tot 10 werkzame personen die een ICT-veiligheidsincident hebben gehad deed 6 procent hier melding van; voor de bedrijven met 10 of meer werkzame personen was dit 9 procent. Dit lijkt weinig, maar lang niet alle ICT-veiligheidsincidenten hoeven te worden gemeld. Een zelf veroorzaakte storing waar derden geen last van hebben ondervonden hoeft niet per se gemeld te worden. Vooral de grootste bedrijven doen vaker melding van een ICT-veiligheidsincident. Hierbij valt op dat deze grotere bedrijven vaak een incident (ook) melden bij de Autoriteit Persoonsgegevens, terwijl de kleinste bedrijven het vaakste melding doen bij hun bank. Het lijkt hier dus om verschillende soorten ICT-veiligheidsincidenten te gaan. Van de bedrijfstakken doet de sector energie & water het vaakst melding van een ICT-veiligheidsincident (zie tabel A4.2 in de annex).

4.3 Melding van ICT-veiligheidsincidenten, 2016



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 2017 zijn 50 van dit soort meldingen gedaan (57 in 2016). Een melding kan gepaard gaan met meerdere verstoringen van telecomdiensten. In 2017 leidden de 50 meldingen tot 114 verstoringen (112 in 2016). In sommige gevallen is de storing wel doelbewust veroorzaakt door een kwaadwillende. Vaak ook is de oorzaak de genoemde defecte zendmast of verkeerd geïnstalleerde software en/of 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.

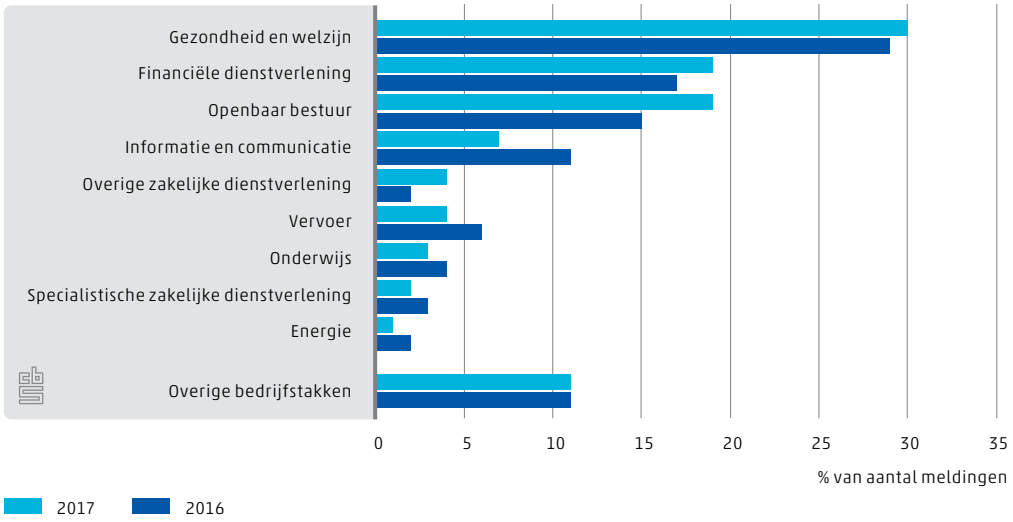
10 duizend meldingen van datalekken

Een ander voorbeeld van incidenten die niet altijd doelbewust en strafbaar zijn, zijn de 10 009 datalekken zoals die in 2017 zijn gemeld bij de Autoriteit Persoonsgegevens. Over 2016 waren dit er 5 617. Het gaat hier over privacygevoelige gegevens die mogelijk in handen van derden zijn gevallen of waar derden toegang toe hebben gehad. Ook hier geldt dat de oorzaak van dit soort datalekken soms onbedoeld is en terug te voeren 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 2017 was 6 procent van de datalekken veroorzaakt door het hacken en/of via *malware* en *phishing* toegang krijgen tot de betreffende gegevens.

Meeste meldingen uit gezondheidssector

In 2017 kwamen de meeste meldingen van datalekken uit de gezondheidssector, gevolgd door de financiële sector en het openbaar bestuur. 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.
De voorgaande voorbeelden van incidenten illustreren dat niet alles wat er mis kan gaan met ICT kwade opzet is. En 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 voortkomen uit menselijk tekortkomingen (slordigheid, vergeetachtigheid, onbekwaamheid e.d.).

4.4 Meldingen datalekken bij Autoriteit Persoonsgegevens, naar bedrijfstak



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 tabel 4.1 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.
Kenmerken van DDoS-aanvallen zijn de omvang (gbps) en de duur (tijd). In 2017 had 12 procent van de DDoS-aanvallen een omvang van meer dan 10 gbps. Dit was ook in 2016 het geval (13 procent). Een vijfde (21 procent) van de aanvallen duurde in 2017 langer dan een uur. 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 te mitigeren.

Drie procent online kopers heeft last van fraude

In 2017 had 3 procent van de personen van 12 jaar en ouder te maken gehad met online fraude bij het online bestellen van goederen en diensten (bijvoorbeeld geen levering van de bestelde producten of misbruik van creditcard-gegevens). In 2016 betrof dit ook 3 procent van de personen. In 2015 was dit 2 procent.

5.

Cybercrime

Cybercrime is in hoofdstuk 2 omschreven als: 'alle delicten die gepleegd worden met behulp van ICT'. Criminaliteit (crime) is hier het plegen van een strafbaar feit (delict). Bij cybercrime is het kwaad dus al geschied. Er zijn computers gehackt en er zijn mensen online opgelicht. De preventieve maatregelen van mens en machine schoten te kort. De statistische informatie over het voorkomen van cybercrime in dit hoofdstuk komt uit de Veiligheidsmonitor, waar aan personen ouder dan 15 jaar onder meer wordt gevraagd of ze slachtoffer zijn geweest van – een inmiddels gelimiteerd aantal – cybercrimedelicten. Daarnaast worden cijfers gepresenteerd uit de bij de politie geregistreerde misdrijven waar cybercrime – zij het niet altijd even adequaat – in opgenomen is. Een uitgebreidere toelichting op deze genoemde bronnen is te vinden in hoofdstuk 6.

5.1 Cybercrime

Indicator	2012	2013	2014	2015	2016	2017	Eenheid	Bron
Ondervonden delicten cybercrime[1)]	19,7	20,8	18,8	18,7	17,9	18,6	**per 100 inwoners**	CBS
Slachtofferschap cybercrime[1)]	12,1	12,6	11,2	11,1	10,7	11,0	**% personen vanaf 15 jaar**	CBS
Meldingen cybercrime[1)]	31,4	29,6	27,7	26,9	26,9	27,0	**% van ondervonden delicten**	CBS
Meldingen bij politie[1)]	12,7	13,3	12,7	12,7	13,1	13,1	**% van ondervonden delicten**	CBS
Aangifte totaal[1)]	7,1	7,4	7,3	7,8	7,6	8,0	**% van ondervonden delicten**	CBS
waarvan identiteitsfraude totaal	1,6	1,3	0,7	0,6	0,4	0,4	**per 100 inwoners**	
slachtoffers	1,5	1,3	0,8	0,6	0,4	0,4	**% personen vanaf 15 jaar**	
melding totaal	90,1	89,0	87,6	84,0	81,9	86,0	**% van ondervonden delicten**	
melding bij politie	16,7	17,6	14,4	20,4	23,1	20,6	**% van ondervonden delicten**	
aangifte totaal	12,5	13,0	11,6	13,1	16,9	16,0	**% van ondervonden delicten**	
koop- en verkoopfraude totaal	3,4	3,9	4,1	4,2	4,1	4,6	**per 100 inwoners**	
slachtoffers	2,9	3,3	3,5	3,5	3,4	3,9	**% personen vanaf 15 jaar**	
melding totaal	41,0	44,9	40,9	39,1	39,8	39,7	**% van ondervonden delicten**	
melding bij politie	24,2	25,7	24,2	23,4	23,6	23,5	**% van ondervonden delicten**	
aangifte totaal	20,2	21,8	20,1	20,0	20,2	19,0	**% van ondervonden delicten**	
hacken totaal	8,8	9,3	7,9	7,6	7,4	7,5	**per 100 inwoners**	
slachtoffers	6,0	6,2	5,2	5,1	4,9	4,9	**% personen vanaf 15 jaar**	
melding totaal	22,1	19,8	18,8	18,4	20,4	20,0	**% van ondervonden delicten**	
melding bij politie	5,9	6,7	4,9	4,3	5,3	5,1	**% van ondervonden delicten**	
aangifte totaal	2,4	1,8	1,8	1,8	2,3	2,7	**% van ondervonden delicten**	
cyberpesten totaal	5,9	6,3	6,0	6,3	6,0	6,1	**per 100 inwoners**	
slachtoffers	3,1	3,3	3,1	3,2	3,2	3,1	**% personen vanaf 15 jaar**	
melding totaal	23,4	21,7	23,1	23,9	22,1	22,6	**% van ondervonden delicten**	
melding bij politie	14,9	14,3	15,1	15,2	14,8	14,5	**% van ondervonden delicten**	
aangifte totaal	5,0	5,3	5,4	6,4	4,9	5,7	**% van ondervonden delicten**	
Computervredebreuk								
Geregistreerde misdrijven	4620	2535	2045	2225	1875	2300	**aantal**	CBS
Geregistreerde misdrijven, relatief	0,4	0,2	0,2	0,2	0,2	0,3	**% van totaal geregistreerde misdrijven**	
Geregistreerde misdrijven per 1 000 inwoners	0,3	0,2	0,1	0,1	0,1	0,1	**per 1 000 inwoners**	
Opgehelderde misdrijven	265	255	195	165	160	105	**aantal**	CBS
Opgehelderde misdrijven, relatief	5,8	10	9,5	7,4	8,6	4,6	**% van geregistreerde misdrijven**	
Registraties van verdachten	300	295	235	195	210	220	**aantal**	CBS

