Centraal Planbureau

CPB Notitie | 15 oktober 2018

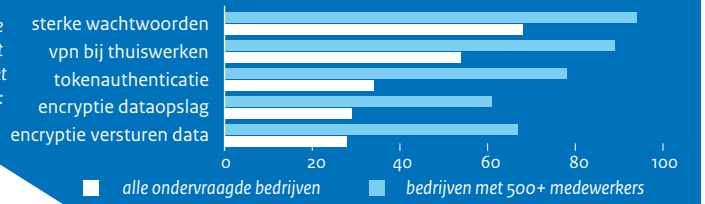
Risicorapportage Cyberveiligheid Economie 2018

Op verzoek van het ministerie van Justitie en Veiligheid

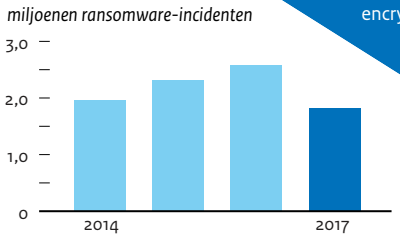
CPB Risicorapportage Cyberveiligheid 2018

Risico's mkb'er & particulier

Beveiligingsachterstand mkb-bedrijven op grote bedrijven



Minder gijzelsoftware



Grote ransomware-uitbraken (waarbij software apparaten gijzelt tot losgeld is betaald) nemen af

20 20% van de Nederlandse Android-gebruikers loopt extra risico door verouderde software

Cybercriminelen verleggen aandacht

In eerste helft 2018 zijn er 180 meldingen gedaan van **fraude via Whatsapp** in Nederland, tegen zestig in de periode 2015-2017

Het aantal incidenten waarbij computers van onwetende McAfee-gebruikers zijn ingezet om **cryptomunten te delven** is met 600% gestegen naar drie miljoen

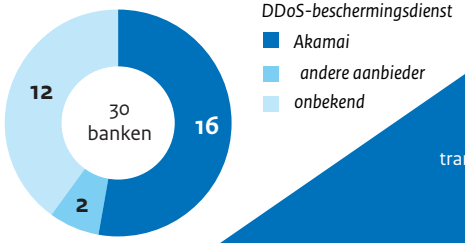
33% van **malafide websites** maakt gebruik van het https-protocol. Veel gebruikers denken ten onrechte dat https-sites altijd bonafide zijn

Continue digitale wapenwedloop

Criminelen gaan geraffineerder te werk waardoor gebruikers vaak lastig onderscheid kunnen maken tussen bonafide en valse berichten en websites. Cyberbeveiliging is een miljardenbusiness met zijn eigen valkuilen.

Marktmacht bij beveiliging banken

53% van 's werelds belangrijkste dertig banken heeft dezelfde beschermingsdienst tegen DDoS-aanvallen; Akamai uit de VS. Uitwisseling van aanvalsdata is van belang voor concurrentie tussen en verbetering van beveiligingsdiensten



Kosten lopen op

11 11% van Nederlandse bedrijven maakte in 2016 kosten door hacks. De hoogte van deze kosten is onbekend

Directe schade: product- en arbeidskosten voor herstel en preventie, schade door aanvallen. **Indirecte schade:** gemiste transacties, verminderd vertrouwen, minder gebruik digitale diensten

114.000.000.000

De wereldwijde omzet aan cyberveiligheidsproducten en –diensten om dat alles tegen te gaan bedroeg $101 miljard in 2017 en groeit naar verwachting door naar $114 miljard dit jaar

Nederland in voorhoede

95 In het Regeerakkoord is €95 miljoen geoormerkt voor cyberveiligheid

De Wet computercriminaliteit III geeft politie meer bevoegdheden om cybercriminaliteit te bestrijden

28 28% van het Nederlandse internetverkeer valideert data via de DNSSEC-standaard. Dat is meer dan het EU-gemiddelde (24%), maar minder dan Noorwegen en Zweden (>80%)

73 Ruim 70% van veelbezochte .nl-websites is goed beveiligd, tegen 61% wereldwijd

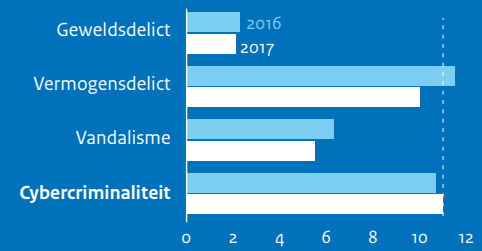
3 Een half miljoen (3%) Nederlanders had in 2016 financiële schade door een online-incident. In de helft van de gevallen bedroeg de schade €100 of meer

Lichte toename cyberdelicten

Nederlanders zijn vaker slachtoffer van een cyberdelict dan van andere delictsvormen. Afgelopen jaar liet van alle soorten delicten alleen cyber-criminaliteit een (lichte) stijging zien. De pakkans blijft bovendien laag.

Meer cyberdelicten

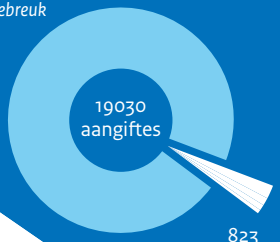
percentage mensen dat aangeeft slachtoffer te zijn geweest



Lage pakkans

Het aantal computervredebreukzaken waarbij een verdachte in beeld is, lag in 2015 op 4,6%, veel lager dan het gemiddelde voor alle misdrijven (26% in 2017). Over de periode 2007-2016 kwam 4,3% van de aangiftes van computervredebreuk terecht bij het Openbaar Ministerie

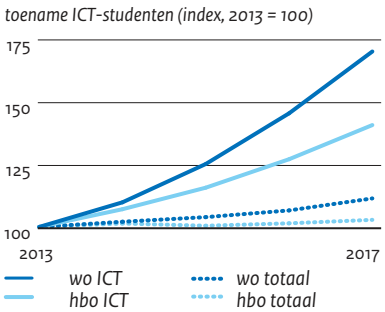
aangiftes van computervredebreuk tussen 2007 en 2016



Toename aanbod ICT'ers

De voorspelde tekorten aan ICT'ers vallen lager uit door een groter aanbod. Desondanks ervaren veel organisaties nog een tekort

toename ICT-studenten (index, 2013 = 100)



25 Het aantal vacatures voor ICT'ers stijgt in twee jaar 25%, maar voor de totale arbeidsmarkt is die toename groter, namelijk 57%

Voor de oorspronkelijke grafieken en de exacte gegevens zie de complete rapportage op www.cpb.nl. Bronnen: CBS, CPB, DUO, Gartner

Centraal Planbureau

CPB Notitie

Centraal Planbureau
Bezuidenhoutseweg 30
2594 AV Den Haag
Postbus 80510
2508 GM Den Haag

T 088 9846000
I www.cpb.nl

Contactpersoon
Bastiaan Overvest
Mariëlle Non
Freek Ruesink
Rinske Windig

Aan: Ministerie van Justitie en Veiligheid

Datum: 15 oktober 2018
Betreft: Risicorapportage Cyberveiligheid Economie 2018

1 Inleiding

1.1 Hoofdpunten

Met de digitalisering van de samenleving neemt ook het economische belang van cyberveiligheid toe. Op verzoek van het ministerie van Justitie en Veiligheid (J en V) schrijft het Centraal Planbureau daarom sinds 2016 jaarlijks een Risicorapportage Cyberveiligheid Economie (RCE). Het doel van deze rapportage is om de belangrijkste risico's voor de economie in kaart te brengen. Dit zijn de hoofdpunten van de RCE 2018:

