Cybersecuritymonitor

2017

Een eerste verkenning van dreigingen, incidenten en maatregelen

Cybersecuritymonitor

2017

Een eerste verkenning van dreigingen, incidenten en maatregelen

Verklaring van tekens

Niets (blanco)	Een cijfer kan op logische gronden niet voorkomen
.	Het cijfer is onbekend, onvoldoende betrouwbaar of geheim
*	Voorlopige cijfers
**	Nader voorlopige cijfers
2016–2017	2016 tot en met 2017
2016/2017	Het gemiddelde over de jaren 2016 tot en met 2017
2016/'17	Oogstjaar, boekjaar, schooljaar enz., beginnend in 2016 en eindigend in 2017
2014/'15–2016/'17	Oogstjaar, boekjaar, enz., 2014/'15 tot en met 2016/'17

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
Ontwerp: Edenspiekermann

Inlichtingen
Tel. 088 570 70 70
Via contactformulier: www.cbs.nl/infoservice

ISBN 978-90-357-2147-0

Inhoud

Samenvatting **5**

1. Waarom een cybersecuritymonitor? 9

2. Hoe te komen tot een cybersecuritymonitor? 11

2.1 Begripsvorming rondom cybersecurity **13**
2.2 Op zoek naar indicatoren **16**

3. Cybersecurity, maatregelen 18

3.1 Bedrijven **19**
3.2 Personen **24**
3.3 Internetstandaarden voor websites **26**

4. Cybersecurity, incidenten 27

5. Cybercrime 31

6. Bronnen 37

7. Editie 2018 41

Referenties **43**
Annex met tabellen **44**

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 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 eerste publicatie over cybersecurity van 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 er tegen 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 wel op termijn te komen tot een vollediger *Cybersecuritymonitor* die een evenwichtig beeld geeft van de situatie in Nederland.

Cybersecuritymaatregelen

- Een op de drie bedrijven (31 procent) had in 2015 een formeel vastgelegd ICT-beveiligingsbeleid.
- Bij 85 procent van de bedrijven was in 2015 sprake van werkzaamheden op het terrein van ICT-beveiliging. Drie kwart van deze bedrijven (74 procent) laat deze werkzaamheden voornamelijk door derden verzorgen.
- Ruim een derde van de bedrijven (35 procent) maakte in 2016 gebruik van betaalde cloud-diensten. De helft van deze bedrijven (49 procent) gebruikte hierbij een apart voor het bedrijf gereserveerde server.
- Eind september 2016 maakte 45 procent van de .nl-domeinnamen gebruik van DNSSEC; een beveiligingsstandaard die o.a. *phishing* en *pharming* bemoeilijkt.
- Ruim de helft (52 procent) van de Nederlanders heeft in 2015 wel eens afgezien van bepaalde internetactiviteiten omdat zij zich zorgen maakten om de veiligheid.
- Een op de drie Nederlanders (34 procent) veranderde in 2016 wel eens de instellingen van de browser om cookies te voorkomen of te beperken.
- In 2015 maakte ruim de helft (55 procent) van de Nederlanders reservekopieën of *back-ups* van bestanden, afbeeldingen e.d. die op hun computer staan.

Cybersecurityincidenten

- 8 procent van de Nederlanders had in 2015 te maken met veiligheidsincidenten op internet zoals computervirussen, misbruik van persoonlijke gegevens of fraude.
- In 2016 had 3 procent van de Nederlanders die online iets kochten te maken met fraude.
- In 2016 ontving de Autoriteit Persoonsgegevens 5 617 meldingen van datalekken. 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 kwaadwillenden (een hack).
- In 2015 waren er 39 meldingen van verstoringen van de continuïteit van openbare telecomdiensten bij het Agentschap Telecom. 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 de tweede helft van 2016 had 13 procent een omvang van meer dan 10 gbps. Dit percentage is ongeveer gelijk aan dat in 2015. Ruim een op de drie DDos-aanvallen (36 procent) duurde langer dan een uur. Dit aandeel is groter dan in 2015.
  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 2015 is 0,6 procent van de Nederlanders slachtoffer geworden van identiteitsfraude. In 84 procent van de gevallen werd dit gemeld bij een officiële instantie, in 72 procent van de gevallen bij een bank of financiële instelling en in 20 procent van de gevallen (ook) bij de politie.
– 3,5 procent van de 15-plussers werd opgelicht bij het online shoppen, bij 0,6 procent gebeurde dit zelfs meer dan eens. In 39 procent van de gevallen werd dit gemeld bij een officiële instantie, in 23 procent van de gevallen (ook) bij de politie.
– In 2015 is 5,1 procent van de 15-plussers gehackt. In 4 procent van de gevallen werd dit gemeld bij de politie, in 15 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 3,2 procent van de Nederlanders last. Met name jongeren, vrouwen en laagopgeleiden worden vaak gepest. In bijna een kwart (24 procent) van de gevallen werd het incident gemeld bij de politie of een andere instantie.
– In 2015 was een op de negen Nederlanders (11 procent) slachtoffer van een of meer van de volgende cyberdelicten: identiteitsfraude, koop- en verkoopfraude, hacken of cyberpesten. Bijna drie kwart van deze delicten werd niet gemeld.
– In 2015 werd 2 175 keer aangifte gedaan van computervredebreuk. Hiervan werd 4,6 procent opgehelderd.

Kerntabel indicatoren cybersecurity

Indicator		Eenheid	Bron	Verslagperiode
Cybersecurity, maatregelen				
Bedrijven met ICT-beveiligingsbeleid	31	**% bedrijven**[1]	CBS	2015
waaronder 12 maanden of korter geleden geactualiseerd	67	**% bedrijven met ICT-beveiligingsbeleid**		
ICT-beveiliging en bescherming van data door bedrijven	85	**% bedrijven**[1]	CBS	2015
waarvan voornamelijk uitgevoerd door				
eigen personeel	26	**% bedrijven met ICT-beveiliging**		
externe leverancier(s)	74	**% bedrijven met ICT-beveiliging**		
Bedrijven die gebruikmaken van betaalde clouddiensten	35	**% bedrijven**[1]	CBS	2016
waarvan op				
gedeelde servers en/of	74	**% bedrijven met clouddiensten**		
servers uitsluitend gereserveerd voor het bedrijf	49	**% bedrijven met clouddiensten**		
Bedrijven die om veiligheidsredenen niet of maar beperkt via een website/app verkopen	19	**% bedrijven**[1]	CBS	2016
Beperkt internetgebruik door zorgen over veiligheid/ incidenten[2]	52	**% personen vanaf 12 jaar**	CBS	2015
Verandert instellingen browser om cookies tegen te gaan of te verminderen	34	**% personen vanaf 12 jaar**	CBS	2016
Maakt reservekopieën of *back-ups* van bestanden, afbeeldingen e.d. die op de computer staan	61	**% personen vanaf 12 jaar**	CBS	2015
Websites in het .nl-domein die gebruikmaken van DNSSEC	45	**% van .nl domeinnamen**	SIDN	2016 (Per 30-9)
Cybersecurity, incidenten				
Geconfronteerd met veiligheidsincidenten op internet[3]	8	**% personen vanaf 12 jaar**	CBS	2015
Fraude bij online aankopen (bijvoorbeeld geen levering of misbruik van creditcardgegevens)	3	**% personen die de afgelopen 12 maanden online aankopen deden**	CBS	2016
Meldingen in het kader van de meldplicht datalekken zoals opgenomen in de Wet bescherming persoonsgegevens	5617	**Aantal meldingen (excl. ingetrokken meldingen)**	Autoriteit Persoons-gegevens	2016
Meldingen in het kader van de zorg- en meldplicht van aanbieders van openbare telecommunicatienetwerken of -diensten zoals opgenomen in de Telecommunicatiewet	39	**Aantal incidenten**	Agentschap Telecom	2015
Omvang en duur (verijdelde) DDos-aanvallen[4]			NBIP	2016
waarvan				(1-07 tot en met 14-12)
> 10 gbps	13	**% van totaal**		
> 1 uur	36	**% van totaal**		
Cybercrime				
Ondervonden delicten cybercrime[5]	19	**Per 100 inwoners**	CBS	2015
Slachtofferschap cybercrime[5]	11	**% personen vanaf 15 jaar**	CBS	2015
Meldingen cybercrime[5]	27	**% van ondervonden delicten**	CBS	2015
Meldingen bij politie[5]	13	**% van ondervonden delicten**	CBS	2015
Aangifte totaal[2]	8	**% van ondervonden delicten**	CBS	2015
waarvan identiteitsfraude totaal	1	**Per 100 inwoners**		2015
slachtoffers	1	**% personen vanaf 15 jaar**		2015
melding totaal	84	**% van ondervonden delicten**		2015
melding bij politie	20	**% van ondervonden delicten**		2015
aangifte totaal	13	**% van ondervonden delicten**		2015
koop- en verkoopfraude totaal	4	**Per 100 inwoners**		2015
slachtoffers	4	**% personen vanaf 15 jaar**		2015
melding totaal	39	**% van ondervonden delicten**		2015
melding bij politie	23	**% van ondervonden delicten**		2015
aangifte totaal	20	**% van ondervonden delicten**		2015

Kerntabel indicatoren cybersecurity (slot)

Indicator		Eenheid	Bron	Verslagperiode
hacken totaal	8	**Per 100 inwoners**		2015
slachtoffers	5	**% personen vanaf 15 jaar**		2015
melding totaal	18	**% van ondervonden delicten**		2015
melding bij politie	4	**% van ondervonden delicten**		2015
aangifte totaal	2	**% van ondervonden delicten**		2015
cyberpesten totaal	6	**Per 100 inwoners**		2015
slachtoffers	3	**% personen vanaf 15 jaar**		2015
melding totaal	24	**% van ondervonden delicten**		2015
melding bij politie	15	**% van ondervonden delicten**		2015
aangifte totaal	6	**% van ondervonden delicten**		2015
Computervredebreuk				
Totaal geregistreerde misdrijven	2 175	**Aantal**	CBS	2015
Geregistreerde misdrijven, relatief	0,0	**% van totaal geregistreerde misdrijven**		2015
Geregistreerde misdrijven per 1 000 inwoners	0,1	**Per 1 000 inwoners**		2015
Totaal opgehelderde misdrijven	100	**Aantal**	CBS	2015
Opgehelderde misdrijven, relatief	4,6	**% van totaal geregistreerde misdrijven**		2015
Totaal geregistreerde verdachten	155	**Aantal**	CBS	2015

[1] Bedrijven met tien of meer werkzame personen.