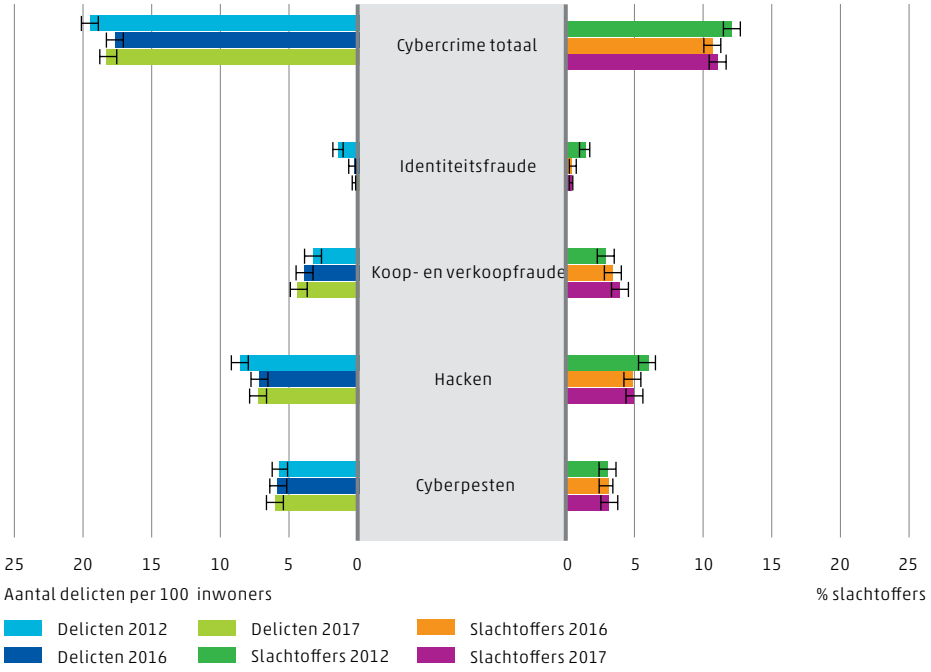
[1)] In het onderzoek is naar een gelimiteerd aantal typen cybercrimedelicten gevraagd (identiteitsfraude, hacken, koop- en verkoopfraude, cyberpesten).

Een op de negen Nederlanders slachto er cybercrime

Vanaf 2012 verzamelt het CBS gegevens over vier belangrijke vormen van cybercrime, te weten identiteitsfraude, hacken, koop- en verkoopfraude en cyberpesten. Het gaat

hier over slachtofferschap van burgers zoals waargenomen in de Veiligheidsmonitor (zie hoofdstuk 6).
In totaal is een op de negen Nederlanders (11,0 procent) in 2017 een of meer malen slachtoffer geweest van een cybercrimedelict. Dit is vergelijkbaar met de voorgaande jaren, maar minder dan in 2012 (12,1 procent) en 2013 (12,6 procent).
In 2017 is 4,9 procent van de 15-plussers gehackt, 3,1 procent is wel eens online gepest en 3,9 procent is naar eigen zeggen opgelicht via internet. Van 0,4 procent van de Nederlanders zijn via internet identificerende gegevens gestolen.
Binnen de categorie hacken is het inbreken op iemands website/profielsite de meest voorkomende variant gevolgd door het inbreken op iemands e-mailaccount. Binnen de categorie identiteitsfraude is skimming de afgelopen jaren afgenomen. *Phishing/pharming* is in de loop der jaren ook iets afgenomen, maar komt in 2017 wel vaker voor dan skimming. Koopfraude komt veel vaker voor dan verkoopfraude. En binnen cyberpesten zijn laster en stalken de meest voorkomende vormen (zie ook tabel A 5.3 achterin deze publicatie).

5.2 Slachtofferschap en ondervonden delicten cybercrime[1)]



Bron: CBS, Veiligheidsmonitor.
[1)] In het onderzoek is naar een gelimiteerd aantal typen cybercrimedelicten gevraagd (identiteitsfraude, hacken, koop- en verkoopfraude, cyberpesten).

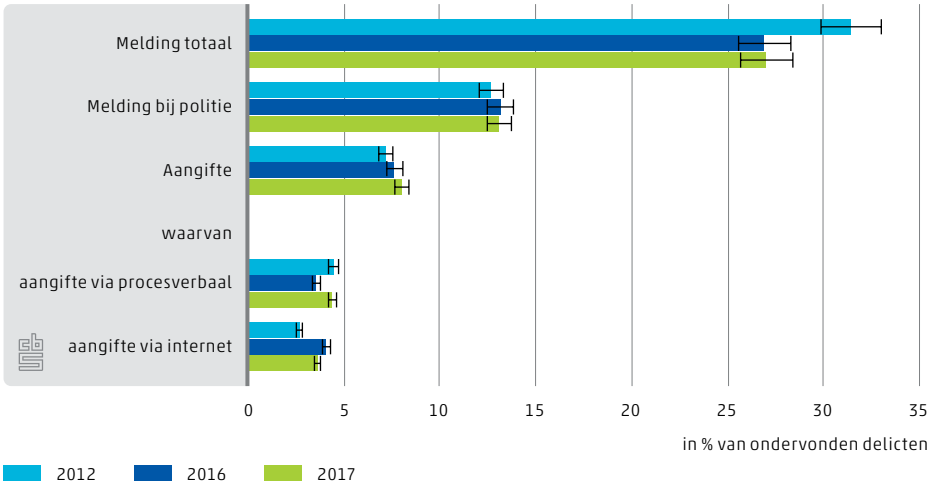
Omdat iemand meerdere keren slachtoffer kan zijn van een cybercrimedelict is het aantal slachtoffers niet altijd gelijk aan het aantal delicten. Bij hacken en vooral cyberpesten is vaker sprake van herhaald slachtofferschap dan bij koop- en verkoopfraude en identiteitsfraude. Cyberpesten is dan ook een meer op de persoon gerichte actie in tegenstelling tot bijvoorbeeld het oplichten van een willekeurige persoon die iets online bestelt. De invloed van het slachtoffer op het voorkomen van herhaling is bij verkoopfraude ook groter ('ik doe dat niet nog een keer zo') dan bij cyberpesten.

Het aantal personen dat slachtoffer is van cybercrime varieert naar achtergrondkenmerken van slachtoffers. Mannen zijn vaker slachtoffer van cybercrime dan vrouwen, vooral van hacken. Jongeren zijn vaker slachtoffer dan ouderen, behalve bij identiteitsfraude. Hiervan zijn 15- tot 25-jarigen het minst vaak slachtoffer. Herkomst speelt nauwelijks een rol. Hoger opgeleiden zijn vaker slachtoffer van identiteitsfraude, koop- en verkoopfraude en hacken dan lager opgeleiden. Lager opgeleiden zijn vaker slachtoffer van cyberpesten. Verder worden homo's vaker online gepest. Er zijn nagenoeg geen verschillen tussen steden en dorpen (zie ook tabel A 5.1 achterin deze publicatie).

Bijna drie kwart cybercrimedelicten wordt niet gemeld

Van alle gevallen van identiteitsfraude, koop- en verkoopfraude, hacken en cyberpesten samen is in 2017 ruim een kwart (27 procent) gemeld bij de politie of een andere instantie. Dit is minder dan in 2012 en 2013. Aangifte bij de politie werd in 2017 in ongeveer een op de dertien gevallen (8 procent) gedaan. Dit is vergelijkbaar met voorgaande jaren. Het aandeel dat via internet werd aangegeven is in 2017 vrijwel even groot als het aandeel dat via een proces-verbaal werd aangegeven. Dit was in 2014 ook het geval. In 2012 en 2013 was het aandeel aangiften van cybercrime via internet nog kleiner dan het aandeel aangiften via een proces-verbaal.

5.3 Melding en aangifte cybercrime[1)]



Bron: CBS, Veiligheidsmonitor.

[1)] In het onderzoek is naar een gelimiteerd aantal typen cybercrimedelicten gevraagd (identiteitsfraude, hacken, koop- en verkoopfraude, cyberpesten).

Cybercrime wordt dus lang niet altijd gemeld, niet bij de politie, maar ook niet bij een andere instantie. En als het wordt gemeld, is dit niet altijd (ook) bij de politie maar soms zelfs vaker bij een andere instantie. Zo wordt identiteitsfraude het vaakst gemeld bij de bank of financiële instelling en beduidend minder vaak (ook) bij de politie. Identiteitsfraude wordt overigens verreweg het vaakst gemeld (86 procent) onder andere omdat het vaak gepaard gaat met verlies van geld en de bank geïnformeerd wordt om bijvoorbeeld de rekening te blokkeren. Bij de andere onderscheiden vormen van cybercrime ligt dit percentage beduidend lager. Ten slotte zij opgemerkt dat er ook

nog een aantal procentpunten verschil zit tussen slachtoffers die een cybercrimedelict melden bij de politie (het slachtoffer wil dat de politie er weet van heeft) en de slachtoffers die dit ook laten vastleggen in een proces-verbaal van aangifte.