1. Cybercriminaliteit leidt tot economische schade voor zowel bedrijven als huishoudens. Elf procent van de Nederlandse bedrijven maakte in 2016 kosten die werden veroorzaakt door een hack.[1] Van de huishoudens had drie procent financiële schade door een online incident, waarbij het in de helft van de gevallen gaat om meer dan honderd euro.[2] Cybercriminaliteit leidt via verschillende kanalen tot economische schade. Als door een hack een bedrijf langere tijd stilvalt, leidt dit tot gemiste omzet. Zo had containerbedrijf Maersk vorig jaar een kostenpost van 200 tot 300 miljoen dollar vanwege het nonPetya-virus. Een hack kan ook tot indirecte schade leiden, als verderop in de productieketen een distributeur producten niet geleverd krijgt. De uitgaven aan diensten van cyberveiligheidsbedrijven zijn in feite ook economische schade; dat geld had anders productief besteed kunnen worden. Deze kosten zijn omvangrijk: de wereldwijde markt voor cyberveiligheid wordt geschat op 114 miljard dollar.[3]

[1] Bron: CBS.
[2] CBS, ICT-gebruik huishoudens en personen.
[3] Bron: Gartner (link).

In sommige gevallen is de schade als gevolg van cybercriminaliteit (of breder: verstoringen van cyberveiligheid) moeilijker te kwantificeren. DDoS-aanvallen op banken of cryptobeurzen kunnen leiden tot afstel van transacties en minder gebruik van digitale financiële diensten, maar onbekend is nog wat de economische schade hiervan is. Internationale cyberconflicten kunnen indirect economische consequenties hebben via aanscherping van handelsbeperkingen. Ten slotte zijn de potentiële economische en maatschappelijke kosten van cybercriminaliteit bij vitale processen waarschijnlijk enorm. Lloyd's (2017) schat bijvoorbeeld de eventuele schade van een uitval van clouddiensten in de Verenigde Staten in op 5 tot 53 miljard dollar en het IMF laat zien dat de mogelijke schade voor financiële instellingen door cyberaanvallen kan oplopen tot honderden miljarden dollars.[4]

2. Cyberveiligheid is een continue wapenwedloop waarbij Nederland in internationaal perspectief voorop loopt. Wereldwijd wordt in 2019 een omzetgroei voor cyberveiligheidsbedrijven verwacht van negen procent ten opzichte van 2018.[5] De Nederlandse overheid draagt ook bij: in het Regeerakkoord wordt structureel 95 miljoen euro extra uitgetrokken voor cyberveiligheid. Tegelijkertijd is een groter percentage Nederlanders slachtoffer van cyberdelicten dan van andere vormen van criminaliteit en blijft cybercriminaliteit vaak onbestraft. De tweestrijd tussen cyberveiligheid en cybercriminelen evolueert continu. Illustratief voor de inventiviteit van criminelen zijn slimmere ransomware, het oneigenlijk delven van cryptomunten en steeds sluwere phishingmails. De maatschappij (in brede zin) probeert via aanpassing van wetgeving, certificering en verplichte updates de reguliere gebruiker te beschermen. Nederland doet het in dit opzicht goed. Zo loopt Nederland voorop in de toepassing van versleutelingsstandaarden en treffen Nederlandse internet-service-providers (zoals KPN en Ziggo) maatregelen om DDoS-aanvallen tegen te gaan.

3. Vooral MKB en thuisgebruikers lopen vermijdbare risico's. Bedrijven uit het MKB treffen minder vaak cyberveiligheidsmaatregelen dan grote bedrijven, zoals encryptie bij het versturen en opslaan van data en token-authenticatie. Thuisgebruikers zijn regelmatig nalatig in het installeren van updates. Daarnaast zijn er veel verouderde smartphones en tablets in omloop waarvan de software niet meer wordt ondersteund en kwetsbaarheden dus niet meer worden gerepareerd.

4. De voorspelde tekorten aan ICT'ers vallen lager uit door een sterke toename van het aanbod. ICT'ers zijn gewild op de arbeidsmarkt. Zo is de helft van de ICT-vacatures moeilijk te vervullen (UWV, 2018). Vier jaar geleden werd al voorzien dat de vraag naar ICT'ers sterk zou toenemen, volgens Dialogic (2014) met 18 procent in 2019. Deze verwachte stijging van de vraag ging in de afgelopen jaren samen met een

[4] https://blogs.imf.org/2018/06/22/estimating-cyber-risk-for-the-financial-sector/.
[5] Bron: Gartner.

stijging van het aanbod van ICT'ers. Zo kregen ICT-opleidingen veel meer studenten. Mede hierdoor steeg het aantal ICT'ers in het laatste decennium met honderdduizend banen. Een signaal van krapte op de arbeidsmarkt is dat lonen stijgen. De lonen voor ICT'ers laten echter geen duidelijke stijging zien ten opzichte van werkenden met een andere opleiding. Voor bepaalde (cyberveiligheid) expertises kan de krapte en de salarisontwikkeling anders zijn dan voor de gemiddelde ICT'er.

5. Delen van aanvalsdata zorgt voor snellere en betere DDoS-mitigatie. DDoS-aanvallen kunnen nooit helemaal voorkomen worden, maar de schade kan wel worden beperkt. Goede DDoS-mitigatie is hierbij van groot belang. Mitigeren gaat beter wanneer er meer DDoS-aanvalsdata beschikbaar zijn. Met deze data worden de algoritmes getraind die aanvallen detecteren en de gegevensstroom filteren. Een gestructureerde uitwisseling van aanvalsdata tussen DDoS-mitigatiediensten ontbreekt echter. Als gevolg hiervan kan een informatiepositie uitgebuit worden: de aanbieder van DDoS-mitigatie met de grootste datastroom kan het beste algoritme ontwikkelen en de concurrentie wegdrukken.

1.2 Leeswijzer

Het volgende hoofdstuk bespreekt de belangrijkste knelpunten rondom cyberveiligheid. We gaan hier in op de achterliggende oorzaken van verstoringen. In paragraaf 2.1 komen knelpunten bij de bestrijding van cybercriminaliteit aan bod. Daarna bespreken we in paragraaf 2.2 de knelpunten rondom hard- en softwarekwetsbaarheden. In paragraaf 2.3 gaan we in op risico's voor een goed werkende markt voor cyberveiligheid. Tot slot bieden we in paragraaf 2.4 een verdieping met een bespreking van de arbeidsmarkt voor cybersecurityprofessionals en ICT'ers.

In hoofdstuk 3 komen verschillende concrete dreigingen en manifestaties aan bod. De onderzoeksvraag is daarbij hoe waarschijnlijk het is dat de dreiging zich voordoet, hoe ernstig deze is en welke risico's zich verder kunnen voordoen. Paragraaf 3.1 begint met een discussie van de risico's bij datalekken. Vervolgens gaat paragraaf 3.2 in op financieel gemotiveerde malware (zoals ransomware) en paragraaf 3.3 bespreekt de risico's op DDoS-aanvallen. Gezien de gebleken kwetsbaarheid van belangrijke websites voor DDoS-aanvallen onderzoekt paragraaf 3.4 de risico's voor de markt voor DDoS-mitigatie. De RCE 2018 sluit af met paragraaf 3.5 over social engineering.