[2] In het onderzoek is deze vraag voor een gelimiteerd aantal typen internetactiviteiten gesteld: persoonlijke informatie op netwerksites plaatsen, bestanden downloaden, draadloos internet gebruiken elders dan thuis, online winkelen voor persoonlijk gebruik, bankzaken uitvoeren, communiceren met overheidsinstellingen. Betreft de 12 maanden voorafgaande aan het onderzoek.

[3] In het onderzoek is naar een gelimiteerd aantal typen veiligheidsincidenten gevraagd; computervirus waardoor gegevens verloren gingen, misbruik van persoonlijke gegevens of andere privacyschending, financiële schade (door *phishing*, *pharming*, fraude met betaalkaarten). Betreft de 12 maanden voorafgaande aan het onderzoek.

[4] Heeft betrekking op de bij de NBIP aangesloten internetproviders die gebruikmaken van de Nationale anti-DDos Wasstraat (NaWas).

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

1.

Waarom een cyber-securitymonitor?

Anno 2017 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 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.

Tegen deze achtergrond is bij 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 eerste 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. 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 kennen, en deze vervolgens te categoriseren. Dit lijkt een moeizamer 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 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.

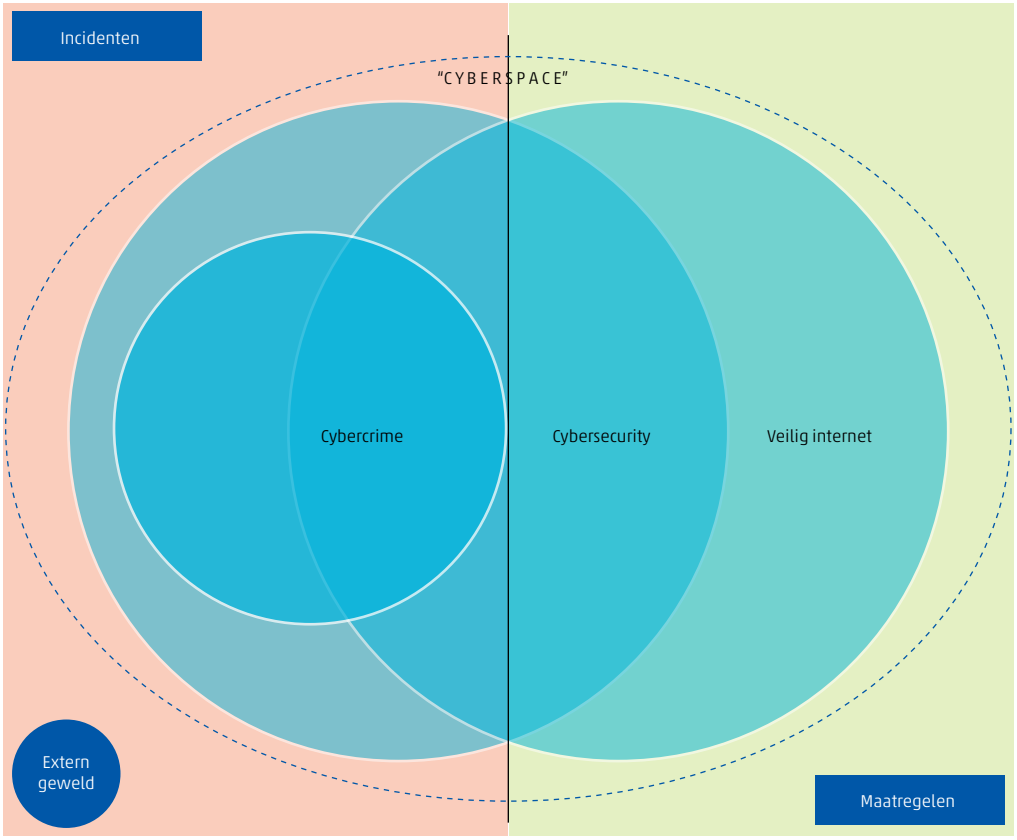
In het vervolg zal de geschetste werkwijze concreter worden toegelicht en uitgewerkt.

[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.

2.1.1 Contextdiagram cybersecurity en gerelateerde begrippen



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.

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 bankrekening wordt geplunderd. 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 CBS gehanteerde classificatie nog niet 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 manifesteren zich 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 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 kwaadwillenden 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 een zelfde 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 eerste 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 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 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 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 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 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. 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. Een eerste selectie van indicatoren voor deze publicatie heeft geleid tot 23 indicatoren waarvan 19 afkomstig van CBS en 4 van andere partijen. Deze indicatoren worden in drie hoofdstukken gepresenteerd. Dertien indicatoren in het domein cybersecurity waarvan acht betreffende de preventieve maatregelen (hoofdstuk 3) en vijf met betrekking tot incidenten (hoofdstuk 4). De resterende tien indicatoren vallen in het domein cybercrime en worden in hoofdstuk 5 gepresenteerd.

3. Cybersecurity, maatregelen

In tabel 3.0.1 zijn maatregelen opgesomd die bedrijven en personen nemen om incidenten op het terrein van cybersecurity te voorkomen of te weten hoe te handelen als zich een incident heeft voorgedaan. Deze maatregelen variëren van het aanpassen van het internetgedrag, het adresseren van veiligheidsrisico's in een formeel vastgelegd beveiligingsbeleid tot en met het nemen van specifieke ICT-technische maatregelen.

3.0.1 Cybersecurity, maatregelen

Indicator	2014	2015	2016	Eenheid	Bron
Bedrijven met ICT-beveiligingsbeleid	.	31	.	**% bedrijven**[1]	CBS
waaronder 12 maanden of korter geleden geactualiseerd	.	67	.	**% bedrijven met ICT-beveiligingsbeleid**	
ICT-beveiliging en bescherming van data door bedrijven	88	85	.	**% bedrijven**[1]	CBS
waarvan voornamelijk uitgevoerd door					
eigen personeel	26	26	.	**% bedrijven met ICT-beveiliging**	
externe leverancier(s)	74	74	.	**% bedrijven met ICT-beveiliging**	
Bedrijven die gebruikmaken van betaalde clouddiensten	28	.	35	**% bedrijven**[1]	CBS
waarvan 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**[1]	CBS
Beperkt internetgebruik door zorgen over veiligheid/incidenten[2]	.	52	.	**% personen vanaf 12 jaar**	CBS
Verandert instellingen browser om cookies tegen te gaan of te verminderen	.	36	34	**% personen vanaf 12 jaar**	CBS
Maakt reservekopieën of *back-ups* van bestanden, afbeeldingen e.d. die op de computer staan	.	61	.	**% personen vanaf 12 jaar**	CBS
Websites in het .nl-domein die gebruikmaken van DNSSEC[3]	34	44	45	**% van .nl domeinnamen**	SIDN

[1] Bedrijven met tien of meer werkzame personen.

[2] In het onderzoek is deze vraag voor een gelimiteerd aantal typen internetactiviteiten gesteld: persoonlijke informatie op netwerksites plaatsen, bestanden downloaden, draadloos internet gebruiken elders dan thuis, online winkelen voor persoonlijk gebruik, bankzaken uitvoeren, communiceren met overheidsinstellingen. Betreft de 12 maanden voorafgaande aan het onderzoek.

[3] Per 30-9.

3.1 Bedrijven

Voor bedrijven zijn drie maatregelen opgenomen die van invloed zijn op de cybersecurity van deze bedrijven. Ten eerste is aan bedrijven gevraagd of ze beschikken over een formeel vastgelegd ICT-beveiligingsbeleid waarin verschillende aspecten van cybersecurity worden behandeld. Een formeel vastgelegd ICT-beveiligingsbeleid geeft aan dat cybersecurity onderwerp van gesprek is binnen een bedrijf. Het getuigt van een zeker bewustzijn dat informatiebeveiliging en beveiliging van ICT-systemen niet vanzelfsprekend zijn. In 2015 had 31 procent van de bedrijven in Nederland een formeel vastgelegd ICT-beveiligingsbeleid.
Een tweede indicator betreft de aanwezigheid van ICT-werkzaamheden op het terrein van ICT-beveiliging en de bescherming van data. 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? In 2015 was er bij 85 procent van de bedrijven sprake van aanwijsbare werkzaamheden op het terrein van ICT-beveiliging en de bescherming van data. In drie kwart van de gevallen werd dit werk 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 A 3.2 achter in deze publicatie).
Een derde indicator is het gebruik van betaalde cloud-diensten 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 bedrijf is immers veiliger. In 2016 maakte een op de drie bedrijven gebruik van betaalde cloud-diensten. Drie kwart van deze bedrijven maakte hierbij gebruik van gedeelde servers. De helft 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.