Cybercrime versus traditionele misdaad

Hoe verhouden aard en omvang van cybercrime zich nu tot de traditionele delicten? In 2017 was het aantal ondervonden traditionele delicten 27,0 per honderd inwoners. In dat jaar bedroeg het aantal cybercrimedelicten 18,6 per honderd inwoners. Hoewel schade en impact op het slachtoffer tussen delicten niet te vergelijken zijn, is het aantal ondervonden cybercrimedelicten getalsmatig niet te verwaarlozen. Zelfs als cybercrimedelicten niet uitputtend worden waargenomen.
Van alle traditionele delicten werd in 2017 ruim een op de drie gemeld bij de politie (34,4 procent). Van ruim twee derde hiervan (24,4 procent) werd daadwerkelijk aangifte gedaan. Voor cybercrime zijn deze percentages beduidend lager, te weten 13,1 en 8,0. Het relatieve aantal meldingen dat in de vorm van een aangifte wordt gedaan, ligt bij cybercrime ook lager dan bij de traditionele misdaden. Zoals hiervoor al opgemerkt worden cybercrimedelicten ook veelvuldig gemeld bij andere instanties dan de politie. Op het punt van melding en aangifte liggen de percentages voor cybercrime nog het dichtst bij de percentages voor de vandalismedelicten (19,1 procent van de vandalismedelicten wordt bij de politie gemeld; 13,7 procent in de vorm van een aangifte).

Geregistreerde cybercrime

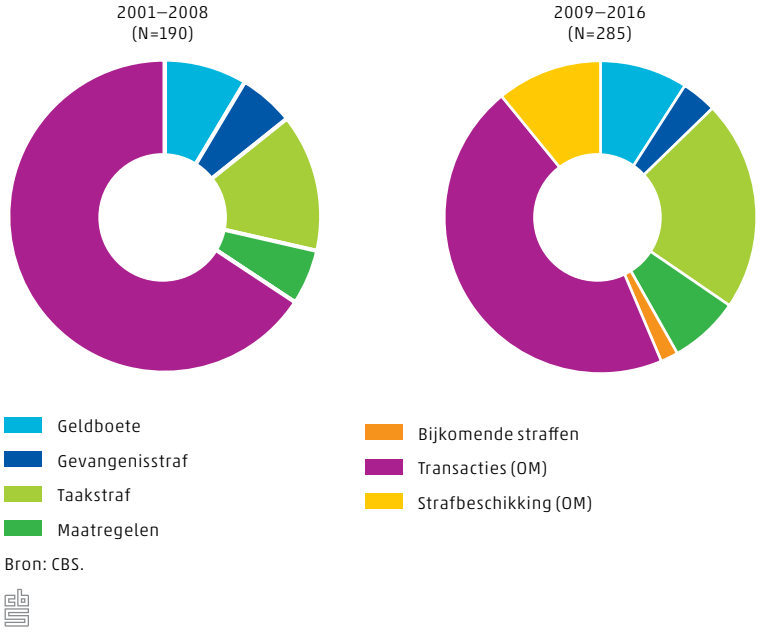
Op dit moment is computervredebreuk in de Standaardclassificatie Misdrijven van het CBS de enige categorie die valt onder cybercrime. Internetoplichting en online zedendelicten bijvoorbeeld vallen in deze classificatie onder de categorieën oplichting en seksuele misdrijven. Zowel de politie, die de bron is van de beschrijving van de geregistreerde criminaliteit in Nederland, als het CBS zijn bezig om de registratie en classificatie van cybercrime te verbeteren. Zo heeft de politie nieuwe feitcodes geïntroduceerd voor het classificeren van misdrijven w.o. de feitcode F636 Fraude met onlinehandel. Deze feitcodes vormen de basis van de indeling van misdrijven in de Standaardclassificatie Misdrijven.
Vanaf Juni 2015 zijn de meldingen van internetoplichting gedaan bij het Landelijk meldpunt Internetoplichting (LMIO) opgenomen in de bij de politie geregistreerde misdrijven. Deze meldingen vallen grotendeels samen met de feitcode Fraude met onlinehandel en komen in de Standaardclassificatie Misdrijven terecht in de categorie Oplichting. In 2016 kwamen er 42 169 meldingen van het LMIO; in 2017 37 329.

Computervredebreuk

Hiervoor kwam al naar voren dat slechts een gering deel van de ondervonden cybercrimedelicten door slachtoffers wordt aangegeven bij de politie. Voor hacken – waar computervredebreuk onder valt – was dit in 2017 maar 5,1 procent (2,7 procent in de vorm van een proces-verbaal). De bij de politie gemelde (geregistreerde) gevallen van computervredebreuk zijn dus maar een fractie van het totale aantal delicten.

In 2017 was het opheldering spercentage[1] van de aangegeven gevallen van computervredebreuk 4,6 procent. Dit is vergeleken met andere geregistreerde misdrijven, aan de lage kant. Voor alle geregistreerde misdrijven tezamen was het opheldering spercentage in 2017 23,0 procent.

5.4 Door Openbaar Ministerie en rechter opgelegde stra en en maatregelen voor computervredebreuk



Bron: CBS.

Opgelegde sancties

In figuur 5.4 is weergegeven welke straffen 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[2] uit of biedt een transactie aan.
In de periode 2001–2008 bedroeg het aantal door het Openbaar Ministerie en de rechter opgelegde straffen 190. In 61 procent van die gevallen deed het Openbaar Ministerie de zaak af zonder tussenkomst van de rechter. Dit zijn zogenoemde transacties die in het geval van computervredebreuk vaak bestonden uit een werkstraf of een geldboete.
In de periode 2009–2016 bedroeg het totale aantal opgelegde straffen voor computervredebreuk 285. In deze periode was het aandeel van door het Openbaar Ministerie aangeboden transacties en opgelegde strafbeschikkingen 54 procent. Zowel in absolute als in relatieve zin zijn in de periode 2009–2016 dus meer gevallen van computervredebreuk voor de rechter gekomen.

[1] Misdrijven waarbij tenminste één verdachte bij de politie bekend is, ook al is deze voortvluchtig of ontkent hij/zij het strafbare feit te hebben gepleegd.
[2] Strafbeschikkingen kunnen worden opgelegd sinds de inwerkingtreding van de Wet OM-afdoening in 2008.

6. Bronnen

Onderstaand een korte omschrijving van de vier belangrijkste bronnen van de in deze publicatie samengebrachte indicatoren.
Voor de vier genoemde bronnen geldt dat deze geen van alle zijn ontworpen om uitsluitend en alleen gegevens te verzamelen op het terrein van cybersecurity. Voor de drie statistieken van CBS geldt dat vragen over cybersecurity moeten concurreren met tal van andere vragen over ICT-gebruik en veiligheid. Dit betekent dat het ook niet mogelijk is binnen het kader van deze statistieken het aantal vragen over cybersecurity enorm uit te breiden. Een (duur) alternatief om toch op korte termijn meer en gedetailleerdere informatie te verkrijgen over cybersecurity is het wél houden van een aparte enquête op dit terrein onder personen en/of bedrijven.

Veiligheidsmonitor

De Veiligheidsmonitor is een jaarlijks terugkerende grootschalige bevolkingsenquête, waarin zaken als leefbaarheid en overlast in de woonbuurt, veiligheidsbeleving, slachtofferschap van veel voorkomende criminaliteit, het oordeel van de burger over het optreden van de politie en preventiegedrag worden onderzocht. Het veldwerk voor de *Veiligheidsmonitor 2017* is uitgevoerd in de periode van 10 augustus tot 30 november onder alle in Nederland wonende personen van 15 jaar en ouder, met uitzondering van de bewoners van inrichtingen en tehuizen. Hierbij werden in totaal ruim 380 duizend steekproefpersonen voor deelname benaderd. Uiteindelijk zijn onderzoeksgegevens verkregen van bijna 150 duizend personen. De respons was dus 39,3 procent. Dit is 0,8 procentpunt hoger dan in 2016 (38,5 procent).
In de Veiligheidsmonitor wordt mensen gevraagd naar ondervonden delicten in de twaalf maanden voorafgaand aan het onderzoek. Voor cybercrime zijn in 2012 vier delicten geformuleerd die toentertijd relevant waren. *Ransomware* wordt hierbij bijvoorbeeld niet expliciet genoemd. De cijfers geven dus geen volledig beeld van de aard en omvang van cybercrime. Daarnaast blijkt uit recent aanvullend onderzoek over internetoplichting dat in de Veiligheidsmonitor het aantal gevallen overschat lijkt te worden. Mensen wordt gevraagd het aantal ondervonden delicten in de afgelopen twaalf maanden te melden. Uit een confrontatie met gegevens van het Landelijk meldpunt Internetoplichting blijkt dat ook delicten die langer dan twaalf maanden geleden hebben plaatsgevonden abusievelijk ook nog wel eens gemeld worden.

Enquête 'ICT-gebruik bedrijven'

Het CBS onderzoekt jaarlijks hoe bedrijven ICT gebruiken. De enquête 'ICT-gebruik bedrijven' hanteert een steekproef van ongeveer 10 duizend bedrijven. De onderzoekspopulatie bestaat standaard uit bedrijven met 10 of meer werkzame personen. Over het verslagjaar 2017 zijn echter ook bedrijven met 2 tot en met 9 werkzame personen opgenomen in het onderzoek. Niet alle bedrijfstakken behoren tot deze populatie. Landbouwbedrijven vallen hier bijvoorbeeld buiten. De onderstaande tabel geeft een overzicht van de bedrijfstakken die het onderzoek omvat. De tabel bevat per bedrijfstak ook een korte benaming die in deze publicatie wordt gebruikt om de tekst leesbaarder te maken.

Naam in deze publicatie	Bedrijfstakken volgens SBI2008
Industrie	C Industrie
Energie & water	D Productie en distributie van elektriciteit, aardgas, stoom en gekoelde lucht, E Winning en distributie van water; afval- en afvalwaterbeheer en sanering
Bouw	F Bouwnijverheid
Handel	G Groot- en detailhandel; reparatie van auto's
Transport	H Vervoer en opslag
Horeca	I Logies-, maaltijd- en drankverstrekking
Informatie en communicatie	J Informatie en communicatie
Financiële instellingen	K Financiële activiteiten en verzekeringen1
Onroerend goed	L Exploitatie van en handel in onroerend goed
Advies en onderzoek	M Vrije beroepen en wetenschappelijke en technische activiteiten
Overige dienstverlening	N Administratieve en ondersteunende dienstverlening
Gezondheidszorg	Q Gezondheids- en welzijnszorg

[1)] Alleen SBI-codes 6419, 6492, 651, 652, 6612 en 6619.