2 Knelpunten

2.1 Bestrijding cybercriminaliteit

Kern

- Er is een continue wapenwedloop gaande tussen cybercriminelen en opsporingsdiensten.[6]
- Het aantal aangiftes en vervolgingen van cyberdelicten is laag in vergelijking met andere typen delicten. Dit komt o.a. doordat cybercriminaliteit vaak grensoverschrijdend is. Cybercriminaliteit blijft zo vaak onbestraft.
- Versterking van internationale samenwerking tussen opsporingsdiensten en bedrijven is daarom wenselijk om cybercriminelen op te sporen en vervolgen.

In deze rapportage verstaan we onder cybercriminaliteit alle delicten die gepleegd worden met behulp van ICT. Het betreft zowel criminaliteit die gericht is op een ICT-systeem (bv. hacking of DDoS-aanvallen), als 'klassieke' criminaliteit die door ICT nieuwe vormen aanneemt (bv. internetoplichting of online verspreiding van kinderporno).[7]

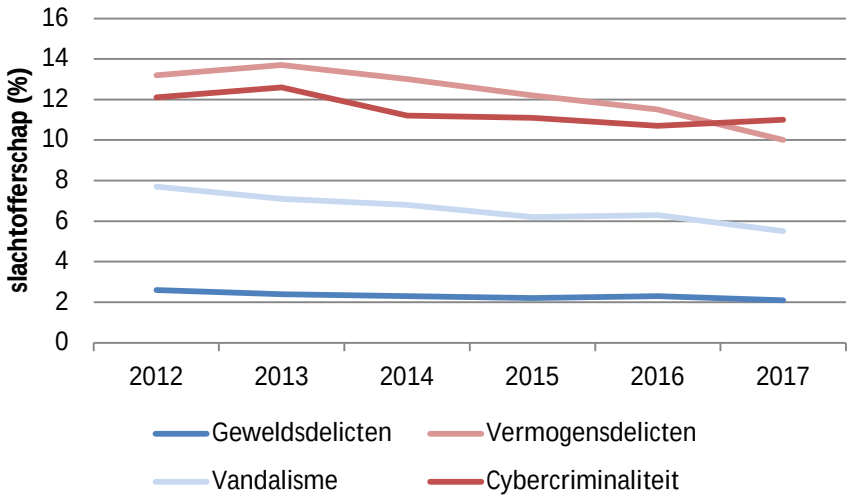
Met de digitalisering van de samenleving is het belang van bestrijding van cybercriminaliteit groter geworden. De CBS Veiligheidsmonitor rapporteert dat in 2017 elf procent van de respondenten slachtoffer is geworden van cybercriminaliteit.[8] Dit is iets meer dan het percentage slachtoffers van vermogensdelicten en ruim meer dan het percentage slachtoffers van vandalisme en geweldsdelicten (figuur 1). Het valt op dat in 2017 een lichte toename van het percentage slachtoffers van cybercriminaliteit is opgetreden, terwijl de overige vormen van criminaliteit een dalende trend vertonen. Het CBS onderscheidt verschillende vormen van cybercriminaliteit. Deze uitsplitsing[9] geeft aan dat koop- en verkoopfraude sinds 2012 toeneemt, terwijl het percentage slachtoffers van hacken en identiteitsfraude afneemt (figuur 2). De daling van identiteitsfraude wordt vooral veroorzaakt door een afname van skimming.

Ook bedrijven hebben te maken met cybercriminaliteit. Dertien procent van de bedrijven die zijn ondervraagd in de CBS-enquête 'ICT-Gebruik Bedrijven', geeft aan dat er in 2016 een ICT-dienst is uitgevallen door een aanval van buitenaf, bij dertien

[6] Preventie van cybercriminaliteit komt aan bod in paragraaf 2.2 en 2.3.
[7] Deze definitie volgt de definitie die het CBS hanteert, zie de Cybersecuritymonitor 2017.
[8] CBS meet alleen incidenten die slachtoffers zelf ervaren. Soms zijn ze zich er niet van bewust dat ze bestolen worden.
[9] Het slachtofferschap van cybercriminaliteit in figuur 1 is lager dan de optelsom van de verschillende vormen van cybercriminaliteit in figuur 2. Een deel van de respondenten is slachtoffer geworden van meerdere vormen van cybercriminaliteit.

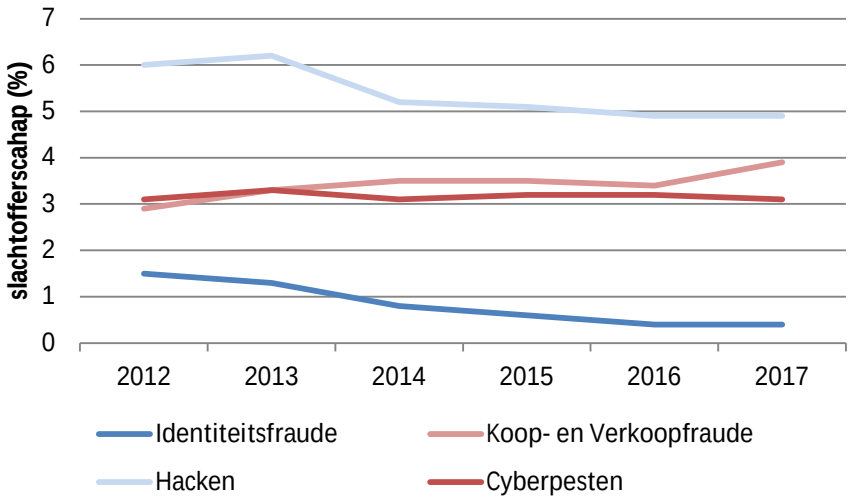
procent van de ondervraagde bedrijven leidde een aanval van buitenaf tot vernietiging van data en bij drie procent lekten persoonsgegevens.[10] Over de gemiddelde financiële impact van een aanval zijn geen enquêtegegevens.

Figuur 1 **Vaker cybercriminaliteit dan vermogensdelicten**



NB: percentage respondenten dat zegt slachtoffer te zijn geworden van type delict. Bron: CBS Statline.

Figuur 2 **Slachtofferschap cybercriminaliteit**



NB: percentage respondenten dat zegt slachtoffer te zijn geworden van type cyberdelict. Bron: CBS Statline.

[10] Bron: CBS Statline.