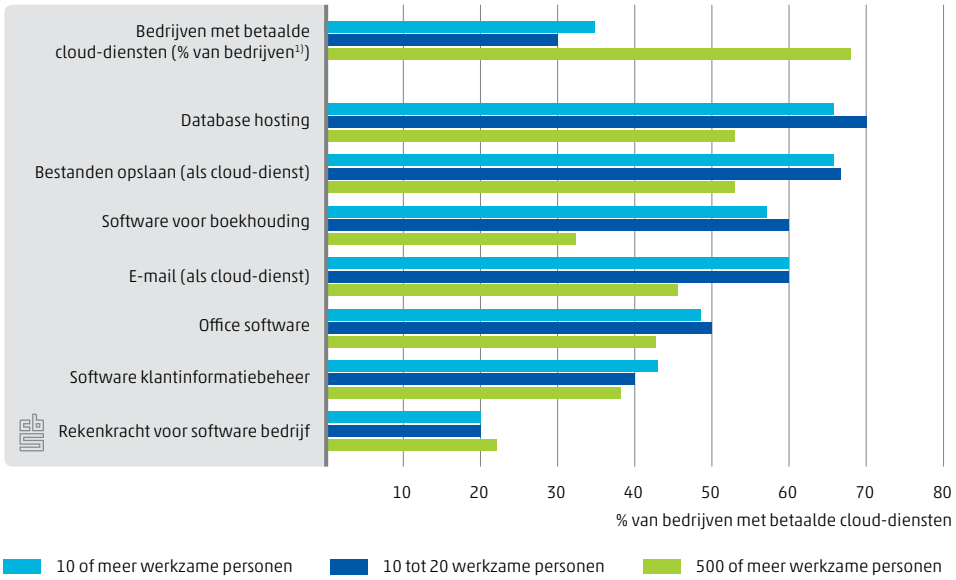
Grotere bedrijven selectiever in gebruik cloud-diensten

In figuur 3.1.1 is voor de grootste en de kleinste bedrijven aangegeven van welke soort cloud-diensten ze gebruikmaken. Hoewel bedrijven met 10 tot 20 werkzame personen minder vaak van cloud-diensten gebruikmaken (30 procent) dan de bedrijven met 500 of meer werkzame personen (68 procent), maken de kleinere bedrijven wel gebruik van meer verschillende typen cloud-diensten. Het gemiddelde aantal cloud-diensten per bedrijf was voor deze groep 3,7; voor de grootste bedrijven was dit 2,9. Anders geformuleerd: twee derde van de kleinere bedrijven maakte gebruik van drie of meer soorten cloud-diensten; voor de grote bedrijven was dit net iets meer dan de helft. Kennelijk maken grote bedrijven selectiever gebruik van cloud-diensten, bijvoorbeeld omdat ze meer zelf kunnen. Alleen bij de vergroting van de rekenkracht scoren de grote bedrijven (relatief) hoger (zie ook tabel A 3.3 achter in deze publicatie).

In 2014 is aan bedrijven gevraagd waarom ze géén, of maar beperkt, gebruikmaken van cloud-diensten. Met name de grotere bedrijven gaven aan dat beveiligingsrisico's een belangrijke rol speelden; 30 procent van de bedrijven met 500 of meer werkzame personen gaf aan geen gebruik te maken van cloud-diensten vanwege veiligheidsrisico's; 37 procent van deze bedrijven gaf aan maar beperkt gebruik te maken van cloud-diensten vanwege veiligheidsrisico's. Bij bedrijven met 10 tot 20 werkzame personen bedroegen deze percentage respectievelijk 25 procent en 9 procent (zie ook tabel A 3.4 achter in deze publicatie). Voor de goede orde: het gaat hier om beveiligingsrisico's die 'tegen' het gebruik van cloud-diensten pleiten. Cloud-diensten worden dus door een deel van de bedrijven als onveiliger beschouwd dan het in eigen beheer of anderszins verzorgen van dezelfde ICT-diensten. Dit beeld is consistent met hetgeen hiervoor is opgemerkt over het selectievere gebruik van cloud-diensten door grotere bedrijven. Het kan zijn dat grotere bedrijven beveiligingsrisico's zwaarder laten wegen bij de beslissing om cloud-diensten af te nemen. Het kan ook zijn dat grotere bedrijven

gewoonweg meer beveiligingsrisco's hebben waardoor de balans vaker doorslaat naar het in eigen beheer houden van de ICT-werkzaamheden. Ten slotte zullen grote bedrijven ook eerder de middelen en de kennis en kunde in huis hebben om ICT-werkzaamheden in eigen beheer te kunnen doen.

3.1.1 Bedrijven met betaalde cloud-diensten, 2016

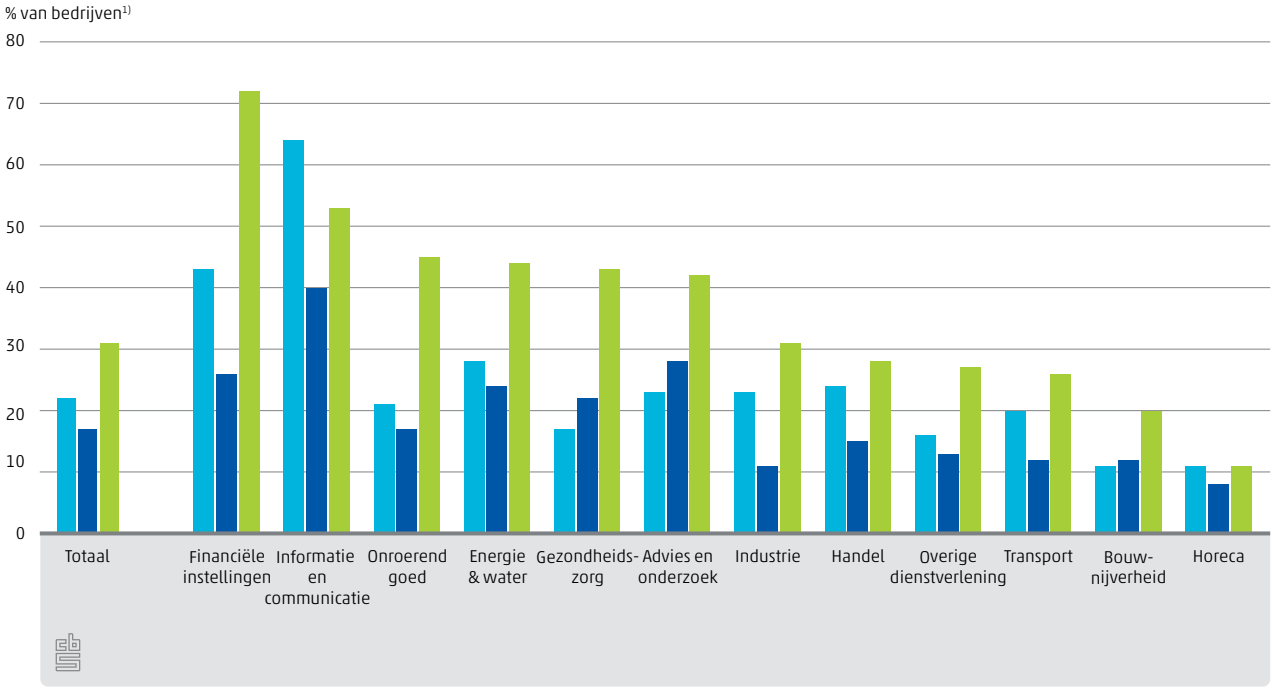


Bron: CBS, ICT-gebruik bedrijven.
[1] Bedrijven met tien of meer werkzame personen.

Verschillen tussen bedrijfstakken groot

In figuur 3.1.2 zijn de drie onderscheiden cybersecuritymaatregelen van bedrijven weergegeven per bedrijfstak. Dit levert een plausibel beeld op. De 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. Van de financiële instellingen had bijvoorbeeld 72 procent een formeel plan voor de ICT-beveiliging, tegen 11 procent van de horecabedrijven. De bedrijfstak informatie en communicatie scoort het hoogst op het uitvoeren van ICT-beveiligingswerk met eigen personeel en het gebruik van een eigen server bij het afnemen van cloud-diensten. Gezien de aard van het werk in deze bedrijfstak en de daarmee gepaard gaande kennis is dit niet zo verwonderlijk. De horeca, maar ook de bouwnijverheid, zijn de bedrijfstakken die het laagst scoren op de hier gepresenteerde maatregelen. Bedrijven maken overigens verschillende afwegingen bij de vraag welke maatregelen genomen moeten worden en welke cloud-diensten zij willen gebruiken. 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.