De meeste vragen in het onderzoek gaan over de huidige situatie van een bedrijf. In dat geval heeft het cijfer betrekking op het jaar waarin het onderzoek is gehouden (jaar t). Sommige vragen gaan over het laatste volledige kalenderjaar. Het verslagjaar is dan t-1. Dit is bijvoorbeeld nodig als de vraag te maken heeft met een afgerond boekjaar, zoals bij vragen over de omzet behaald met e-commerce. Doordat ICT-toepassingen zich zeer snel ontwikkelen, wijzigt de inhoud van de ICT-enquête ook steeds. In de jaren tachtig stond centraal of bedrijven computers bezaten, en of zij automatiseringspersoneel in dienst hadden. In recente jaren ligt de nadruk meer op onderwerpen zoals internet, e-commerce, en toepassingen van software. Deze sterke inhoudelijke veranderingen zorgen ervoor dat lange tijdreeksen niet beschikbaar zijn. Het is wel mogelijk Nederland te vergelijken met andere landen in Europa, doordat EU-landen sinds 2001 onderling dezelfde vragen en definities gebruiken.

Enquête 'ICT-gebruik van huishoudens en personen'

Om informatie te verkrijgen over hoe huishoudens en personen ICT en internet gebruiken, voert CBS sinds 2005 jaarlijks de enquête 'ICT-gebruik van huishoudens en personen' uit. Ieder jaar doen bijna 5 duizend mensen mee aan dit onderzoek. De onderzoekspopulatie bestaat uit alle inwoners van Nederland van 12 jaar en ouder. De tekst in deze publicatie spreekt vaak over Nederlanders, waar het eigenlijk gaat om inwoners van Nederland, ongeacht hun nationaliteit. Hier is voor gekozen om de tekst makkelijker leesbaar te maken.
Ook voor deze statistiek geldt dat de uitkomsten voor Nederland vergeleken kunnen worden met die van andere EU-landen, omdat deze statistiek onderdeel is van een geharmoniseerde enquête die in alle EU-landen wordt gehouden.

Geregistreerde criminaliteit

Het doel van deze statistiek is het geven van een beschrijving van de aard, omvang en ontwikkeling van de geregistreerde misdrijven in Nederland. Wat er gemeten wordt, zijn alle in Nederland door de politie geregistreerde misdrijven. Deze gegevens worden van de verschillende politiekorpsen ontvangen. Het betreft dus een integrale waarneming.

De frequentie van het onderzoek is jaarlijks. In de maand juni volgend op het verslagjaar worden de voorlopige cijfers gepubliceerd; de definitieve cijfers volgen in november. Er zijn vergelijkbare cijfers beschikbaar vanaf 2005. Op basis van de door de politie toegekende feitcodes worden de misdrijven door het CBS geclassificeerd volgens de Standaardclassificatie Misdrijven (Politie) 2010.
De geregistreerde criminaliteit omvat meldingen en aangiftes van misdrijven bij de politie. Onder andere uit de Veiligheidsmonitor blijkt dat mensen lang niet alle delicten aangeven. Daarnaast is er in deze registratie de afgelopen jaren maar één delict onderscheiden dat rechtstreeks te koppelen is aan cybercrime, namelijk computervredebreuk. Andere vormen van cybercrime zoals oplichting via internet of identiteitsfraude zijn opgenomen in de algemene feitcodes voor oplichting en fraude. Een groot deel van de cyberdelicten die door de politie worden geregistreerd zijn dus niet apart onderscheiden. De politie doet wel inspanningen om dit te verbeteren omdat cybercrime een groeiende categorie delicten is die zowel qua preventie als vervolging een eigen aanpak nodig heeft. Zo worden er nieuwe feitcodes geïntroduceerd om cyberdelicten beter te registreren en zijn de online aangiftes van internetfraude bij het Landelijk meldpunt Internetoplichting sinds kort ook opgenomen in de geregistreerde criminaliteit.

Referenties

(CBS, 2017). *Cybersecuritymonitor 2017. Een eerste verkenning van dreigingen, incidenten en maatregelen*. CBS, Den Haag/Heerlen/Bonaire.

(ENISA, 2016). *ENISA Threat Landscape 2015*. January 2016.

(HCSS, 2015). The Hague Centre for Strategic Studies, 2015. *Assessing cyber security, A meta-analysis of threats, trends, and responses to cyber attacks*.

(NCSC, 2016). Nationaal Cyber Security Centrum, *Cybersecuritybeeld Nederland CSBN 2016*. September 2016.

(Shapiro en Varian, 2000). Shapiro C. & H.R. Varian, *De nieuwe economie: een strategische gids voor de netwerkeconomie*. Amsterdam: Nieuwezijds, 2000.

Overige literatuur

Autoriteit Persoonsgegevens, 2015. *De meldplicht datalekken in de Wet bescherming persoonsgegevens (Wbp). Beleidsregels voor toepassing van artikel 34a van de Wbp*. December 2015.

Agentschap Telecom, 2014. *Regels voor de continuïteit van telecomdiensten*. Juli 2014.

CBS, 2016. *ICT, kennis en economie 2016*. CBS, Den Haag/Heerlen/Bonaire.

CBS, 2016. *Veiligheidsmonitor 2015*. CBS, Den Haag/Heerlen/Bonaire.

CPB, 2016. *Risicorapportage Cyberveiligheid Economie*. CPB Notitie, 6 juli 2016.

Deloitte. *Cyber Value at Risk in the Netherlands*.

ENISA, 2015. *Definition of Cybersecurity*. December 2015.

KPN, 2016. *European Cyber Security Perspectives 2016*.

Meulen, Nicole van der, 2015. *Investing in Cybersecurity*. RAND Europe, August 2015.

NCTV, 2018. *Nederlandse Cybersecurity Agenda. Nederland digitaal veilig*.

PWC. *Turnaround and transformation in cybersecurity. Key findings from The Global Stat of Information Security Survey 2016*.

Symantec, 2015. *ISTR20 Internet security threat report*. Volume 20, April 2015.

Verizon, 2016. *2016 Data Breach Investigations Report*.

WODC, 2016. *Cybercrime in cijfers*. Memorandum 2016-1.

Bijlage 1: Het Nederlandse 'Internet of Things' volgens Censys

Bij het zoeken naar relevante data over cybersecurity is het CBS naast het verbeteren van zijn eigen enquêtes op dit punt, ook nadrukkelijk op zoek naar andere manieren en bronnen van onderzoek. Er is immers een grens aan wat je personen en bedrijven kan vragen op het punt van cybersecurity. Het langs andere weg (objectiever) vaststellen van kwetsbaarheden in onze ICT-infrastructuur is een belangrijke complementaire aanpak. Een moeilijk punt bij het exploiteren van andere bronnen van gegevens is het vellen van een oordeel over de kwaliteit en representativiteit van deze gegevens (zie ook hoofdstuk 2). Desalniettemin worden in deze bijdrage enkele bevindingen gedeeld uit een eerste exploratief onderzoek met publiek beschikbare data met informatie over apparatuur die was aangesloten op ruim 150 miljoen IP4-adressen wereldwijd zoals verzameld en beschikbaar gesteld door Censys.
Het internet bestaat uit miljarden individuele netwerken. Elk netwerk heeft een beheerder. Dit kan een Internet Service Provider (ISP) zijn, maar bijvoorbeeld ook een universiteit of een bedrijf. Een verzameling van netwerken die onder het beheer staat van één beheerder wordt een 'Autonomous System' (AS) genoemd. Medio oktober 2017 telde Nederland 764 'Autonomous Systems' (AS's) die onder het beheer stonden van 712 verschillende beheerders. De meeste beheerders beheerden één AS. Vijf beheerders voerden het beheer over meer dan twee AS's.
Het aantal AS's per land wordt door de OESO gezien als een maatstaf voor de mate van marktcompetitie binnen een land. Het geeft aan in hoeverre enkele bedrijven in staat zijn om de routing van het internetverkeer te controleren. In 2010 telde Nederland 2,36 AS-nummers per honderdduizend inwoners. Dat aantal steeg verder naar 3,01 in 2012 en 3,58 in 2014.[1)] In oktober 2017 was dat aantal gestegen naar 4,47 AS-nummers per honderdduizend inwoners.
De vanuit Nederland beheerde netwerken telden in totaal 1 376 015 servers of apparaten die op dat moment via een IP-adres publiek toegankelijke diensten leverden op het internet. In dit artikel waarin we ingaan op een aantal eigenschappen van het Nederlandse 'Internet of Things' (IoT), op basis van een op internet beschikbare bron, beperken we ons bij het geven van informatie tot deze 'Things' die zich dus op het internet kunnen identificeren via een uniek IP4-adres.[2)]

'Internet of Things'

Over wat precies gerekend moet worden tot het IoT wordt verschillend gedacht.[3)] Definities worden vooral beïnvloed door de invalshoeken die door de opsteller gekozen

1) Bron: OECD Digital Economy Outlook 2015.
2) De twee gekozen invalshoeken (vallend onder beheer van een Nederlands AS of Nederland als locatie van de apparaten) geven nog geen volledig beeld. Om een goed overzicht te krijgen van het IoT van Nederlandse bedrijven is ook nog informatie nodig waarmee IP-adressen aan Nederlandse bedrijven gekoppeld kunnen worden. Het CBS werkt wel aan een dergelijk register, maar momenteel is dit nog niet gereed. Ter illustratie: een in dit artikel geteld apparaat hoeft niet per se van een Nederlands bedrijf te zijn. Het kan bijvoorbeeld ook gaan om een apparaat dat door een Zweeds bedrijf via een Nederlandse ISP aan het Internet is verbonden. Eveneens zitten bijvoorbeeld niet in de telling servers die een Nederlands bedrijf via een buitenlandse ISP gebruikt en zich niet in een datacentrum in Nederland bevinden.
3) Op het concept 'Internet of Things' en verschillende definities wordt uitgebreid ingegaan in een publicatie van IEEE: 'Towards a definition of the Internet of Things (IoT)' uit mei 2015.