Risico's

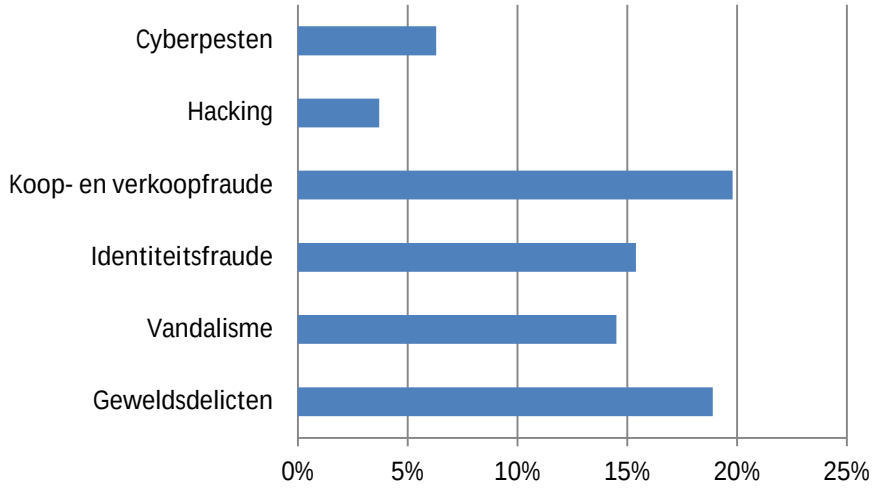
Er is sprake van een continue wapenwedloop tussen enerzijds cybercriminelen en anderzijds opsporingsdiensten. De technische drempel tot het plegen van cybercriminaliteit wordt steeds lager. Cybercriminaliteit-as-a-service maakt het bijvoorbeeld mogelijk om online een DDoS- of phishingaanval te kopen (zie ook de paragraaf over DDoS-aanvallen). Deze ontwikkeling kan een nieuwe groep criminelen zonder technische achtergrond aantrekken. Ook de groep professionele criminelen blijft innoveren, zowel op technisch gebied als op het gebied van misleiding van de burger. Het is daarom te verwachten dat cybercriminaliteit de komende jaren verder zal groeien. Tegelijkertijd ontwikkelt de opsporing ook. Zo geeft de recente Wet computercriminaliteit III de politie meer bevoegdheden om cybercriminaliteit te bestrijden en is er in het Regeerakkoord structureel 95 miljoen euro extra uitgetrokken voor cyberveiligheid. Desondanks blijft het risico bestaan dat de opsporing achterloopt op cybercriminelen.

Inadequate bestrijding van cybercriminaliteit maakt het voor criminelen aantrekkelijker om een delict te plegen. De economische literatuur over criminaliteit[11] neemt als uitgangspunt dat criminelen een afweging maken tussen de kosten en de baten van het plegen van een delict. De baten kunnen bestaan uit financieel gewin, zoals bij verkoopfraude, maar kunnen ook bijvoorbeeld betrekking hebben op het opbouwen van een criminele reputatie. De pakkans, de kans op straf en de zwaarte van de straf zijn onderdeel van de kosten van het plegen van een delict. Van adequate bestrijding van cybercriminaliteit gaat daarom een afschrikwekkende werking uit.

De aangiftebereidheid en pakkans bij cybercriminaliteit is lager dan bij andere typen delicten. Figuur 3 geeft het percentage slachtoffers weer dat aangifte heeft gedaan bij de politie.[12] Met name bij cyberpesten en hacking ligt de aangiftebereidheid laag. Bij online fraude is de aangiftebereidheid redelijk vergelijkbaar met 'klassieke' vormen van criminaliteit. Slachtoffers van cybercriminaliteit maken, wellicht onbewust, een afweging tussen de kosten en baten van het doen van aangifte. Voor slachtoffers van fraude kunnen de baten van aangifte relatief hoog zijn als aangifte nodig is voor een schadevergoeding. De potentiële baten van aangifte zijn daarnaast hoger als het een ernstig delict betreft. Wanneer het slachtoffer echter inschat dat de kans klein is dat de dader wordt opgespoord, verlaagt dat de baten van aangifte. De kosten bestaan uit de tijd en moeite om aangifte te doen, maar ook schaamtegevoelens kunnen een rol spelen.[13]

[11] Zie o.a. Becker (1986), Crime and punishment: an economic approach.
[12] De politie is niet het enige meldpunt van cybercriminaliteit. Identiteitsfraude wordt in ongeveer driekwart van de gevallen gemeld bij de bank of financiële instelling en 15 procent van de slachtoffers van hacking meldt zich bij een andere instantie dan de politie.
[13] Zie ook Jong, Leukfeldt en Van de Wijer (2018), Determinanten en motivaties voor intentie tot aangifte na slachtofferschap van cybercrime, *Tijdschrift voor Veiligheid*, 17(1-2).

Figuur 3 Aangiftebereidheid



NB: percentage slachtoffers dat aangifte heeft gedaan bij de politie van type delict. Bron: CBS Statline.

Net als bij burgers doen lang niet alle bedrijven aangifte bij de politie van ICT-veiligheidsincidenten. Hoewel 21 procent van de bedrijven zegt dat er in 2016 een veiligheidsincident[14] is opgetreden door een aanval van buiten, heeft slechts 2 procent aangifte gedaan. Daarnaast worden incidenten soms ook gemeld bij de Autoriteit Persoonsgegevens (2 procent) en banken (2 procent). Bij het doen van aangifte door bedrijven spelen waarschijnlijk dezelfde overwegingen als bij burgers.

Bij slechts een klein deel van de aangiftes van computervredebreuk[15] wordt uiteindelijk een verdachte geïdentificeerd, en van deze verdachten wordt slechts een klein deel door de rechter veroordeeld. Het ophelderingspercentage, het aantal zaken waarbij een verdachte in beeld is, lag bij computervredebreuk in 2015 op 4,6 procent.[16] Voor alle misdrijven lag het ophelderingspercentage in 2017 op 26 procent.[17] Dit verschil wordt onder andere veroorzaakt door een beperkte recherchecapaciteit (onderzoek naar cybercriminaliteit kost veel tijd i.v.m. bevragingen en rechtshulpverzoeken) en een beperkte opsporingsindicatie. Zo zit de mogelijke dader vaak in het buitenland en zijn er vaak geen directe concrete sporen of getuigenverklaringen (zoals bij een mishandeling of vernieling). Daarnaast geeft de politie aan dat bij cyberveiligheid relatief vaak sprake is van dubbele aangiftes. Op dit moment gebruiken de elf eenheden aparte systemen; hierdoor leidt de overdracht van aangiftes tussen eenheden tot dubbele registratie.

[14] Veiligheidsincidenten betreffen zowel incidenten veroorzaakt door aanvallen van buitenaf als interne incidenten.
[15] Computervredebreuk, ofwel inbreken in een computersysteem, is de enige vorm van cybercriminaliteit waarvoor aparte cijfers over verdachten en veroordelingen worden bijgehouden. Internetoplichting wordt geregistreerd in de algemene categorie 'oplichting'.
[16] CBS Cybersecuritymonitor 2017.
[17] Factsheet strafrechtketen 2017 (link).

Van de zaken die in de periode 2007-2016 bij het OM terechtkwamen, leidde uiteindelijk 16,5 procent tot een schuldigverklaring van de rechter (figuur 4). Daarnaast werd in 23,9 procent van de zaken geschikt, of zonder tussenkomst van de rechter een straf opgelegd. Bij alle ingeschreven misdrijfzaken in 2007-2016 volgde in 45 procent een schuldigverklaring door de rechter; veel meer dus dan bij computervredebreuk. Het percentage zaken waarin werd geschikt of zonder tussenkomst van de rechter een straf werd opgelegd, is voor alle misdrijfzaken samen 20,7 procent. Dit is redelijk vergelijkbaar met het percentage bij computervredebreuk.