3.1.2 Cybersecuritymaatregelen bedrijven, naar bedrijfstak

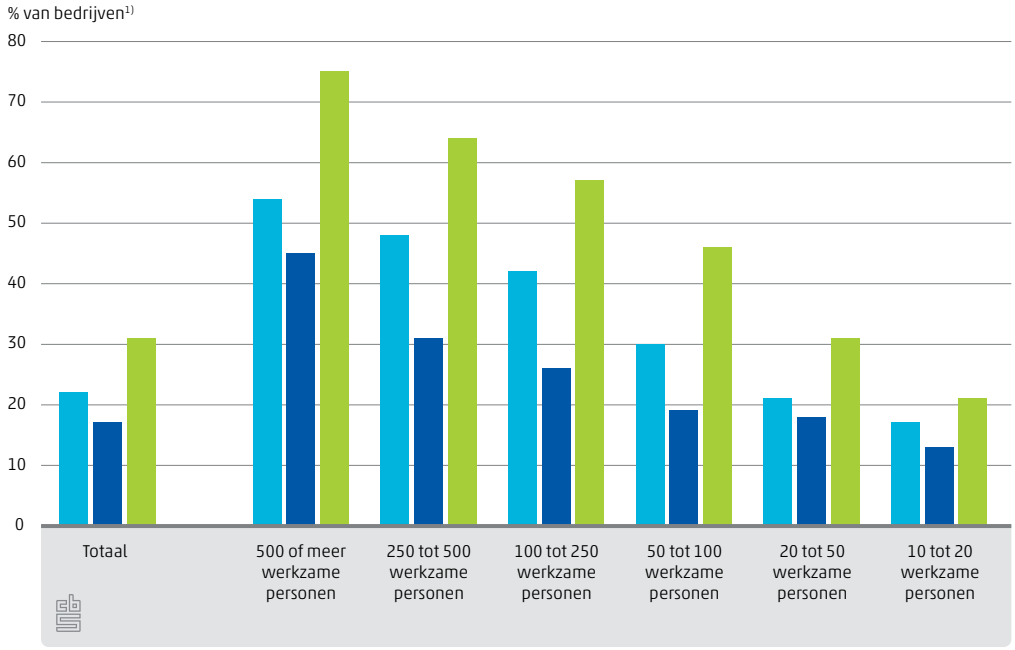


Bron: CBS, ICT-gebruik bedrijven.
1) Bedrijven met tien of meer werkzame personen.

Grotere bedrijven tre en meer maatregelen

Ook het verschil tussen grote en kleine bedrijven is aanzienlijk. Van de bedrijven met 500 of meer werkzame personen had 75 procent een formeel vastgelegd ICT-beveiligingsbeleid in 2015. Bij bedrijven met 10 tot 20 werknemers was dit slechts 21 procent. Van de grootste bedrijven maakte 45 procent gebruik van cloud-diensten op een eigen server, van de kleinste bedrijven 13 procent. De werkzaamheden op het terrein van ICT-beveiliging en de beveiliging van data werden door de grootste bedrijven in meer dan de helft van de gevallen (54 procent) voornamelijk uitgevoerd door eigen personeel; voor de kleinste bedrijven was dit 17 procent. Ten aanzien van dit laatste geldt overigens dat dit meer een indicatie is hoe het ICT-beveiligingswerk is georganiseerd dan dat het een impliciet oordeel is dat het uitbesteden van dit werk meer risico's met zich meebrengt dan het in eigen beheer verzorgen van dit werk.
Wel komt hier 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 kleinere 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.

3.1.3 Cybersecuritymaatregelen bedrijven, naar bedrijfsgrootte



Bron: CBS, ICT-gebruik bedrijven.
1) Bedrijven met tien of meer werkzame personen.

ICT-beveiligingsbeleid

Het ICT-beveiligingsbeleid van bedrijven bevat maatregelen om ICT-problemen te voorkomen, en procedures die beschrijven hoe het bedrijf handelt als er toch een incident optreedt. Van alle bedrijven met een formeel ICT-beveiligingsbeleid in 2015, heeft 80 procent vastgelegd hoe om te gaan met het risico op vernietiging of verminking van gegevens door een aanval van buitenaf of door een incident binnen het bedrijf. Ook de uitval van ICT-diensten door een aanval van kwaadwillenden komt veel voor in het ICT-beveiligingsbeleid. Van de bedrijven met een dergelijk formeel beleid behandelt 77 procent dit risico in het ICT-beveiligingsplan. Ten slotte heeft 80 procent van de bedrijven procedures rondom beveiliging van vertrouwelijke gegevens formeel vastgelegd. Medewerkers van bedrijven kunnen dergelijke gegevens bijvoorbeeld per ongeluk onthullen. Maar hier kan ook sprake zijn van kwade opzet, bijvoorbeeld door inbraak en aanvallen via *pharming* of *phishing* (zie ook tabel A 3.1 achter in deze publicatie).

Meerderheid bedrijven herziet beveiligingsbeleid regelmatig

De meeste bedrijven herzien het formele ICT-beveiligingsbeleid regelmatig. Twee derde van de bedrijven had dit beleid maximaal een jaar voordat het onderzoek plaatsvond nog bijgewerkt. Bij één op de zes was dit meer dan twee jaar geleden. In de financiële

sector hebben niet alleen veel bedrijven een formeel ICT-beveiligingsbeleid; in deze branche is dit beleid ook bovengemiddeld actueel. Van de financiële instellingen met een ICT-beveiligingsplan had 82 procent dit in het voorgaande jaar nog herzien. In de onroerendgoedbranche was dit aandeel veel kleiner, te weten 46 procent (zie ook tabel A 3.1 achter in deze publicatie).

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 aan niet of beperkt online te verkopen via een website of app vanwege problemen met ICT-beveiliging of gegevensbescherming (zie ook tabel A.3.4 achter in deze publicatie).

3.2 Personen

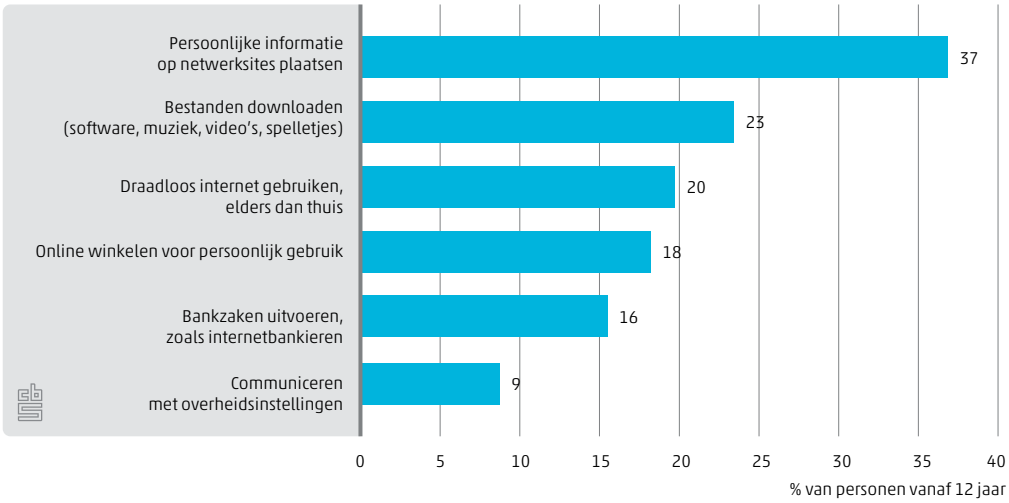
Net zo goed als bedrijven nemen personen ook maatregelen om zo veilig mogelijk te internetten. CBS heeft informatie over het aanpassen van het internetgedrag vanwege zorgen om de veiligheid, het daadwerkelijk handelend optreden om cookies te verwijderen en/of de instellingen van de browser op dat punt te wijzigen en het regelmatig maken van *back-ups* van bestanden, foto's e.d. die op de computer, laptop of tablet staan.

Aanpassen gedrag

Meer dan de helft van de personen van 12 jaar of ouder heeft internetactiviteiten wel eens afgebroken of vermeden omdat hij of zij het niet vertrouwde. Het gaat hier om een beperkt aantal gemeten activiteiten (zie figuur 3.2.1). Van de hoogopgeleiden heeft 65 procent dit wel eens gedaan, tegen 41 procent van de laagopgeleiden. Van de personen van 12 tot 25 jaar deed 49 procent dit wel eens. Vergeleken met de 25- tot 45-jarigen en de 45- tot 65-jarigen is dit weinig. In deze laatste leeftijdscategorieën besloot 58 procent van de personen wel eens om af te zien van bepaalde internet-activiteiten vanwege zorgen om de veiligheid (zie ook tabel A 4.1. achterin deze publicatie).
Overigens is het niet altijd zo dat degenen die vaker afzien van bepaalde activiteiten wantrouwender of voorzichtiger zijn dan anderen. Het hangt ook af van de activiteiten die een persoon op internet onderneemt. Zo ziet maar 21 procent van de 75-plussers af van bepaalde activiteiten. Dit is niet uitsluitend omdat deze groep geen oog heeft voor veiligheidsrisico's, maar ook omdat deze groep minder (geavanceerde) activiteiten onderneemt op internet, die minder veiligheidsrisico's met zich meebrengen. Bij het aanpassen van het gedrag gaat het nadrukkelijk om het incidenteel vermijden of afbreken van activiteiten, bijvoorbeeld het niet doorzetten van een online aankoop, omdat ergens in het proces iets verontrustends optreedt. Op zich is dit een goede reflex van de internetgebruiker. Het is, aan de andere kant, verontrustend omdat veel verhalen en scenario's over de (positieve) invloed van ICT en internet op de welvaart en de samen-leving ervan uitgaan dat het potentieel van ICT en internet volledig wordt benut. Een

toenemend wantrouwen ten aanzien van ICT en internet kan deze ontwikkeling in de weg staan.

3.2.1 Vermeden activiteiten vanwege zorgen om internetveiligheid, 2015[1)]



Bron: CBS, ICT-gebruik huishoudens en personen.

[1)] Mensen die in de twaalf maanden voorafgaand aan het onderzoek vanwege zorgen om de veiligheid wel eens hebben afgezien van de betreffende activiteit op 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 vanaf 12 jaar 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 (zie ook tabel A 4.1 achter in deze publicatie).