worden en maken daarmee zo'n definitie niet waardevrij. De in dit artikel gekozen aanpak is vooral ook praktisch van aard. De analyse is namelijk gebaseerd op één bron (Censys) die op basis van IP4-metingen het IoT wereldwijd in kaart brengt. Censys is een onafhankelijk organisatie en ook de naam van een website met een zoekmachine waarop informatie over 'hosts' en netwerken beschikbaar worden gesteld.[4)]

AS versus locatie

De omvang van het Nederlandse 'Internet of Things' (IoT) – geredeneerd vanuit de AS-indeling – bestaat dus uit bijna 1,4 miljoen 'Things'. Het merendeel (95 procent) daarvan betreft servers waarop bijvoorbeeld ook websites gehost worden die in geval van 'shared hosting' functioneren via een gedeeld (server) IP-adres. Elke server kan op zijn beurt ook weer onderdak bieden aan vele IP-adressen. Bij een server hoeft ook niet altijd gedacht te worden aan een fysieke computer. Zware fysieke computers kunnen softwarematig opgedeeld worden in meerdere virtuele servers die dan weer bereikbaar kunnen worden gemaakt via een eigen IP-adres. Dit verklaart het verschil in aantallen IP-adressen waarover in dit artikel gerapporteerd wordt en de aantallen beschikbare IP-adressen. De IP-adressen waarover we in dit artikel rapporteren representeren 'hosts'. Hosts zijn technisch gezien de kleinste zelfstandige onderdelen van het internet die voorzien zijn van een uniek IP-adres en zelfstandig data creëren, opslaan, ontvangen of verzenden (of een combi van meerdere van deze zaken). Elke 'host' beschikt over een eigen besturingssysteem dat gehackt kan worden en daarom goed beveiligd moet worden om misbruik te voorkomen. Communicatievoorzieningen zoals een wireless local area network (WLAN) access point hebben geen IP-adres en worden beschouwd als onderdeel van het fysieke netwerk waarop zij zijn aangesloten en dus niet als 'hosts'.
Van IP-adressen die toegerekend werden aan een vanuit Nederland beheerd AS was ook bekend waar de server of het apparaat zich daadwerkelijk fysiek bevond. 1 204 278 apparaten of servers (87,5 procent) bleken fysiek in Nederland aanwezig te zijn. Daarna kwamen als locaties naar boven: de Verenigde Staten (2,4 procent), Kroatië (1,4 procent), Rusland (1,3 procent), Duitsland (0,6 procent) en het Verenigd Koninkrijk (0,5 procent). Van 2,7 procent van de servers of apparaten was de locatie onbekend.
Het Nederlandse 'Internet of Things' kan in plaats van op basis van 'Autonomous Systems' ook bekeken worden vanuit het perspectief locatie. Onder IoT wordt dan verstaan de 'Things' die fysiek in Nederland aanwezig waren ongeacht of zij gelinkt waren aan een netwerk dat viel onder een AS dat tot het Nederlandse domein gerekend wordt. Dit perspectief levert een aanmerkelijk groter IoT op. Het aantal apparaten bedraagt dan niet meer circa 1,4 miljoen maar is opeens ruim 3,2 miljoen. Opvallend is dat de meeste 'Things' – bijna 63 procent – die in Nederland aanwezig zijn, gelinkt zijn met een onder buitenlandse beheer opererend netwerk (AS). Circa 54 procent van de Nederlandse 'Things' zijn gelinkt met vanuit de Verenigde Staten beheerde netwerken. Eén Amerikaans bedrijf alleen al is goed voor ruim 1,1 miljoen 'Things'. Nederland zelf komt dan op de tweede plaats met 37 procent en ver daarachter volgen Zweden, het Verenigd Koninkrijk en Duitsland met respectievelijk 3, 3 en 2 procent.
Bij de interpretatie van de cijfers over fysieke locatie moet rekening worden gehouden met het feit dat veel websites tegenwoordig ook gebruikmaken van een zogeheten

[4)] Uitgebreide informatie over Censys is te vinden in het volgende artikel van de makers van Censys: Zakir Durumeric, David Adrian, Ariana Mirian, Michael Bailey en J. Alex Halderman, A Search Engine Backed by {I}nternet-Wide Scanning, in Proceedings of the 22nd ACM Conference on Computer and Communications Security, oktober 2015.

Content Delivery Network (CDN). Dit betekent in de praktijk dat de website veelal gelinkt is met een grote Amerikaanse CDN waardoor het beheer administratief verschuift naar de Verenigde Staten terwijl de website technisch gezien aanwezig kan zijn op een server in een ander land. CDN's worden gebruikt om webcontent snel en efficiënt af te leveren bij eindgebruikers o.a. door kopieën van websites op te slaan zo dicht mogelijk bij eindgebruikers.

'Things'

Behalve servers registreert Censys ook andere soorten 'apparaten' ('things'). Na servers zijn 'NAS' en 'Soho router' de meest voorkomende apparaten die gemeten zijn. 'NAS' staat voor 'Network Attached Storage'. Het betreft externe harde schijven die via een IP-adres data wereldwijd beschikbaar stellen voor gebruikers die toegang hebben tot deze NAS. 'SOHO router' staat voor 'Small Office Home Office router'. Het gaat om breedband routers die gebruikt worden door kleine bedrijven om een Local Area Network (LAN) te bedienen. 'SCADA' gerelateerde apparaten krijgen doorgaans veel aandacht vanuit cybersecurity-perspectief. 'SCADA' staat voor 'Supervisory Control And Data Acquisition. SCADA-systemen bieden de mogelijkheid om industriële machines te controleren zoals motoren, generatoren en fysieke sensoren. SCADA-geschikte apparaten worden veel gebruikt in de industrie, in fabrieken maar ook in energiecentrales en waterbehandelingsinstallaties. Aanvallen op deze systemen kunnen dramatische gevolgen hebben. Modbus is een van de belangrijkste protocollen bij SCADA. Dit protocol was oorspronkelijk ontwikkeld voor kleinschalige lokale communicatie maar is steeds meer ook in gebruik geraakt op grotere netwerken en het internet.
Onderzoek van Censys wijst uit dat er wereldwijd, ondanks de aandacht die het probleem heeft, nog tal van Modbus-apparaten in verbinding staan met het internet waarbij de veiligheidssituatie nog niet optimaal is. Volgens Censys draaiden er in oktober 2017 in Nederland nog 250 industriële systemen waarbij gebruik wordt gemaakt van een SCADA-controler.
Met de groei van IoT nemen ook de kansen toe voor cybercriminelen om misbruik te maken van apparaten en servers. In het vervolg van deze bijdrage wordt ingegaan op een aantal van deze kwetsbaarheden zoals die uit de analyse van de Censys-data over Nederland naar voren kwamen.

Kwetsbaarheden bij het HTTPS-protocol

Secure Sockets Layer (SSL) en Transport Layer Security (TLS) zijn veiligheidsprotocollen om websites te beveiligen. Om van SSL/TLS gebruik te kunnen maken moet een certificaat geïnstalleerd worden op de server dat SSL/TLS ondersteunt. Met behulp van een dergelijk certificaat en het HTTPS-protocol kunnen browsers en servers encryptie en authenticatie gebruiken om veilig te communiceren. De eerste versies van SSL (1.0 en 2.0) bevatten een aantal kwetsbaarheden die aanvankelijk met versie 3.0 nog konden worden opgelost. Inmiddels wordt sinds 2015 ook het gebruik van SSL 3.0 afgeraden. TLS is daarmee de nieuwe veilige standaard geworden. Servers die dus nog gebruikmaken van SSL 2.0 en/of SSL 3.0 lopen risico's. Uit de analyse van de Censys-data kwam naar voren dat medio oktober 2017 van de 525 duizend onder Nederlands beheer vallende servers die HTTPS-verkeer aanbieden er nog bijna 170 duizend zijn waarop een van beide of beide versies geïnstalleerd is. Als we kijken naar de in Nederland aanwezig servers die HTTPS-verkeer

aanbieden (1,608 miljoen) dan gaat het om ruim 210 duizend servers, waarvan slechts 46 bij een overheidsorganisatie.
In 2014 werd een fout ontdekt in 'OpenSSL', de opensource-software die gebruikmaakt van SSL/TLS. Het wordt gebruikt door alle grote besturingssystemen zoals Windows en Linux en applicaties zoals browsers. Een nieuwe versie van het product (1.01.g) waarin het probleem was opgelost, werd op dezelfde dag beschikbaar gesteld. OpenSSL werd op dat moment veel gebruikt o.a. bij betalingen via iDEAL. Het lek kreeg de naam **'Heartbleed'** waarmee verwezen werd naar een klein onderdeel binnen de software (de heartbeat-extensie) dat het probleem veroorzaakte. De Censys-data tonen dat in oktober 2017 nog 1 975 van de onder Nederlands beheer vallende servers gebruikmaken van de OpenSSL-versie die de fout bevat. Als we kijken naar de in Nederland aanwezige servers dan gaat het om 2 505 servers, waarvan slechts één bij een overheidsorganisatie.
In 2015 kwamen onder de naam **'FREAK attack'** nieuwe problemen aan het licht die gerelateerd waren aan HTTPS-verkeer. Het probleem kon worden opgelost door ervoor te zorgen dat de server geen 'RSA-EXPORT cipher suites' accepteert. Een 'cipher suite' is een methode om het verkeer tussen een server en een client (browser) te versleutelen en te verwerken. Het gebruik van een aantal van deze cipher suites wordt inmiddels vanuit de beveiligingswereld afgeraden. Maar deze zijn vaak nog wel aanwezig op servers waardoor het omleiden en afluisteren van verkeer mogelijk is. In oktober 2017 accepteerden nog ruim 22 duizend van de onder Nederlands beheer vallende servers RSA-EXPORT cipher suites. Ruim 24 duizend van alle in Nederland aanwezige servers kenden deze kwetsbaarheid, waarvan drie bij een overheidsorganisatie.
'Logjam Attack' is een ander encryptie-lek dat zich in 2015 openbaarde en sterke overeenkomsten heeft met 'FREAK attack'. Bij dit lek doen zich problemen voor in de zogeheten 'Diffie-Helmann sleuteluitwisseling' bij het opzetten van een versleutelde verbinding. Het algoritme is niet alleen essentieel voor het HTTPS-protocol, maar o.a. ook voor SMTPS (mail) en SSH en protocollen die van TLS afhankelijk zijn. Alle mail- en webservers die 'Diffie-Hellman export encryptie' ondersteunen lopen risico's.
In oktober 2017 accepteerden nog ruim 16 duizend van de onder Nederlands beheer vallende servers deze vorm van encryptie. Bijna 18 duizend van alle in Nederland aanwezige servers kenden deze kwetsbaarheid, waarvan slechts één bij een overheidsorganisatie.