Figuur 4 Computervredebreuk in de strafrechtketen: totaal aantal zaken 2007-2016.

Bron: CBS Misdrijfstatistieken.

Beleidsopties

Vergroot de zichtbaarheid van digitale aangifte. Een laagdrempelig, online en centraal meldpunt helpt om het aangiftepercentage van cybercriminaliteit te verhogen en geeft de politie sneller informatie over type en ernst van het delict. Voor sommige cyberdelicten, zoals (ver-)koopfraude kan al digitaal aangifte gedaan worden. Ondanks deze mogelijkheid doen slachtoffers nu vaak nog geen aangifte. Meer bekendheid van de optie van digitale aangifte kan het aangiftepercentage verhogen. Om te zorgen dat vervolgens de pakkans daadwerkelijk omhoog gaat, is voldoende recherchecapaciteit nodig.

Investeer in internationale samenwerking rond bestrijding van cybercriminaliteit. Cybercriminelen zijn vaak internationaal actief. Samenwerking tussen opsporingsdiensten en (cyberveiligheids-)bedrijven lijkt een effectieve manier om cybercriminaliteit tegen te gaan – zie het 'No More Ransom' project.[18] Voor

[18] Het 'No More Ransom' project helpt slachtoffers van ransomware hun bestanden terug te krijgen. Bij dit project zijn onder andere Europol, Kaspersky, McAfee en de Nederlandse Politie aangesloten.

effectieve internationale opsporing in het cyberdomein kunnen bestaande (en mogelijk gedateerde) verdragen voor wederzijdse rechtshulp bij strafrechtelijk onderzoek (de 'Mutual legal assistance treaties') worden gemoderniseerd.

2.2 Hard- en softwarekwetsbaarheden

Kern

- Hard- en softwarekwetsbaarheden zijn een blijvend probleem. Het aantal gerapporteerde (hoogrisico-) kwetsbaarheden is in 2017 en 2018 sterk toegenomen.
- Afgelopen jaar zijn belangrijke kwetsbaarheden gevonden in veel gebruikte hardware. Repareren van deze kwetsbaarheden is complex.
- Er is nog veel oude software in omloop die niet meer wordt ondersteund door de fabrikant, maar ook bij nieuwere software zijn consumenten vaak slordig met het installeren van updates.
- Kwetsbaarheden voorkomen is moeilijk. Beleid zal zich moeten richten op het beperken van de schade, bijvoorbeeld door automatische installatie van updates als *default*-instelling.

Een kwetsbaarheid is een ontwerpfout in hard- of software waarvan cybercriminelen misbruik kunnen maken. Het risico van een kwetsbaarheid voor eindgebruikers is afhankelijk van de kans op misbruik en van de schade als misbruik plaatsvindt. Kwetsbaarheden in hard- en software kunnen zeer ernstige gevolgen hebben. Zo maakte de nonPetya ransomware-aanval in 2017 onder meer gebruik van een kwetsbaarheid in Microsoft Windows.

Het aantal nieuwe kwetsbaarheden dat is opgenomen in de National Vulnerability Database (NVD)[19] is in 2017 en de eerste helft van 2018 explosief gestegen (zie figuur 5). Vanwege een toegenomen aantal melders hoeft de stijging in het aantal kwetsbaarheden niet noodzakelijk te betekenen dat hard- en software in 2017 en 2018 meer bugs bevat dan in de periode vóór 2017. Het is ook mogelijk dat kwetsbaarheden die in het verleden niet officieel werden geregistreerd, nu wel worden opgenomen in de NVD-database. Hoewel een directe vergelijking met eerdere jaren dus complex is, is het wel duidelijk dat er nog altijd veel nieuwe kwetsbaarheden worden gevonden.

[19] De NVD is een database van bekende softwarekwetsbaarheden die wordt onderhouden door het National Institute of Standards and Technology, een onderdeel van het U.S. Department of Commerce.

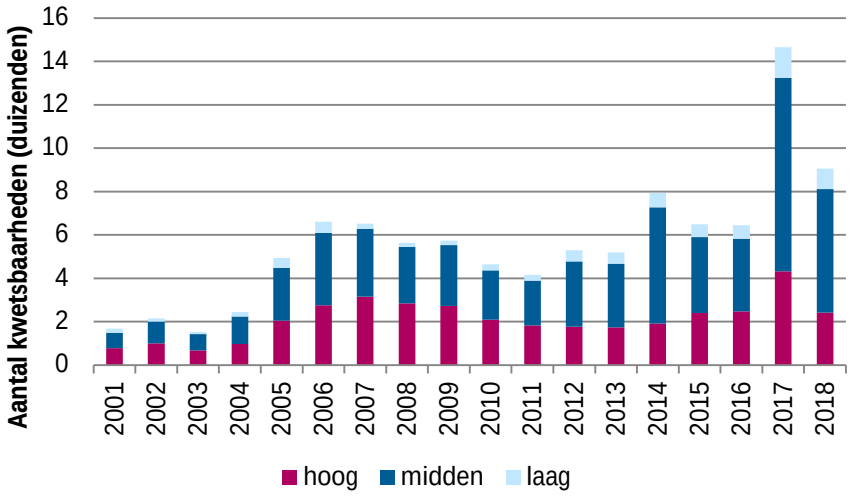
Risico's

Het is te verwachten dat ook in de komende jaren nieuwe kwetsbaarheden ontdekt zullen worden. Met de ontwikkeling van hard- en software neemt ook de complexiteit toe, waardoor ook het risico op fouten toeneemt. Ontwikkelaars maken een soms impliciete afweging tussen het verminderen van fouten en snelheid en betaalbaarheid van productontwikkeling. Daarnaast zijn kwetsbaarheden niet direct zichtbaar voor de klant, waardoor de producent geen sterke prikkel heeft om een foutloos product te leveren. Dit ligt anders wanneer een kwetsbaarheid eenmaal ontdekt is – snel uitbrengen van een update draagt dan bij aan de reputatie van de producent.

Kwetsbaarheden in hardware, zoals die het afgelopen jaar aan het licht zijn gekomen, zijn bijzonder risicovol omdat ze grote aantallen gebruikers treffen en moeilijk te repareren zijn. Terugkijkend op afgelopen jaar springen drie kwetsbaarheden eruit: Broadpwn (juli 2017), Meltdown en Spectre (beide januari 2018).[20] Broadpwn treft WiFi-chipsets die zich in meer dan 1 miljard smartphones bevinden.[21] Meltdown en Spectre zijn kwetsbaarheden in processoren die sinds 1995 in vrijwel alle PC's, smartphones en tablets worden toegepast.[22] Het aantal potentiële slachtoffers is daarmee zeer groot. Het feit dat de kwetsbaarheden zich in hardware bevinden, maakt het repareren van de kwetsbaarheden moeilijker. Hardware kan over het algemeen niet via het internet worden gerepareerd. In het geval van Broadpwn, Meltdown en Spectre bleek het mogelijk om de kwetsbaarheid uiteindelijk te verhelpen door updates uit te brengen voor alle software die via de kwetsbaarheid kan worden misbruikt. Een risico hierbij is dat vaak meerdere softwareproducenten als derde partij nodig zijn om een kwetsbaarheid in hardware te verhelpen. Hierdoor kunnen coördinatieproblemen ontstaan die de ontwikkeling van een update vertragen en cybercriminelen de tijd geven om de kwetsbaarheid te misbruiken. Daarnaast is de fabrikant van hardware afhankelijk van softwareproducenten die geen direct belang hebben bij het oplossen van het probleem.