Bijna zes op de tien personen maken back-ups

Bijna zes op de tien personen (55 procent) maken wel eens *back-ups* van bestanden, foto's e.d. die op hun computer staan. Dit getuigt van een zeker bewustzijn dat dingen mis kunnen gaan en informatie, bedoeld of onbedoeld, beschadigd of vernietigd kan worden. Het is een maatregel om de schade te beperken mocht er iets misgaan met de betreffende bestanden en/of de computer. Ook hier geldt dat het maken van *back-ups* of reservekopieën niet per se heel systematisch en frequent behoeft te gebeuren. De vraag in het onderzoek had betrekking op de twaalf maanden voorafgaand aan het onderzoek.

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 zou hij wachtwoorden of andere gevoelige informatie kunnen buitmaken.
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 voorkomt hij dat hij geleid wordt naar een vals IP-adres. 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.
Eind september 2016 waren er 5,6 miljoen .nl-domeinnamen geregistreerd bij de Stichting Internet Domeinregistratie Nederland (SIDN). Ruim 2,5 miljoen van deze domeinnamen (45 procent) maakten gebruik van DNSSEC. Eind september 2014 was dit nog 34 procent.
De 5,6 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 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 kwaadwillenden maar ook tegen 'jezelf'.

4.1 Cybersecurity, incidenten

Indicator	2014	2015	2016	Eenheid	Bron
Geconfronteerd met veiligheidsincidenten op internet[1)]	.	8	.	**% personen vanaf 12 jaar**	CBS
Fraude bij online aankopen (bijvoorbeeld geen levering of misbruik van creditcardgegevens)				**% personen die de afgelopen 12 maanden online aankopen deden**	
Meldingen in het kader van de meldplicht datalekken zoals opgenomen in de Wet bescherming persoonsgegevens	.	.	5 617	**Aantal meldingen (excl. ingetrokken meldingen)**	Autoriteit Persoons-gegevens
Meldingen in het kader van de zorg- en meldplicht van aan-bieders van openbare telecommunicatienetwerken of -diensten zoals opgenomen in de Telecommunicatiewet	41	39	.	**Aantal incidenten**	Agentschap Telecom
Omvang en duur (verijdelde) DDos-aanvallen[2)]					NBIP
waarvan					
> 10 gbps	.	.	13	**% van totaal**	
> 1 uur	.	.	36	**% van totaal**	

[1)] In het onderzoek is naar een gelimiteerd aantal typen veiligheidsincidenten gevraagd; computervirus waardoor gegevens verloren gingen, misbruik van persoonlijke gegevens of andere privacyschending, financiële schade (door *phishing*, *pharming*, fraude met betaalkaarten). Betreft de 12 maanden voorafgaande aan het onderzoek.

[2)] Heeft betrekking op de de bij de NBIP aangesloten internetproviders die gebruikmaken van de Nationale anti-DDos Wasstraat (NaWas). Periode: 1-07 tot en met 14-12.

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 2016 zijn 39 van dit soort belangrijke verstoringen gemeld (41 in 2014). 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.

Ruim 5,5 duizend datalekken

Een ander voorbeeld van incidenten die niet altijd doelbewust en strafbaar zijn, zijn de 5 617 datalekken zoals die in 2016 zijn gemeld bij de Autoriteit Persoonsgegevens. 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 is op slordige omgang door de houder van de gegevens. Aan de andere kant van het spectrum staat het moedwillig hacken van dit soort gegevensbronnen om te illustreren hoe slecht deze gegevens beveiligd zijn, of om er daadwerkelijk iets mee te gaan doen, bijvoorbeeld te verkopen. 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.).

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 is minder veelzeggend dan de karakteristieken van de DDos-aanvallen.
Kenmerken van DDos-aanvallen zijn de omvang (gbps) en de duur (tijd). In de tweede helft van 2016 had 13 procent van de DDos-aanvallen een omvang van meer dan 10 gbps. Dit was ook in 2015 het geval. Ruim een derde (36 procent) van de aanvallen duurde langer dan een uur. Dit percentage is fors toegenomen ten opzichte van 2015 (zie voor cijfers over 2015 (NCSC, 2016)).

8 procent van de Nederlanders maakte een incident mee

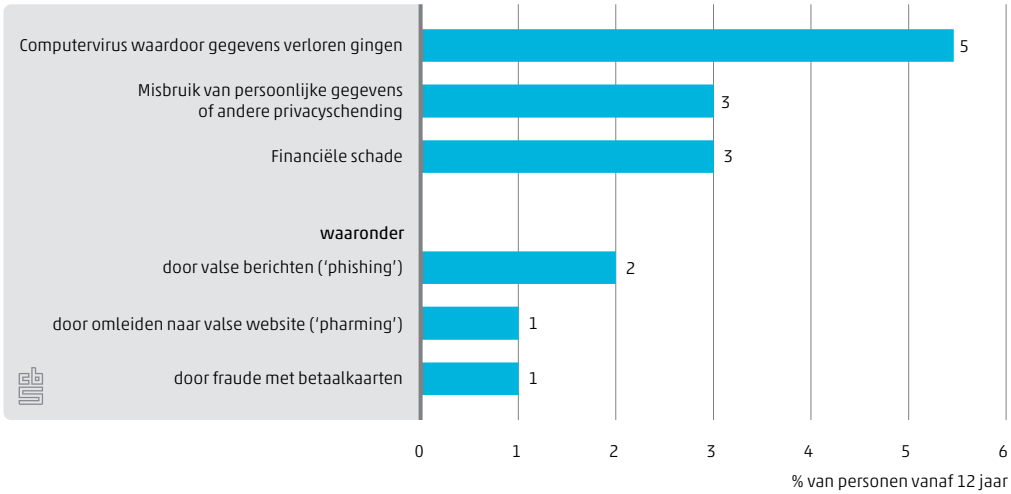
In 2015 heeft 8 procent van de Nederlanders een veiligheidsincident op internet meegemaakt. Mensen van 75 jaar of ouder ondervonden de minste problemen op dit punt: 4 procent. Deze leeftijdsgroep is ook al het minst bezorgd over de internet-veiligheid. Als echter alleen de internetgebruikers van 75 jaar of ouder worden meegenomen, blijkt dat ook van hen 8 procent een veiligheidsincident heeft onder-vonden. Bij personen jonger dan 75 jaar is dit 9 procent. Zij zijn online veel actiever dan 75-plussers. De 25- tot 65-jarigen maakten zich het meest zorgen over internetveiligheid, maar zij zijn niet vaker dan gemiddeld slachtoffer (zie ook tabel A 4.1. achterin deze publicatie).

Computervirussen eisen de meeste slachto ers

De meeste problemen werden veroorzaakt door computervirussen, waardoor gegevens verloren gingen; 5 procent van de Nederlanders kreeg hiermee te maken (figuur 4.2). Daarnaast is van 3 procent van de Nederlanders de privacy geschonden door bijvoorbeeld

misbruik van persoonlijke gegevens. Andere online incidenten veroorzaken financiële schade, zoals fraude met creditcards, *phishing* en *pharming*. In totaal heeft 3 procent van de Nederlanders financiële schade gehad als gevolg van dergelijke praktijken. Aan deze 3 procent is gevraagd hoe groot de schade was. In de helft van de gevallen was de schade minder dan honderd euro. In ruim 5 procent van de gevallen bedroeg de schade meer dan duizend euro.

4.2 Veiligheidsincidenten op internet, naar type, 2015[1]



Bron: CBS, ICT-gebruik huishoudens en personen.
[1)] Mensen die in de twaalf maanden voorafgaand aan het onderzoek het betreffende incident hebben meegemaakt.

Drie procent online kopers heeft last van fraude

In 2016 had 3 procent van de personen die in de twaalf maanden voor het onderzoek online iets besteld hadden te maken met fraude (bijvoorbeeld geen levering van de bestelde producten of misbruik van creditcard-gegevens). In 2015 was dit 2 procent van de online kopers.

5.
Cybercrime

Cybercrime is in hoofdstuk 2 omschreven als: 'alle delicten die gepleegd worden met behulp van ICT'. Criminaliteit 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 opgelicht. De preventieve maatregelen van mens en machine schoten tekort.

5.1 Cybercrime

Indicator	2012	2013	2014	2015	Eenheid	Bron
Ondervonden delicten cybercrime[1)]	20	21	19	19	**Per 100 inwoners**	CBS
Slachtofferschap cybercrime[1)]	12	13	11	11	**% personen vanaf 15 jaar**	CBS
Meldingen cybercrime[1)]	31	30	28	27	**% van ondervonden delicten**	CBS
Meldingen bij politie[1)]	13	13	13	13	**% van ondervonden delicten**	CBS
Aangifte totaal[1)]	7	7	7	8	**% van ondervonden delicten**	CBS
waarvan identiteitsfraude totaal	2	1	1	1	**Per 100 inwoners**	
slachtoffers	2	1	1	1	**% personen vanaf 15 jaar**	
melding totaal	90	89	88	84	**% van ondervonden delicten**	
melding bij politie	17	18	14	20	**% van ondervonden delicten**	
aangifte totaal	12	13	12	13	**% van ondervonden delicten**	
koop- en verkoopfraude totaal	3	4	4	4	**Per 100 inwoners**	
slachtoffers	3	3	4	4	**% personen vanaf 15 jaar**	
melding totaal	41	45	41	39	**% van ondervonden delicten**	
melding bij politie	24	26	24	23	**% van ondervonden delicten**	
aangifte totaal	20	22	20	20	**% van ondervonden delicten**	
hacken totaal	9	9	8	8	**Per 100 inwoners**	
slachtoffers	6	6	5	5	**% personen vanaf 15 jaar**	
melding totaal	22	20	19	18	**% van ondervonden delicten**	
melding bij politie	6	7	5	4	**% van ondervonden delicten**	
aangifte totaal	2	2	2	2	**% van ondervonden delicten**	
cyberpesten totaal	6	6	6	6	**Per 100 inwoners**	
slachtoffers	3	3	3	3	**% personen vanaf 15 jaar**	
melding totaal	23	22	23	24	**% van ondervonden delicten**	
melding bij politie	15	14	15	15	**% van ondervonden delicten**	
aangifte totaal	5	5	5	6	**% van ondervonden delicten**	
Computervredebreuk						
Totaal geregistreerde misdrijven	4580	2480	1990	2175	**Aantal**	CBS
Geregistreerde misdrijven, relatief	0	0	0	0	**% van totaal geregistreerde misdrijven**	
Geregistreerde misdrijven per 1000 inwoners	0,3	0,1	0,1	0,1	**Per 1 000 inwoners**	
Totaal opgehelderde misdrijven	255	215	165	100	**Aantal**	CBS
Opgehelderde misdrijven, relatief	5,5	8,8	8,4	4,6	**% van totaal geregistreerde misdrijven**	
Totaal geregistreerde verdachten	290	250	205	155	**Aantal**	CBS