Dataencryptie

OpenSSH is een populaire opensource-implementatie van het SSH-protocol waarbij wachtwoorden en data met encryptie verstuurd kunnen worden om afluisteren, aanvallen en het ontsluiten van gevoelige informatie te voorkomen. Het draait op vrijwel alle besturingssystemen. Een versie van OpenSSH is aan te treffen op 214 duizend van de onder Nederlands beheer vallende servers en op ruim 363 duizend van de in Nederland aanwezige servers. Voor de servers die gelinkt zijn met een Nederlands 'Autonomous System' is met 51 505 installaties versie 5.3 de meest voorkomende versie is. Deze versie dateert uit oktober 2009. De op een na meest recente versie 7.5 was een half jaar na verschijnen (maart 2017) nog maar aanwezig op 1 770 servers. Het beeld voor de in Nederland aanwezige servers is enigszins anders. Versie 7.2p2 (maart 2016) is daar het meest geïnstalleerd met 72 600 installaties.
De laatste jaren is gebleken dat ook binnen OpenSSH beveiligingsissues aan de orde zijn die alleen voorkomen kunnen worden met regelmatige updates. Een ernstig probleem werd manifest begin 2016 toen bleek dat de OpenSSH versies 5.4 tot en met

7.1 niet konden voorkomen dat vanaf andere 'kwaadwillende' of gehackte servers SSH-sleutels uitgelezen konden worden bij inlogprocedures. Het probleem bij deze versies is met een kleine ingreep in de serverinstellingen wel oplosbaar maar het is niet waarschijnlijk dat dit op veel servers is doorgevoerd. Het probleem verklaart mogelijk wel waarom versie 7.2 nog redelijk hoog staat op de lijst van meest geïnstalleerde versies. In oktober 2017 werkten nog 99 015 servers die gelinkt zijn met een Nederlands 'Autonomous System' met een versie die kwetsbaar was voor dit probleem. Hoeveel servers daarvan alsnog de server hebben aangepast om het probleem te neutraliseren is niet bekend. Van alle in Nederland aanwezige servers werkten in oktober 2017 nog ruim 177 duizend servers met een kwetsbare versie. Het gebruik van OpenSSH bij overheidsorganisaties lijkt bijna niet voor te komen.
Het is niet zomaar mogelijk om uitsluitend op basis van de geïnstalleerde versie van OpenSSH te constateren dat kwetsbaarheden aan de orde zijn. Het is namelijk ook mogelijk om op basis van 'patches' (software of bestanden die software kunnen updaten) kwetsbaarheden in OpenSSH-versies op te lossen. De versie blijft dan hetzelfde, maar het probleem wordt verholpen. Er is geen onderzoek gedaan naar het gebruik van patches door beheerders van servers.

Experimenteel onderzoek

Bij het onderzoek is gebruikgemaakt van een database met informatie over apparatuur die was aangesloten op ruim 150 miljoen IP4-adressen wereldwijd. De kwaliteit van dit onderzoek is voor een belangrijk deel afhankelijk van de kwaliteit van de waarneming die is verricht door Censys. Er is door het CBS geen uitgebreid onderzoek gedaan naar deze kwaliteit. Dit artikel betreft dus bovenal een verkenning van het onderwerp en de bron en de uitkomsten wil het CBS daarom ook kwalificeren als experimenteel.

Annex met tabellen

A3.1 Bedrijven met ICT-veiligheidsmaatregelen, 2017

	Antivirus-software	Beleid voor sterke wacht-woor-den	Authen-ticatie via soft of hard-ware-token	Encryp-tie voor het opslaan van data	Encryp-tie voor het verstu-ren van data	Gege-vens op andere fysieke locatie	Net-work access con-trol	VPN bij internet-gebruik buiten het eigen	Log-bestan-den voor analyse inciden-ten	Methodes voor beoor-delen ICT-vei-ligheid	Risico-analy-ses	Andere maat-regelen
	% van bedrijven											
Totaal	87	57	26	21	21	71	31	29	31	22	22	14
Bedrijfsgrootte												
2 tot 10 werkzame personen	86	55	23	19	19	68	28	23	25	17	17	11
10 of meer werkzame personen	94	68	34	29	28	82	47	54	55	40	40	23
2 werkzame personen	84	54	21	17	18	64	23	18	20	14	14	10
3 tot 5 werkzame personen	87	54	25	20	20	69	29	24	25	18	19	11
5 tot 10 werkzame personen	87	59	27	22	21	74	36	30	34	24	22	14
10 tot 20 werkzame personen	92	61	27	23	22	77	39	42	42	31	29	16
20 tot 50 werkzame personen	95	68	34	28	28	85	49	57	60	41	42	23
50 tot 100 werkzame personen	96	78	44	36	36	89	57	70	72	52	56	31
100 tot 250 werkzame personen	98	86	56	47	45	92	66	80	82	62	64	41
250 tot 500 werkzame personen	98	92	65	54	56	94	65	82	86	70	72	50
500 of meer werkzame personen	98	94	78	61	67	95	70	89	90	74	77	62
Bedrijfstak												
Industrie	93	58	24	19	18	77	35	36	36	27	24	15
Energie & water	91	67	34	27	25	78	37	42	48	36	34	21
Bouw	85	50	17	14	13	64	20	20	20	16	16	10
Handel	88	57	21	17	16	66	29	26	29	19	20	12
Transport	84	56	22	15	14	61	23	23	26	18	20	11
Horeca	76	38	16	8	8	52	17	13	13	8	10	2
Informatie en communicatie	87	77	47	53	48	87	51	54	60	35	39	31
Financiële instellingen	88	74	45	35	29	75	48	51	50	41	38	24
Onroerend goed	80	51	28	22	23	69	36	34	31	25	22	15
Advies en onderzoek	90	67	31	26	24	83	38	36	39	28	25	17
Overige dienstverlening	83	56	20	19	18	70	29	25	29	21	20	12
Gezondheidszorg	97	66	47	39	46	84	46	37	39	29	31	23

Bron: CBS, ICT-gebruik bedrijven.

A3.2 Organisatie ICT-beveiliging; security patches (2017) en ICT-beveiligingswerk (2016)

	Uitvoeren van software-updates (security patches)			ICT-beveiligingswerk voornamelijk uitgevoerd door		
	meestal volledig automatisch	meestal (deels) handmatig	niet van toepassing	eigen personeel	externe leverancier(s)	niet van toepassing
Totaal	47	26	27	26	42	32
Bedrijfsgrootte						
2 tot 10 werkzame personen	47	24	29	26	38	36
10 of meer werkzame personen	51	33	17	28	58	14
2 werkzame personen	44	22	33	28	29	43
3 tot 5 werkzame personen	46	24	30	26	42	33
5 tot 10 werkzame personen	53	26	21	21	52	27
10 tot 20 werkzame personen	48	30	22	21	58	21
20 tot 50 werkzame personen	52	34	14	28	62	9
50 tot 100 werkzame personen	56	34	10	36	58	5
100 tot 250 werkzame personen	54	40	6	51	46	3
250 tot 500 werkzame personen	55	40	4	56	42	2
500 of meer werkzame personen	50	45	5	61	36	2
Bedrijfstak						
Industrie	48	29	23	24	49	27
Energie & water	48	26	26	24	56	20
Bouw	47	21	32	19	41	40
Handel	48	25	27	28	39	33
Transport	42	21	37	21	35	44
Horeca	33	17	50	19	26	55
Informatie en communicatie	48	40	12	65	20	15
Financiële instellingen	61	19	20	35	50	15
Onroerend goed	44	23	33	12	57	31
Advies en onderzoek	53	31	16	30	48	22
Overige dienstverlening	47	22	31	24	42	34
Gezondheidszorg	56	30	14	21	65	14

Bron: CBS, ICT-gebruik bedrijven.