[20] Meer informatie is te vinden in het Cybersecuritybeeld Nederland.
[21] Zie bijvoorbeeld dit nieuwsbericht.
[22] Hier is meer informatie te vinden over Spectre en Meltdown.

Figuur 5 Toename gerapporteerde (hoogrisico-)kwetsbaarheden



Bron: National Vulnerability Database, https://nvd.nist.gov. NB. Aantal kwetsbaarheden 2018 is tot en met augustus 2018.

De vondst van nieuwe typen kwetsbaarheden in hardware in het afgelopen jaar kan ertoe leiden dat er meer soortgelijke kwetsbaarheden worden ontdekt. Tot afgelopen jaar had het weinig zin om specifiek te zoeken naar fouten in hardware. De kans op een grote vondst was klein en de investering in tijd en moeite niet waard. Nu duidelijk is dat er een ontwerpfout bestaat, wordt het aantrekkelijk om verder te zoeken naar vergelijkbare kwetsbaarheden. Omdat dit soort vondsten veel aandacht krijgen in de IT-wereld, draagt het vinden van een kwetsbaarheid bij aan de reputatie van een (legitieme) onderzoeker en kan het in sommige gevallen leiden tot financiële beloning. Het hoge aantal potentiële slachtoffers maakt van dit type kwetsbaarheden ook een aantrekkelijk onderzoeksterrein voor cybercriminelen. De prijs voor kwetsbaarheden en exploits wordt op de zwarte markt in belangrijke mate bepaald door de populariteit van de soft- en hardware waarin de kwetsbaarheid is gevonden.[23] Sinds de eerste bekendmaking van Meltdown en Spectre in januari 2018 zijn dan ook verschillende nieuwe varianten opgedoken.[24]

Software die niet meer wordt ondersteund door de ontwikkelaar, is nog altijd veel in omloop en vormt daarmee een risico. Zo draait in Nederland ruim 20 procent van de Android smartphones en tablets op een verouderde versie van het besturingssysteem.[25] Dit is lager dan in heel Europa (30 procent), maar wel hoger dan in landen met een vergelijkbaar percentage mensen dat dagelijks online is: Zweden (17 procent), Finland (19 procent), Noorwegen (15 procent) en Luxemburg (16 procent). Het probleem wordt verergerd doordat beschikbare updates niet altijd

[23] Zie ook deze analyse.
[24] Zie onder andere de nieuwsberichten hier en hier.
[25] Bron: statcounter, bezocht op 30 juli 2017. Hierbij zijn versies 6.0, 7.0, 7.1 en 8.0 geteld als 'nog ondersteund'.

(of tijdig) worden doorgegeven door de hardwarefabrikant. Afgelopen jaar heeft de Consumentenbond aandacht gevraagd voor Samsung smartphones die geen updates meer doorkrijgen van Samsung, ondanks dat Android het besturingssysteem nog wel ondersteunt. Bij IoT-apparaten speelt hetzelfde probleem. Zo krijgt een aantal smartwatches die draaien op Android 7.0 geen update meer naar versie 8.0, waardoor te verwachten is dat deze smartwatches over enige jaren niet meer ondersteund worden.[26] Zeker bij apparaten met een lange levensduur kan dit ertoe leiden dat consumenten nog lange tijd gebruik maken van een slecht beveiligd apparaat. Niet alleen loopt de consument hierbij het risico dat het apparaat door criminelen onbruikbaar wordt gemaakt; gehackte IoT-apparaten kunnen ook worden ingezet om een botnet te vormen en DDoS-aanvallen uit te voeren waar anderen last van hebben. Consumenten hebben geen prikkel om rekening te houden met dit laatste risico bij hun beslissing om een niet ondersteund apparaat al dan niet te vervangen. Hierdoor is te verwachten dat onveilige apparaten langer in omloop blijven dan wenselijk.

Ook sommige vitale processen lopen risico's door gebruik van niet (meer) ondersteunde software. Denk hierbij bijvoorbeeld aan de systemen van sluizen en gemalen van waterschappen. De gebruikte oplossingen gaan lang mee, maar worden niet altijd meer voorzien van beveiligingsupdates[27]. Dit kan zorgen voor gevaarlijke situaties, zoals afgelopen jaar ook in Saudi-Arabië bleek. Daar ontsnapte de omgeving – door een fout van de hackers zelf – ternauwernood aan een explosie van een petrochemische fabriek[28]. Omdat veel industriële gebruikers dezelfde technieken hanteren, is een eenmaal gevonden kwetsbaarheid vermoedelijk snel uit te buiten bij meerdere vitale processen[29].

Een deel van de gebruikers loopt daarnaast risico door nalatigheid in het installeren van updates. Een internationale studie uit 2015[30] laat zien dat vrijwel geen enkele update door meer dan 90 procent van de gebruikers wordt geïnstalleerd. Het kan ook lang duren voordat gebruikers updates installeren; bij Chrome had 15 dagen na het uitbrengen van een update de helft van de gebruikers deze geïnstalleerd, bij Word duurde dit gemiddeld 79 dagen en bij Flash zelfs 247 dagen. De verschillen tussen de pakketten worden waarschijnlijk veroorzaakt door het updatebeleid. Tijdens de periode van onderzoek werden updates voor Chrome automatisch geïnstalleerd, terwijl Flash eerst toestemming vroeg voor het downloaden en installeren van updates.

[26] Voor meer informatie, zie hier.
[27] Zie bijvoorbeeld dit nieuwsbericht.
[28] Zie bijvoorbeeld de berichtgeving in de New York Times.
[29] Een voorbeeld is een kwetsbaarheid in veel gebruikte technologie van Schneider Electric.
[30] Hier te vinden.

Er zijn meerdere redenen voor de nalatigheid van gebruikers. Bij bedrijven kan het installeren van een update ertoe leiden dat bedrijfsspecifieke systemen niet meer werken. Grote bedrijven kiezen er daarom vaker voor om updates eerst te testen en handmatig te installeren. Dit is een arbeidsintensief proces, waardoor bedrijven kunnen achterlopen met hun beveiliging. Ook consumenten kunnen bang zijn dat het installeren van updates leidt tot crashende programma's of een langzamer apparaat. Daarnaast kost het installeren van een update enige tijd en zijn consumenten zich niet altijd bewust van het belang van updates. Met name bij IoT-apparaten realiseren gebruikers zich niet altijd dat ook bijvoorbeeld de slimme koelkast van tijd tot tijd een beveiligingsupdate nodig heeft – als een update al mogelijk is.