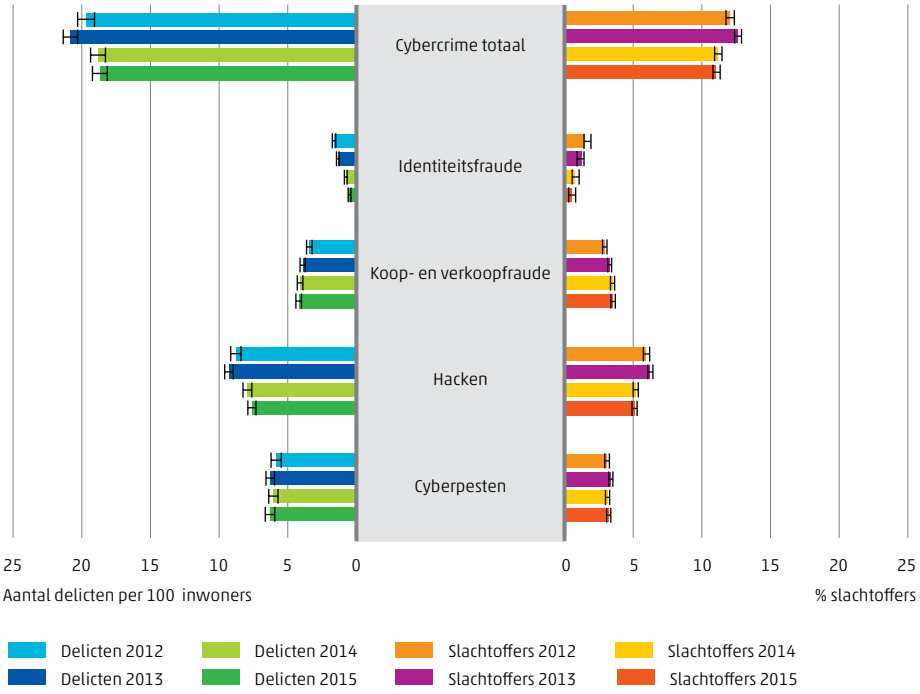
[1)] In het onderzoek is naar een gelimiteerd aantal typen cybercrimedelicten gevraagd (identiteitsfraude, hacken, koop- en verkoopfraude, cyberpesten).

Een op de negen Nederlanders slachto er cybercrime

Vanaf 2012 heeft CBS informatie 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 één op de negen Nederlanders (11,1 procent) in 2015 eenmaal of vaker slachtoffer geweest van één of meer cybercrimedelicten. Dit is vergelijkbaar met 2014, maar lager dan in 2012 (12,1 procent) en 2013 (12,6 procent).
In 2015 is 5,1 procent van de 15-plussers gehackt, 3,2 procent is wel eens online gepest en 3,5 procent is naar eigen zeggen opgelicht via internet. Van 0,6 procent van de

Nederlanders zijn via internet identificerende gegevens gestolen en misbruikt voor financieel gewin.
Bij hacken en vooral cyberpesten is vaker sprake van herhaald slachtofferschap (dat wil zeggen men is meer dan een keer slachtoffer van hetzelfde delict) 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.
Binnen de categorie hacken is het inbreken op iemands e-mailaccount de meest voorkomende variant gevolgd door het inbreken op iemands website/profielsite. Binnen de categorie identiteitsfraude is skimming de afgelopen jaren afgenomen. *Phishing/pharming* is in 2015 niet toegenomen en kwam in 2015 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 Cybercrime naar soort delict[1)]



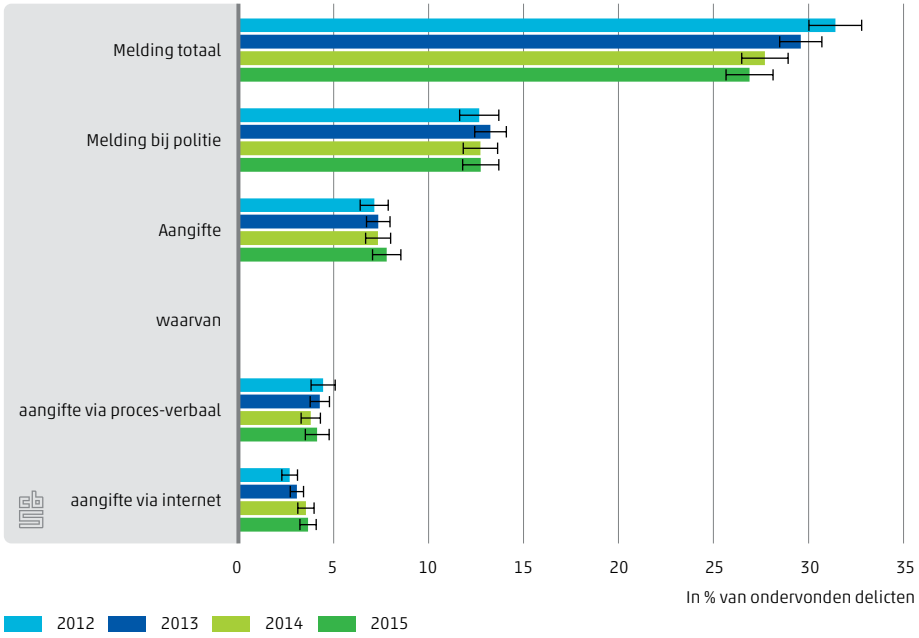
Bron: CBS, Veilgheidsmonitor.
[1)] In het onderzoek is naar een gelimiteerd aantal typen cybercrimedelicten gevraagd (identiteitsfraude, hacken, koop- en verkoopfraude, cyberpesten).

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. 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 2015 ruim een kwart gemeld (27 procent) bij de politie of een andere instantie. Dit is minder dan in 2012 en 2013. Aangifte bij de politie werd in 2015 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 2015 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 Cybercrime melding en aangifte[1)]



Bron: CBS, Veilgheidsmonitor.

[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, 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 (84 procent). 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 2015 was het aantal ondervonden traditionele delicten 31,8 per honderd inwoners. In dat jaar bedroeg het aantal cybercrimedelicten 18,7 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 niet als er maar vier typen cybercrimedelict worden waargenomen.
Van alle traditionele delicten werd in 2015 ruim een op de drie gemeld bij de politie (36,3 procent). Van ruim twee derde hiervan (26,8 procent) werd daadwerkelijk aangifte gedaan. Voor cybercrime zijn deze percentages beduidend lager, te weten 12,7 en 7,8. 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 (18,7 procent van de vandalismedelicten wordt bij de politie gemeld; 12,8 procent in de vorm van een aangifte).

Geregistreerde cybercrime

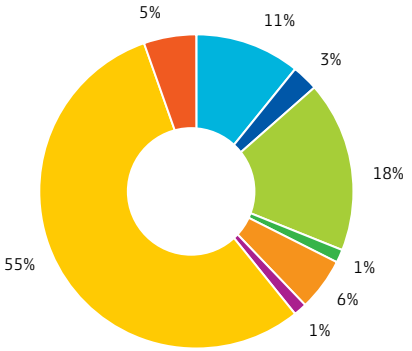
Op dit moment is computervredebreuk in de Standaardclassificatie Misdrijven van CBS de enige categorie die valt onder cybercrime. Internetoplichting en online zedendelicten bijvoorbeeld vallen in deze classificatie onder de categorieën oplichting en seksuele misdrijven. Zowel de politie, die de bron is van de beschrijving van de geregistreerde criminaliteit in Nederland, als CBS is bezig om de registratie en classificatie van cybercrime te verbeteren.

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 2015 maar 4 procent. De bij de politie gemelde (geregistreerde) gevallen van computervredebreuk zijn dus maar een fractie van het totale aantal delicten.
In 2015 was het ophelderingspercentage[1)] van de aangegeven gevallen van computervredebreuk 4,6 procent. Dit ligt het dichtst bij het ophelderingspercentage van het misdrijf 'vernielingen aan auto' (6,7 procent). Voor alle geregistreerde misdrijven tezamen was het ophelderingspercentage in 2015 22,8 procent.

[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.

5.4 Door Openbaar Ministerie (OM) en rechter opgelegde straffen en maatregelen voor computervredebreuk, 2005–2015 (N=405)



Bron: CBS, Rechtbankstrafzaken.

1) Het 'afpakken' van de bij het delict betrokken middelen.
2) Hier vooral geldboetes, werkstraffen en betaling schadevergoeding aan benadeelde.
3) Hier vooral geldboetes.