A3.3 Gebruik van clouddiensten door personen, 2017

	Maakt gebruik van internet als opslagmedium	Soort van opgeslagen bestanden						Betaling voor opslaan van bestanden
		tekst, spreadsheets, presentaties	foto's	e-books of e-magazins	muziek	video's, film of tv programma's	andere bestanden	
	% personen vanaf 12 jaar							
Totaal personen	46	27	41	6	14	12	16	8
Geslacht								
Mannen	48	31	43	7	16	13	20	9
Vrouwen	43	23	39	6	12	10	12	7
Leeftijd								
12 tot 25 jaar	63	48	52	6	27	25	27	6
25 tot 45 jaar	59	35	54	9	15	14	20	12
45 tot 65 jaar	42	21	38	7	12	8	13	8
65 jaar of ouder	19	8	17	2	4	3	4	3
Onderwijsniveau								
Laag	33	18	28	3	13	10	10	3
Middelbaar	47	27	43	6	14	12	18	7
Hoog	60	39	54	11	14	13	19	14
Migratieachtergrond								
Nederland	46	26	40	6	13	10	15	8
met migratieachtergrond	44	26	39	8	14	10	16	10
met migratieachtergrond niet-westers	50	33	45	8	20	20	21	9
Inkomenskwintiel								
1e 20%-groep	45	31	37	5	14	10	19	5
2e 20%-groep	33	16	29	6	11	9	10	4
3e 20%-groep	42	24	38	6	14	13	13	5
4e 20%-groep	48	27	43	5	14	11	16	7
5e 20%-groep	56	36	52	10	16	13	20	16

Bron: CBS, ICT-gebruik huishoudens en personen.

A3.4 Beveiligingssoftware computers en mobiele telefoon of smartphone personen, 2017[1)]

	Computer				Mobiele telefoon of smartphone			
	inbegrepen bij besturingssysteem of automatisch geïnstalleerd	zelf geïnstalleerd of door iemand anders	geen beveiligingssoftware	weet niet	inbegrepen bij besturingssysteem of automatisch geïnstalleerd	zelf geïnstalleerd of door iemand anders	geen beveiligingssoftware	weet niet
	% personen vanaf 12 jaar met een computer en/of mobiele telefoon							
Totaal personen	35	54	4	7	32	20	24	24
Geslacht								
Mannen	37	55	4	4	36	22	25	17
Vrouwen	34	53	4	10	28	18	22	31
Leeftijd								
12 tot 25 jaar	35	48	6	11	30	17	25	28
25 tot 45 jaar	36	54	6	5	34	19	29	19
45 tot 65 jaar	33	58	2	6	34	24	19	23
65 jaar of ouder	39	52	1	8	29	19	23	30
Onderwijsniveau								
Laag	34	48	5	13	31	19	22	28
Middelbaar	35	57	3	5	32	21	25	22
Hoog	36	58	3	3	33	20	25	23

Bron: CBS, ICT-gebruik huishoudens en personen.

[1)] Computer (PC, desktop, laptop, notebook, tablet) of smartphone of mobiele telefoon voor privé-doeleinden met bijv. antivirus- of anti-spamprogramma's en/of firewall.

A4.1 Bedrijven met ICT-veiligheidsincidenten en de daaruit voortvloeiende kosten, 2016

		ICT-incidenten					
	Een of meer ICT-incidenten (totaal)	uitval door storing	uitval door aanval	vernietiging of verminking van data door storing	vernietiging of verminking van data door aanval	onthulling gegevens door aanval	onthulling gegevens door eigen personeel
	% van bedrijven						
ICT-veiligheidsincidenten							
Totaal	30	26	8	5	6	2	2
Bedrijfsgrootte							
2 tot 10 werkzame personen	26	21	6	5	4	1	2
10 of meer werkzame personen	50	43	13	8	13	3	4
2 werkzame personen	21	18	5	4	3	1	1
3 tot 5 werkzame personen	26	22	6	6	5	2	1
5 tot 10 werkzame personen	33	27	9	5	6	2	2
10 tot 20 werkzame personen	43	37	10	6	9	2	2
20 tot 50 werkzame personen	54	47	15	9	14	3	4
50 tot 100 werkzame personen	60	50	16	10	16	2	5
100 tot 250 werkzame personen	65	53	19	10	22	3	8
250 tot 500 werkzame personen	67	52	20	12	23	4	12
500 of meer werkzame personen	73	58	25	15	24	8	21
Bedrijfstak							
Industrie	36	29	8	7	9	2	5
Energie & water	35	22	9	5	9	2	2
Bouw	28	26	8	6	6	2	2
Handel	31	22	5	4	6	2	1
Transport	25	13	3	5	4	1	1
Horeca	17	28	12	6	5	1	3
Informatie en communicatie	35	28	12	6	4	1	3
Financiële instellingen	37	29	7	4	8	2	3
Onroerend goed	36	29	6	8	6	1	2
Advies en onderzoek	35	29	9	5	5	2	2
Overige dienstverlening	28	22	9	4	7	2	2
Gezondheidszorg	36	33	4	3	5	1	2
Kosten van ICT-veiligheidsincidenten							
Totaal	14	11	4	2	3	1	1
Bedrijfsgrootte							
2 tot 10 werkzame personen	11	8	3	3	2	0	1
10 of meer werkzame personen	25	19	7	4	6	2	1
2 werkzame personen	9	6	3	2	1	0	0
3 tot 5 werkzame personen	12	9	3	3	3	1	0
5 tot 10 werkzame personen	16	12	4	2	4	1	1
10 tot 20 werkzame personen	20	16	5	3	5	1	1
20 tot 50 werkzame personen	26	21	8	4	7	2	1
50 tot 100 werkzame personen	30	23	9	5	7	1	2
100 tot 250 werkzame personen	34	28	10	5	8	1	3
250 tot 500 werkzame personen	35	27	12	5	8	2	3
500 of meer werkzame personen	38	30	13	9	9	3	5

A4.1 Bedrijven met ICT-veiligheidsincidenten en de daaruit voortvloeiende kosten, 2016 (slot)

		ICT-incidenten					
	Een of meer ICT-incidenten (totaal)	uitval door storing	uitval door aanval	vernietiging of verminking van data door storing	vernietiging of verminking van data door aanval	onthulling gegevens door aanval	onthulling gegevens door eigen personeel
	% van bedrijven						
Bedrijfstak							
Industrie	19	14	6	3	5	1	1
Energie & water	18	12	3	4	5	0	3
Bouw	14	9	4	2	3	0	1
Handel	14	11	4	3	3	1	1
Transport	11	9	3	2	3	1	1
Horeca	6	5	1	2	2	0	0
Informatie en communicatie	13	10	5	2	2	0	0
Financiële instellingen	15	12	2	2	4	1	1
Onroerend goed	16	11	3	3	2	0	1
Advies en onderzoek	17	12	5	2	2	1	0
Overige dienstverlening	13	8	5	2	5	1	1
Gezondheidszorg	15	12	2	2	3	0	0

Bron: CBS, ICT-gebruik bedrijven.

A4.2 Melding van ICT-veiligheidsincidenten door bedrijven, 2016

		Gemeld bij			
	Melding gedaan	politie (aangifte)	autoriteit persoons-gegevens	sectoraal, nationaal of ander securityteam	bank
	% van bedrijven met een ICT-veiligheidsincident				
Totaal	7	3	2	2	3
Bedrijfsgrootte					
2 tot 10 werkzame personen	6	2	1	1	4
10 of meer werkzame personen	9	4	4	2	3
2 werkzame personen	6	2	0	1	4
3 tot 5 werkzame personen	5	2	1	2	3
5 tot 10 werkzame personen	5	2	1	1	4
10 tot 20 werkzame personen	7	3	2	2	4
20 tot 50 werkzame personen	7	3	2	1	2
50 tot 100 werkzame personen	9	4	5	1	2
100 tot 250 werkzame personen	14	7	7	2	2
250 tot 500 werkzame personen	23	10	14	4	1
500 of meer werkzame personen	41	15	32	8	3
Bedrijfstak					
Industrie	8	3	2	2	5
Energie & water	15	9	8	3	2
Bouw	8	3	1	3	4
Handel	7	3	2	2	4
Transport	10	4	0	0	10
Horeca	8	3	0	0	7
Informatie en communicatie	7	2	3	2	2
Financiële instellingen	7	2	5	3	2
Onroerend goed	8	4	3	1	1
Advies en onderzoek	4	1	1	1	2
Overige dienstverlening	6	3	1	0	3
Gezondheidszorg	5	2	5	1	1

Bron: CBS, ICT-gebruik bedrijven.

A. 5.1 Slachto ers cybercrime naar achtergrondkenmerken, 2017

	Identiteits-fraude	Marge	Koop- en verkoop-fraude	Marge	Hacken	Marge	Cyberpesten	Marge	Cybercrime totaal[1]	Marge
	% slachtoffers									
Totaal	1,0	0,0	3,9	0,1	4,9	0,2	3,1	0,1	11,0	0,2
Geslacht										
Man	0,4	0,1	4,0	0,2	5,5	0,3	3,0	0,2	11,6	0,4
Vrouw	0,3	0,1	3,7	0,2	4,3	0,2	3,2	0,2	10,4	0,3
Leeftijd										
15-24 jaar	0,1	0,1	5,3	0,5	6,7	0,6	7,4	0,6	17,3	0,9
25-44 jaar	0,5	0,1	5,6	0,3	5,5	0,3	3,4	0,3	13,2	0,5
45-64 jaar	0,4	0,1	3,6	0,2	4,5	0,2	2,3	0,2	9,9	0,4
65 jaar en ouder	0,4	0,1	0,9	0,1	3,4	0,2	1,2	0,1	5,4	0,3
Herkomst										
Autochtoon	0,4	0,0	3,9	0,2	5,0	0,2	3,0	0,2	11,0	0,3
Westerse allochtoon	0,5	0,2	3,5	0,4	5,1	0,5	2,6	0,4	10,5	0,7
Niet-westerse allochtoon	0,3	0,1	3,9	0,5	4,2	0,5	4,2	0,6	11,1	0,9
Opleiding										
Lager onderwijs	0,2	0,1	2,5	0,2	3,5	0,3	3,3	0,3	8,4	0,4
Middelbaar onderwijs	0,4	0,1	4,4	0,3	5,6	0,3	3,6	0,3	12,5	0,5
Hoger onderwijs	0,6	0,1	4,8	0,3	5,8	0,3	2,6	0,2	12,6	0,4
Seksuele geaardheid										
Homo	.	.	4,5	1,4	5,8	1,6	5,0	1,5	14,5	2,4
Lesbienne	0,4	0,4	4,2	1,7	5,5	1,9	6,3	2,2	14,4	3,1
Biseksuele man	0,3	0,2	3,3	1,2	6,8	1,9	4,4	1,7	13,1	2,5
Biseksuele vrouw	0,2	0,1	4,5	1,3	4,6	1,1	5,1	1,3	12,7	1,9
Hetero man	0,5	0,1	4,4	0,3	5,7	0,3	2,9	0,2	12,0	0,4
Hetero vrouw	0,4	0,1	4,3	0,3	4,7	0,3	3,4	0,2	11,4	0,4
Stedelijkheid										
Zeer sterk stedelijk	0,4	0,1	3,8	0,3	4,9	0,3	3,2	0,3	11,1	0,5
Sterk stedelijk	0,4	0,1	4,0	0,3	5,4	0,3	3,3	0,3	11,7	0,5
Matig stedelijk	0,3	0,1	3,6	0,3	4,9	0,4	3,2	0,3	10,9	0,6
Weinig stedelijk	0,4	0,1	3,9	0,3	4,1	0,3	2,8	0,3	10,2	0,5
Niet stedelijk	0,3	0,1	3,8	0,5	4,7	0,6	2,6	0,4	10,4	0,8