Beleidsopties

Idealiter ondersteunen fabrikanten hun producten gedurende de hele levensduur met tijdige updates. De rechtszaak van de Consumentenbond tegen Samsung heeft laten zien dat dit in de praktijk moeilijk af te dwingen is.[31] De wetgeving op dit gebied kan worden aangescherpt door een wettelijk verplichte ondersteuningsperiode op te nemen. Een verplichte ondersteuningsperiode heeft ook nadelen: het kan kostbaar zijn en kan leiden tot schijnveiligheid als een fabrikant slechte *updates* gaat aanbieden. Ook kan het innovatie afremmen als fabrikanten gedwongen wordt om met hun oude producten te concurreren.[32]

Gedragseconomische inzichten helpen om nalatigheid van gebruikers te voorkomen. De gedragseconomie onderzoekt hoe mensen tot (economische) keuzes komen en op welke manier beleid kan helpen om tot betere beslissingen te komen. Empirisch onderzoek naar financiële geletterdheid laat zien dat het heel moeilijk is om via voorlichting of trainingen mensen tot verstandiger keuzes te laten komen.[33] Effectiever is het vaak om een bepaalde standaard of *default* te stellen, waarbij mensen automatisch iets verstandigs doen, tenzij ze daar bewust van afstappen. In de context van softwareveiligheid is een interessante *default* bijvoorbeeld automatische installatie van updates. Dit zorgt ervoor dat gebruikers veel sneller bijgewerkt zijn.

2.3 Markt voor cyberveiligheid

Kern

- Door voortgaande digitalisering is de markt voor cyberveiligheid een groeimarkt.
- Er is veel onzekerheid over de omvang van cyberrisico's en de kwaliteit en betrouwbaarheid van oplossingen, waardoor risico ontstaat voor zowel onder- als overinvesteringen in cyberveiligheid.

[31] Voor meer details zie de website van de Consumentenbond.
[32] Zie de te verschijnen CPB Policy Brief over veilige digitale middelen.
[33] Zie de meta-analyse van Fernandes e.a. (2014), 'Financial literacy, financial education, and downstream financial behaviors', *Management Science*, 60(8).

- MKB-bedrijven hebben een beveiligingsachterstand op grote bedrijven en lopen onnodige risico's.

In de afgelopen jaren is de vraag naar cyberveiligheid toegenomen en die groei zet waarschijnlijk door. De wereldwijde omzet aan cyberveiligheidsproducten en -diensten bedroeg in 2017 101 miljard dollar en groeit naar verwachting door naar 114 miljard dollar dit jaar.[34] Het is aannemelijk dat de vraag naar cyberveiligheidsoplossingen de komende jaren vanwege drie factoren verder zal stijgen. De belangrijkste factor is de digitalisering van de samenleving: door de toenemende behoefte aan digitale diensten en oplossingen ontstaat ook een grotere noodzaak voor cyberveiligheid. Ten tweede stelt de overheid scherpere eisen aan cyberveiligheid. Een bekend voorbeeld is de Algemene Verordening Gegevensbescherming (AVG) die vereist dat organisaties die persoonsgegevens verwerken, deze met moderne technieken beschermen, maar ook via de Wet gegevensverwerking en meldplicht cybersecurity (Wgmc)[35] stelt de overheid cyberveiligheidsverplichtingen. De derde factor is dat door een aantal incidenten, zoals WannaCry en nonPetya, organisaties zich, wereldwijd, bewuster lijken te worden van cyberdreigingen. Ter illustratie: tien jaar geleden stonden cyberaanvallen onderaan de top-10 van de meest waarschijnlijke risico's in het Global Risk Report van het World Economic Forum (bovenaan: daling van beurskoersen, onrust in het Midden-Oosten en olieprijsstijgingen). In 2018 staan cyberaanvallen op de derde plek van de dertig genoemde risico's.

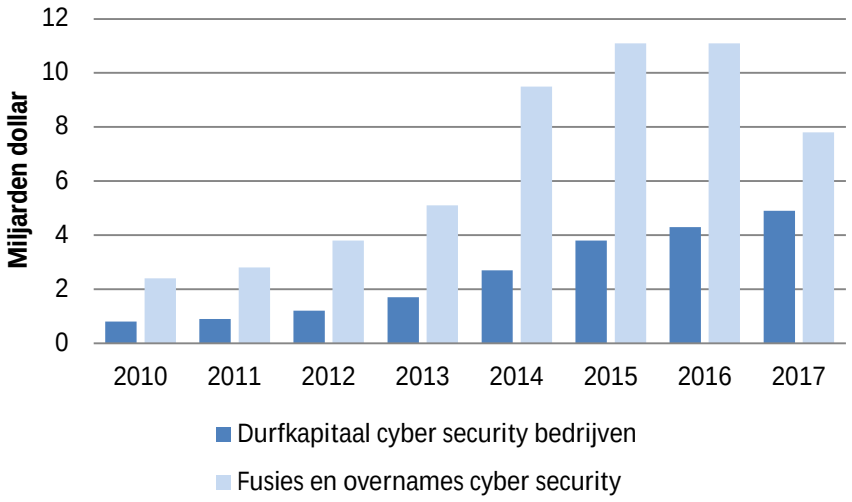
Ook de Nederlandse overheid geeft meer geld uit aan cyberveiligheid. In het Regeerakkoord 2017-2021 is structureel 95 miljoen euro gereserveerd voor cyberveiligheid. Hiervan is 26 miljoen euro beschikbaar vanaf 2018. Dit geld is bedoeld om cyberspionage en –sabotage aan te pakken en cybercriminaliteit te bestrijden. Daarnaast wordt een deel besteed aan het opzetten van een Digital Trust Center dat cyberveiligheid bevordert bij het bedrijfsleven.[36] De overige 69 miljoen uit het regeerakkoord wordt onder andere ingezet voor uitbreiding van de personele capaciteit en ICT-voorzieningen en wordt verdeeld over verschillende departementen, waaronder Justitie en Veiligheid (NCTV), Defensie (MIVD) en Binnenlandse Zaken en Koninkrijksrelaties (AIVD).

De toegenomen vraag naar cyberveiligheidsoplossingen leidt tot een toename van het aanbod. Dit blijkt uit het aantal investeringen in nieuwe cyberveiligheidsbedrijven. Tussen 2010 en 2017 vervijfvoudigde wereldwijd de omvang van durfkapitaal in cyberveiligheidsbedrijven (figuur 6). In diezelfde periode nam de waarde van fusies en overnames voor cyberveiligheidsbedrijven met meer

[34] Gartner (link).
[35] De Wgmc zal na goedkeuring door de Eerste Kamer opgaan in de Wet beveiliging netwerk- en informatiesystemen.
[36] Zie miljoenennota 2018.

dan vijf miljard dollar toe. Ook in Nederland is er durfkapitaal voor de sector.[37] De toegenomen vraag naar cyberveiligheid leidt tot extra vraag naar cybersecurity-professionals. Voor cybersecurityprofessionals ontbreken administratieve cijfers, maar in de Nederlandse ICT-sector als geheel nam het aantal banen tussen 2015 en 2017 toe met 7,3 procent, tegen 3 procent in de gehele economie.[38] In paragraaf 2.4 gaan we dieper in op de arbeidsmarkt voor cybersecurity-experts en ICT'ers.

Figuur 6 Toename venture capital in cyberveiligheidssector



Bron: Thomson Reuters (link).