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 uit of biedt een transactie aan. In de periode 2005–2015 bedroeg het aantal door het Openbaar Ministerie en de rechter opgelegde straffen ruim 400. In 60 procent van de gevallen legde het Openbaar Ministerie een straf op zonder tussenkomst van de rechter. Dit zijn zogenoemde transacties die in het geval van computervredebreuk vaak bestonden uit een werkstraf of een geldboete. Daarnaast zijn dit strafbeschikkingen die in het geval van computervredebreuk vaak bestonden uit een taakstraf. Ook de rechter legde vaak een taakstraf (18 procent) of een geldboete (11 procent) op. De geldstraf bedroeg bijna nooit meer dan enkele honderden euro's. In 3 procent van de gevallen werd een voorwaardelijke gevangenisstraf opgelegd.

6. Bronnen

Onderstaand een korte omschrijving van de vier belangrijkste statistische 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. De *Veiligheidsmonitor 2015* is uitgevoerd in de periode begin augustus tot eind november 2015 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 299 duizend steekproefpersonen voor deelname benaderd. Onderzoeksgegevens zijn verkregen van ruim 111 duizend personen. Iets minder dan de helft van deze mensen vulde de internetvragenlijst in (48,4 procent), iets meer dan helft de schriftelijke vragenlijst (51,6 procent). Uiteindelijk respondeerde 37,2 procent van alle benaderde personen. Dit is minder dan in voorgaande jaren; in 2014 bedroeg de respons 38,8 procent, in 2013 40,8 procent en in 2012 38,4 procent.
In de Veiligheidsmonitor wordt mensen gevraagd naar ondervonden delicten in de twaalf maanden voorafgaand aan het onderzoek. Voor cybercrime worden echter maar vier delicten gevraagd. *Ransomware* behoort hier bijvoorbeeld niet toe. De cijfers geven dus een onvolledig 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 worden gemeld.

Enquête 'ICT-gebruik bedrijven'

CBS onderzoekt jaarlijks hoe bedrijven ICT gebruiken. De enquête 'ICT-gebruik bedrijven' hanteert een steekproef van ongeveer 10 duizend bedrijven. De onderzoekspopulatie bestaat uit bedrijven met 10 of meer werkzame personen. 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 verzekeringen[1)]
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 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.

7.

Editie 2018

Zoals gezegd is deze publicatie een eerste verkenning van de mogelijkheden om cybersecurity te meten. Uit zijn eigen statistieken heeft CBS met name informatie over wat personen en bedrijven zoal overkomt op het terrein van cybersecurity en hoe ze zich hier tegen wapenen. Deze gegevens zijn ook in deze publicatie gepresenteerd. Een belangrijke witte vlek daarentegen is een kwantitatieve beschrijving van dreigingen zoals *malware* waarmee de ICT-systemen van bedrijven, overheden en personen stelselmatig geconfronteerd worden. Een andere witte vlek betreft een beschrijving van de kwetsbaarheden van de ICT-systemen van bedrijven, overheden en personen bijvoorbeeld in de vorm van verouderde software waarvan bekend is dat er kwetsbaarheden inzitten. CBS zal samen met andere partijen bekijken in hoeverre dit soort witte vlekken ingevuld kan worden om te komen tot een volledigere en evenwichtigere monitor.

Ook de in deze publicatie gebruikte bronnen zijn zeker nog voor verbetering vatbaar. Dit geldt bijvoorbeeld voor het waarnemen van cybercrime binnen de door de politie geregistreerde criminaliteit. Maar ook voor het gebruik van internetstandaarden zoals DNSSEC door het Nederlandse bedrijfsleven. Deze laatste informatie zou aan kracht winnen als ze uitgebreid zou kunnen worden met andere erkende internetstandaarden en bijvoorbeeld per bedrijfstak gepresenteerd zou kunnen worden. CBS zal samen met betrokken partijen bezien in hoeverre dit mogelijk is.

Ten slotte zal CBS binnen de kaders van zijn eigen statistieken de waarneming van cybercrime verbeteren en bijvoorbeeld proberen meer cyberdelicten op te nemen in de Veiligheidsmonitor. Deze bronnen waaruit ook ten behoeve van deze publicatie is geput leveren in 2017 geactualiseerde cijfers op. Deze zullen samengebracht worden in de volgende editie van de *Cybersecuritymonitor*. Zo worden in de enquête ICT-gebruik bedrijven in 2017 nieuwe vragen gesteld over cybersecurity (ICT-veiligheidsmaatregelen, ICT-veiligheidsincidenten, de kosten van deze incidenten, uitgaven aan ICT-veiligheids-maatregelen). Een aantal van deze statistieken biedt ook de mogelijkheid om Nederland te vergelijken met andere EU-landen omdat het in EU-verband geharmoniseerde enquêtes betreft. Een dergelijke internationale vergelijking is in deze publicatie nog niet opgenomen maar dat zou in een volgende editie wel kunnen gebeuren.

Referenties

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

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

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

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

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.

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.

Annex met tabellen

A3.1 Bedrijven met een ICT-beveiligingsbeleid, naar bedrijfstak en bedrijfsgrootte, 2015

		Behandelde risico's			Werd voor het laatst herzien		
	Bedrijven met ICT-beveiligingsbeleid	vernietiging of verminking gegevens	onthulling van vertrouwelijke gegevens	uitval van ICT-diensten	12 maanden of korter geleden	13 t/m 24 maanden geleden	langer dan 24 maanden geleden
	% van bedrijven[1]	% van bedrijven met ICT-beveiligingsbeleid					
Totaal	31	80	80	77	67	17	16
Bedrijfstak							
Industrie	31	80	78	74	63	19	18
Energie & water	44	84	85	76	67	19	14
Bouwnijverheid	20	82	78	75	73	15	12
Handel	28	79	79	77	70	14	16
Transport	26	83	76	79	65	20	15
Horeca	11	75	73	75	61	23	15
Informatie en communicatie	53	88	89	89	72	16	13
Financiële instellingen	72	88	88	89	82	8	11
Onroerend goed	45	77	69	79	46	35	19
Advies en onderzoek	42	79	78	75	64	18	19
Overige dienstverlening	27	81	82	77	72	13	16
Gezondheidszorg	43	77	83	73	66	20	14
Bedrijfsgrootte							
10 tot 20 werkzame personen	21	77	77	74	69	13	19
20 tot 50 werkzame personen	31	79	81	77	67	17	16
50 tot 100 werkzame personen	46	84	82	80	65	21	14
100 tot 250 werkzame personen	57	85	82	79	69	21	10
250 tot 500 werkzame personen	64	81	82	77	62	23	16
500 of meer werkzame personen	75	87	84	83	66	20	14

Bron: CBS, ICT-gebruik bedrijven.

[1] Bedrijven met tien of meer werkzame personen.

A3.2 Bedrijven met werkzaamheden op het terrein van ICT-beveiliging en bescherming van data, naar bedrijfstak en bedrijfsgrootte, 2015

		Dit werk wordt voornamelijk uitgevoerd door	
	Bedrijven met ICT-beveiligingswerkzaamheden	eigen personeel	externe leveranciers
	% van bedrijven[1]	% van bedrijven met ICT-beveiligingswerkzaamheden	
Totaal	85	26	74
Bedrijfstak			
Industrie	86	27	73
Energie & water	86	33	67
Bouwnijverheid	85	13	87
Handel	87	28	72
Transport	85	24	76
Horeca	64	17	83
Informatie en communicatie	92	70	30
Financiële instellingen	91	47	53
Onroerend goed	90	23	77
Advies en onderzoek	92	25	75
Overige dienstverlening	82	20	80
Gezondheidszorg	90	19	81

A3.2 Bedrijven met werkzaamheden op het terrein van ICT-beveiliging en bescherming van data, naar bedrijfstak en bedrijfsgrootte, 2015 (slot)

	Bedrijven met ICT-beveiligingswerkzaamheden	Dit werk wordt voornamelijk uitgevoerd door	
		eigen personeel	externe leveranciers
	% van bedrijven[1]	% van bedrijven met ICT-beveiligingswerkzaamheden	
Bedrijfsgrootte			
10 tot 20 werkzame personen	81	21	79
20 tot 50 werkzame personen	88	24	76
50 tot 100 werkzame personen	92	33	67
100 tot 250 werkzame personen	93	45	55
250 tot 500 werkzame personen	95	51	49
500 of meer werkzame personen	94	57	43

Bron: CBS, ICT-gebruik bedrijven.

[1] Bedrijven met tien of meer werkzame personen.

A3.3 Bedrijven met betaalde cloud-diensten, naar bedrijfstak en bedrijfsgrootte, 2016

		Welke cloud-diensten							Eigen en/of gedeelde server	
	Cloud-diensten gebruikt	e-mail (als cloud-dienst)	office software	database hosting	bestanden opslaan (als cloud-dienst)	software voor boek-houding	software klantin-formatie-beheer	reken-kracht voor software bedrijf	gedeelde servers	servers uitsluitend voor het bedrijf
	% van bedrijven[1]									
Totaal	35	21	17	23	23	20	15	7	26	17
Bedrijfstak										
Industrie	25	14	11	13	14	12	7	4	20	11
Energie & water	43	18	18	27	25	20	16	9	27	24
Bouwnijverheid	32	17	15	19	19	15	10	6	25	12
Handel	31	19	15	21	21	17	13	6	23	15
Transport	30	15	11	16	17	16	9	5	23	12
Horeca	21	14	9	16	14	12	7	4	16	8
Informatie en communicatie	64	41	35	48	49	37	33	17	46	40
Financiële instellingen	43	22	21	25	26	19	16	9	29	26
Onroerend goed	50	26	25	28	30	24	22	12	41	17
Advies en onderzoek	53	31	26	34	34	33	22	11	38	28
Overige dienstverlening	37	24	21	26	26	23	18	8	30	13
Gezondheidszorg	44	25	21	31	28	26	24	10	31	22
Bedrijfsgrootte										
10 tot 20 werkzame personen	30	18	15	21	20	18	12	6	23	13
20 tot 50 werkzame personen	36	23	19	25	24	21	16	8	27	18
50 tot 100 werkzame personen	40	22	19	25	25	21	17	8	30	19
100 tot 250 werkzame personen	47	22	19	25	25	20	19	9	34	26
250 tot 500 werkzame personen	54	26	23	30	29	25	21	14	43	31
500 of meer werkzame personen	68	31	29	36	36	22	26	15	48	45

Bron: CBS, ICT-gebruik bedrijven.