Bron: CBS, Veiligheidsmonitor

[1] In het onderzoek is naar een gelimiteerd aantal typen cybercrimedelicten gevraagd (identiteitsfraude, hacken, koop- en verkoopfraude, cyberpesten).

A 5.2 Melding en aangifte cybercrime naar delictsoort

	2012		2013		2014		2015		2016		2017	
	In % delicten	Marge	In % delicten	Marge	In % delicten	Marge	In % delicten	Marge	In % delicten	Marge	In % delicten	Marge
Cybercrime totaal[1]												
Melding totaal[2]	31,4	1,4	29,6	1,1	27,7	1,2	26,9	1,2	26,9	1,3	27,0	1,1
bij politie	12,7	1,0	13,3	0,8	12,7	0,9	12,7	1,0	13,1	1,0	13,1	0,8
bij andere instantie	21,4	1,2	19,1	0,9	17,2	1,0	16,4	1,0	16,0	1,0	16,5	0,9
Aangifte totaal	7,1	0,7	7,4	0,6	7,3	0,7	7,8	0,7	7,6	0,7	8,0	0,6
via procesverbaal	4,4	0,6	4,3	0,5	3,8	0,5	4,1	0,6	3,6	0,5	4,4	0,5
via internet	2,7	0,4	3,1	0,3	3,5	0,4	3,7	0,4	4,1	0,5	3,6	0,4
Identiteitsfraude												
Melding totaal	90,1	2,6	89,0	2,6	87,6	4,1	84,0	5,3	81,9	7,0	86,0	5,4
bij politie	16,7	3,0	17,6	2,9	14,4	3,5	20,4	6,3	23,1	6,4	20,6	5,3
bij bank/financiële instelling	85,2	1,7	82,6	3,0	79,6	4,6	71,9	6,6	68,5	7,5	70,3	6,2
bij andere instantie	3,2	2,6	3,3	1,4	4,1	2,2	8,7	4,6	7,9	4,3	14,8	5,0
Aangifte totaal	12,5	2,7	13,0	2,6	11,6	3,2	13,1	4,6	16,9	5,7	16,0	4,7
via procesverbaal	11,7	2,7	10,9	2,5	9,7	2,9	11,2	4,4	16,0	5,6	14,4	4,6
via internet	0,9	0,6	2,0	1,0	1,9	1,2	2,0	1,4	0,9	0,9	1,6	1,1
Koop- en verkoopfraude												
Melding totaal	40,4	2,8	44,4	2,2	40,9	2,4	39,1	2,4	39,8	2,5	39,7	2,1
bij politie	24,2	2,5	26,4	2,0	24,2	2,1	23,4	2,0	23,6	2,1	23,5	1,8
bij consumentenorganistatie	7,0	1,5	8,4	1,2	5,2	1,1	5,2	1,1	3,9	0,8	5,4	1,0
bij andere instantie	16,6	2,0	17,7	1,7	16,6	1,9	16,4	1,8	17,2	1,9	17,2	1,6
Aangifte totaal	20,5	2,3	22,6	1,9	20,1	1,9	20,0	1,9	20,2	2,0	19,0	1,6
via procesverbaal	8,0	1,5	9,0	1,3	7,0	1,2	6,3	1,2	5,6	1,1	6,8	1,1
via internet	12,6	1,9	13,6	1,5	13,0	1,6	13,7	1,6	14,6	1,8	12,2	1,3
Hacken												
Melding totaal	22,1	1,8	19,8	1,3	18,8	1,5	18,4	1,5	20,4	1,7	20,0	1,5
bij politie	5,9	1,0	6,7	0,8	4,9	0,8	4,3	0,8	5,3	1,0	5,1	0,8
bij andere instantie	16,8	1,6	13,5	1,1	14,3	1,4	14,7	1,4	15,7	1,5	15,7	1,4
Aangifte totaal	2,4	0,7	1,8	0,4	1,8	0,5	1,8	0,5	2,3	0,6	2,7	0,6
via procesverbaal	1,7	0,6	1,2	0,4	1,0	0,4	1,1	0,4	1,2	0,4	1,8	0,5
via internet	0,7	0,3	0,6	0,2	0,9	0,4	0,7	0,3	1,0	0,5	0,9	0,3
Cyberpesten												
Melding totaal	23,4	2,7	21,7	2,1	23,1	2,4	23,9	2,4	22,1	2,4	22,6	2,1
bij politie	14,9	2,4	14,3	1,8	15,1	2,0	15,2	2,0	14,8	2,0	14,5	1,8
bij andere instantie	9,7	1,8	9,6	1,5	10,5	1,7	10,3	1,7	9,4	1,7	10,5	1,6
Aangifte totaal	5,0	1,4	5,3	1,2	5,4	1,2	6,4	1,5	4,9	1,2	5,7	1,1
via procesverbaal	4,5	1,3	4,7	1,1	4,6	1,2	5,8	1,5	4,1	1,1	5,1	1,1
via internet	0,5	0,5	0,6	0,4	0,8	0,5	0,6	0,4	0,8	0,5	0,6	0,3

Bron: CBS, Veiligheidsmonitor.

[1] In het onderzoek is naar een gelimiteerd aantal typen cybercrimedelicten gevraagd (identiteitsfraude, hacken, koop- en verkoopfraude, cyberpesten).

[2] Melding totaal omvat melding bij politie en/of melding bij andere onder identiteitsfraude, koop/verkoopfraude, hacken, cyberpesten genoemde instanties.

A 5.3 Cybercrimedelicten naar soort[1)]

	2012		2013		2014		2015		2016		2017	
	Per 100 inwoners	Marge	Per 100 inwoners	Marge	Per 100 inwoners	Marge	Per 100 inwoners	Marge	Per 100 inwoners	Marge	Per 100 inwoners	Marge
Cybercrime totaal[1]	19,7	0,6	20,8	0,5	18,8	0,5	18,7	0,5	17,9	0,5	18,6	0,5
Identiteitsfraude	1,6	0,1	1,3	0,1	0,7	0,1	0,6	0,1	0,4	0,1	0,4	0,0
waarvan												
skimming	1,1	0,1	0,8	0,1	0,4	0,1	0,2	0,0	0,1	0,0	0,1	0,0
phishing/pharming	0,5	0,1	0,5	0,1	0,4	0,1	0,4	0,1	0,3	0,1	0,3	0,0
Koop- en verkoopfraude	3,4	0,2	3,9	0,2	4,1	0,2	4,2	0,2	4,0	0,2	4,6	0,2
waarvan												
koopfraude	3,2	0,2	3,7	0,2	3,9	0,2	4,0	0,2	3,9	0,2	4,3	0,2
verkoopfraude	0,2	0,1	0,2	0,1	0,2	0,0	0,2	0,0	0,2	0,1	0,3	0,1
Hacken	8,8	0,4	9,3	0,3	7,9	0,3	7,6	0,3	7,3	0,3	7,5	0,3
waarvan												
ingebroken op computer	1,5	0,2	1,5	0,1	1,2	0,1	1,1	0,1	1,0	0,1	0,9	0,1
ingebroken op emailaccount	3,9	0,3	3,5	0,2	3,2	0,2	2,7	0,2	2,5	0,2	2,3	0,2
ingebroken op website/profielsite	2,2	0,2	2,5	0,2	2,1	0,2	2,4	0,2	2,5	0,2	2,6	0,2
anders	3,3	0,2	2,7	0,2	2,1	0,2	2,1	0,2	2,1	0,2	2,2	0,2
Cyberpesten	5,9	0,4	6,3	0,3	6,0	0,3	6,3	0,3	6,0	0,3	6,1	0,3
waarvan												
laster	1,8	0,2	2,0	0,2	1,8	0,2	1,8	0,2	1,7	0,2	1,9	0,2
stalken	1,6	0,2	1,5	0,2	1,6	0,2	1,9	0,2	1,5	0,2	1,7	0,2
chantage	0,5	0,1	0,3	0,1	0,4	0,1	0,6	0,1	0,4	0,1	0,5	0,1
bedreiging met geweld	1,0	0,2	1,1	0,1	1,0	0,1	1,1	0,2	1,1	0,2	1,2	0,1
anders	2,2	0,2	2,3	0,2	2,2	0,2	2,2	0,2	2,2	0,2	2,2	0,2

Bron: CBS, Veiligheidsmonitor.

[1)] In het onderzoek is naar een gelimiteerd aantal typen cybercrimedelicten gevraagd (identiteitsfraude, hacken, koop- en verkoopfraude, cyberpesten).