[1] Bedrijven met tien of meer werkzame personen.

A3.4 Bedrijven met beperkt of geen gebruik cloud-diensten en e-commerce uit veiligheidsoverwegingen, naar bedrijfstak en bedrijfsgrootte

	Geen of minder verkoop via website/app (2016)	Gebruik cloud-diensten (2014)	
		geen gebruik	beperkt gebruik
	% van bedrijven[1]		
Totaal	19	27	11
Bedrijfstak			
Industrie	18	33	10
Energie & water	16	27	19
Bouwnijverheid	22	27	6
Handel	19	28	9
Transport	19	25	8
Horeca	20	21	8
Informatie en communicatie	15	18	19
Financiële instellingen	21	40	22
Onroerend goed	15	31	12
Advies en onderzoek	18	26	19
Overige dienstverlening	19	20	10
Gezondheidszorg	21	27	16
Bedrijfsgrootte			
10 tot 20 werkzame personen	20	25	9
20 tot 50 werkzame personen	19	28	10
50 tot 100 werkzame personen	16	29	13
100 tot 250 werkzame personen	17	29	21
250 tot 500 werkzame personen	14	28	31
500 of meer werkzame personen	18	30	37

Bron: CBS, ICT-gebruik bedrijven.

[1] Bedrijven met tien of meer werkzame personen.

A4.1 Veiligheidsincidenten, bezorgdheid en maatregelen internetgebruik personen

	Beperkt internet-gebruik door zorgen over veiligheid/ incidenten (2015)[1]	Geconfronteerd met veiligheids-incidenten (2015)[2]	Maakt reserve-kopieën of *back-ups* van bestanden, afbeeldingen e.d. die op de computer staan (2015)	Maakt zich erg zorgen dat activiteiten op internet worden bijgehouden door cookies (2016)	Verandert instellin-gen browser om cookies tegen te gaan of te verminderen (2016)
	% van personen vanaf 12 jaar				
Totaal	52	8	55	11	34
Geslacht					
Man	52	10	60	12	42
Vrouw	52	7	50	11	27
Opleidingsniveau					
Lager onderwijs	41	8	38	10	19
Middelbaar onderwijs	55	8	59	12	32
Hoger onderwijs	65	8	73	12	48
	% van personen				
Leeftijd					
12 tot 25 jaar	49	10	54	6	29
25 tot 45 jaar	58	8	66	9	43
45 tot 65 jaar	58	9	59	16	38
65 tot 75 jaar	49	8	40	15	27
75 jaar en ouder	21	4	21	8	8

Bron: CBS, ICT-gebruik huishoudens en personen.

[1] In het onderzoek is deze vraag voor een gelimiteerd aantal typen internetactiviteiten gesteld: persoonlijke informatie op netwerksites plaatsen, bestanden downloaden, draadloos internet gebruiken elders dan thuis, online winkelen voor persoonlijk gebruik, bankzaken uitvoeren, communiceren met overheidsinstellingen. Betreft de 12 maanden voorafgaande aan het onderzoek.

[2] In het onderzoek is naar een gelimiteerd aantal typen veiligheidsincidenten gevraagd; computervirus waardoor gegevens verloren gingen, misbruik van persoonlijke gegevens of andere privacyschending, financiële schade (door *phishing*, *pharming*, fraude met betaalkaarten). Betreft de 12 maanden voorafgaande aan het onderzoek.

A5.1 Slachto ers cybercrime naar achtergrondkenmerken, 2015

	Identiteits-fraude	Marge	Koop- en verkoop-fraude	Marge	Hacken	Marge	Cyberpesten	Marge	Cybercrime totaal[1)]	Marge
	% slachtoffers									
Totaal	0,6	0,1	3,5	0,2	5,1	0,2	3,2	0,2	11,1	0,3
Geslacht										
Man	0,6	0,1	3,6	0,2	5,6	0,3	3,1	0,2	11,5	0,4
Vrouw	0,5	0,1	3,5	0,2	4,6	0,2	3,3	0,2	10,6	0,4
Leeftijd										
15-24 jaar	0,2	0,1	5,1	0,5	6,5	0,6	7,6	0,7	17,1	0,9
25-44 jaar	0,6	0,1	5,1	0,4	5,9	0,4	3,6	0,3	13,5	0,6
45-64 jaar	0,7	0,1	3,2	0,2	4,8	0,3	2,2	0,2	9,8	0,4
65 jaar en ouder	0,5	0,1	0,8	0,1	3,5	0,3	0,9	0,1	5,3	0,3
Herkomst										
Autochtoon	0,5	0,1	3,6	0,2	5,1	0,2	3,1	0,2	11,0	0,3
Westerse allochtoon	0,9	0,2	3,4	0,5	5,5	0,6	3,1	0,5	11,3	0,8
Niet-westerse allochtoon	0,5	0,2	3,4	0,6	4,7	0,7	4,1	0,6	11,1	1,0
Opleiding										
Lager onderwijs	0,3	0,1	2,0	0,2	4,0	0,3	3,2	0,3	8,4	0,4
Middelbaar onderwijs	0,5	0,1	4,0	0,3	5,4	0,3	3,7	0,3	12,1	0,5
Hoger onderwijs	0,9	0,1	4,8	0,3	6,3	0,3	2,8	0,3	13,3	0,5
Seksuele geaardheid										
Homo	1,0	0,7	6,2	1,9	6,7	2,0	7,3	2,2	18,1	3,1
Lesbienne	0,3	0,3	2,3	1,4	5,5	2,2	5,8	2,4	11,9	3,2
Biseksuele man	0,5	0,4	3,0	1,4	8,8	2,4	4,5	1,8	14,8	3,0
Biseksuele vrouw	0,7	0,5	3,6	1,2	5,6	1,3	5,9	1,5	13,0	2,1
Hetero man	0,7	0,1	3,8	0,3	5,7	0,3	3,0	0,2	11,8	0,4
Hetero vrouw	0,5	0,1	4,1	0,3	5,1	0,3	3,5	0,3	11,9	0,4
Stedelijkheid										
Zeer sterk stedelijk	0,6	0,1	3,7	0,3	5,1	0,4	3,5	0,3	11,4	0,6
Sterk stedelijk	0,6	0,1	3,7	0,3	5,4	0,3	3,3	0,3	11,6	0,5
Matig stedelijk	0,5	0,1	3,4	0,3	5,3	0,4	3,1	0,3	10,9	0,6
Weinig stedelijk	0,6	0,1	3,3	0,3	4,7	0,4	2,8	0,3	10,4	0,6
Niet stedelijk	0,5	0,2	3,4	0,5	4,6	0,6	3,2	0,5	10,5	0,9

Bron: CBS, Veiligheidsmonitor.

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

A5.2 Melding en aangifte cybercrime naar delictsoort

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

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.

A5.3 Cybercrimedelicten naar soort[1)]

	2012		2013		2014		2015	
	Per 100 inwoners	Marge	Per 100 inwoners	Marge	Per 100 inwoners	Marge	Per 100 inwoners	Marge
Identiteitsfraude	1,6	0,1	1,3	0,1	0,7	0,1	0,6	0,1
waarvan								
skimming	1,1	0,1	0,8	0,1	0,4	0,1	0,2	0,0
phishing/pharming	0,5	0,1	0,5	0,1	0,4	0,1	0,4	0,1
Koop- en verkoopfraude	3,4	0,2	3,9	0,2	4,1	0,2	4,2	0,2
waarvan								
koopfraude	3,2	0,2	3,7	0,2	3,9	0,2	4,0	0,2
verkoopfraude	0,2	0,1	0,2	0,1	0,2	0,0	0,2	0,0
Hacken	8,8	0,4	9,3	0,3	7,9	0,3	7,6	0,3
waarvan								
ingebroken op computer	1,5	0,2	1,5	0,1	1,2	0,1	1,1	0,1
ingebroken op emailaccount	3,9	0,3	3,5	0,2	3,2	0,2	2,7	0,2
ingebroken op website/profielsite	2,2	0,2	2,5	0,2	2,1	0,2	2,4	0,2
anders	3,3	0,2	2,7	0,2	2,1	0,2	2,1	0,2
Cyberpesten	5,9	0,4	6,3	0,3	6,0	0,3	6,3	0,3
waarvan								
laster	1,8	0,2	2,0	0,2	1,8	0,2	1,8	0,2
stalken	1,6	0,2	1,5	0,2	1,6	0,2	1,9	0,2
chantage	0,5	0,1	0,3	0,1	0,4	0,1	0,6	0,1
bedreiging met geweld	1,0	0,2	1,1	0,1	1,0	0,1	1,1	0,2
anders	2,2	0,2	2,3	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).