Risico's

Een afname van vertrouwen in buitenlandse cyberveiligheidsbedrijven vergroot de afhankelijkheid van Nederlandse aanbieders. De markt voor cyberveiligheid kan grofweg worden afgebakend in een markt voor hoogwaardige cyberveiligheidsoplossingen (zoals beveiliging van staatsgeheimen, beveiliging van intellectueel eigendom of gevoelige persoonsgegevens) en laagwaardige cyberveiligheidsoplossingen (zoals antivirussoftware voor huishoudens). Met name voor het hoogwaardige deel van de markt is er een gebrek aan vertrouwen in buitenlandse aanbieders, wat leidt tot een marktfragmentatie langs landsgrenzen.[39] Voorbeelden zijn de oproep om software van Kaspersky niet meer te gebruiken[40], de zorgen bij de Nederlandse overheid na de overname van Fox-IT[41] en de samenwerking van Nederlandse cyberveiligheidsbedrijven.[42] Een verdere afname

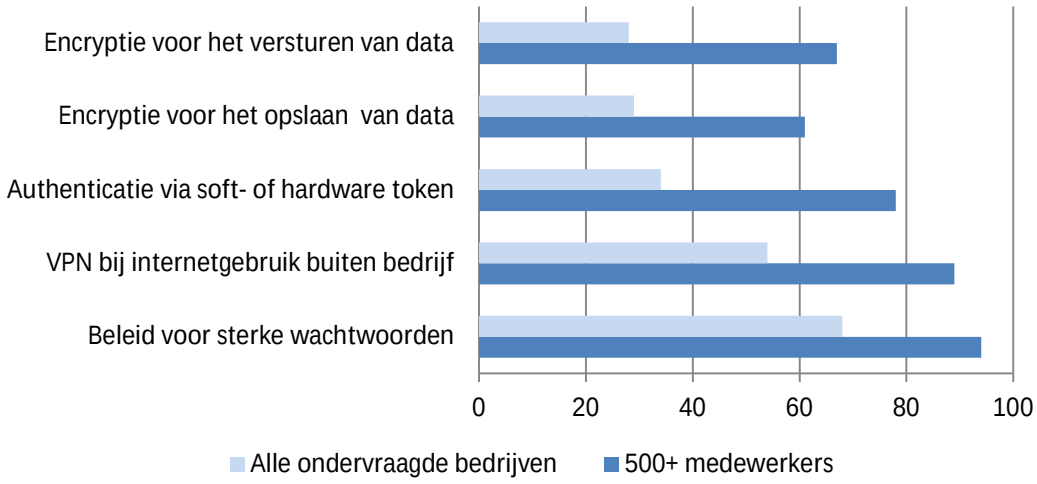
[37] Zie bijvoorbeeld dit artikel in het FD.
[38] Bron: CBS Statline.
[39] Zie EC (2017, link) en Overvest e.a. (2018), 'Knelpunten op de Europese markt voor cyberveiligheid', CPB Policy Brief.
[40] Zie deze Kamerbrief.
[41] Volgens dit artikel in NRC.
[42] Zie dit FD-artikel.

van het vertrouwen in buitenlandse aanbieders leidt tot een verschraling van het aanbod en kan tot hogere prijzen of lagere kwaliteit leiden.

Het gebrek aan betrouwbare informatie over cyberdreigingen leidt tot onzekerheid over kosten en baten van investeringen in cyberveiligheid, met een risico op zowel onder- als overinvesteringen. Mede door het ontbreken van openbaar toegankelijke data is er veel onzekerheid over de kans en kosten van een cyberaanval en de effectiviteit van specifieke maatregelen. De weinige beschikbare schattingen zijn doorgaans gebaseerd op gemiddeldes en op niet transparante wijze tot stand gekomen. Hierdoor ontstaat het risico dat organisaties investeren in de verkeerde maatregelen of juist te weinig doen.

MKB-bedrijven hebben een beveiligingsachterstand op grote bedrijven en lopen mogelijk onnodige risico's. Van de kleine bedrijven met tien tot twintig werknemers had vijftien procent in 2016 te kampen met een cyberaanval.[43] Ook grotere bedrijven worden aangevallen, maar zij nemen meer voorzorgsmaatregelen. Zo gebruikt bijna tachtig procent van de grote bedrijven tokenauthenticatie, tegen 34 procent voor het gemiddelde bedrijf (figuur 7). Onduidelijk is of het verschil in beveiliging tussen MKB en grote bedrijven veroorzaakt wordt door een rationale kosten-batenafweging of door een kennisachterstand.

Figuur 7 Gebruik encryptie en authenticatie door Nederlandse bedrijven



Bron: CBS enquête ICT gebruik bedrijven 2017.

[43] Bron: CBS.

Beleidsopties

Om over- of onderinvesteringen te voorkomen kunnen overheden en bedrijven informatie delen over cyberveiligheid. Deze informatie helpt MKB-bedrijven bij de keuze om te investeren in cyberveiligheid. De overheid kan hier ook een intermediaire rol spelen, bijvoorbeeld door een netwerkrol of door het verzamelen en delen van statistische gegevens. Verder kunnen bedrijven, overheden en wetenschappers meer samenwerken in onderzoek naar de effectiviteit van specifieke maatregelen.

Maak internationale afspraken over gedrag van opsporings- en inlichtingendiensten in het cyberdomein. Zulke afspraken kunnen bijdragen aan het vertrouwen in buitenlandse aanbieders en zorgen voor schaalvergroting. Mogelijke internationale afspraken zijn een EU-standpunt over de voorwaarden waaronder inlichtingen- en opsporingsdiensten digitaal onderzoek mogen doen. Om de naleving van internationale afspraken te borgen kan een onafhankelijke autoriteit worden ingesteld – zoals de OPCW (chemische wapens) en de IAEA (atoomenergie). Zulke internationale afspraken kunnen het vertrouwen in buitenlandse aanbieders van cyberveiligheidsdiensten vergroten en leiden tot een grotere en effectievere Interne Markt voor cyberveiligheid.

2.4 De arbeidsmarkt voor cybersecurityprofessionals en ICT'ers

Kern

- Veel organisaties ervaren een tekort aan cybersecurityprofessionals (CSP'ers).
- Het aantal ICT'ers is sterk toegenomen in de afgelopen vijf jaar, waardoor de voorspelde tekorten lager uitvallen.
- Ondanks de relatieve krapte zijn er geen aanwijzingen dat salarissen van ICT'ers structureel harder stijgen dan bij andere beroepen.
- Organisaties met moeilijk te vullen vacatures kunnen hogere salarissen bieden, de kwaliteit van het werk verbeteren, cyberveiligheid meer automatiseren, buitenlandse CSP's aantrekken of genoegen nemen met lagere kwalificaties.

Volgens veel partijen uit het veld is er een groot tekort aan cybersecurity-professionals (CSP'ers) in Nederland. UWV (2018) noemt CSP als een van de zes moeilijk-invulbare ICT-vacatures[44] en afgelopen jaar waarschuwden verschillende hoogleraren voor een tekort aan cyberveiligheidsexperts in Nederland.[45] BCG (2016)[46] spreekt over een schaarste van ICT-professionals in Nederland en waarschuwt voor een tekort van 54 duizend fte in 2020.

[44] Bron: UWV (2018), 'ICT-beroepen factsheet arbeidsmarkt', 20 april 2018.
[45] Zie deze open brief en dit FD-artikel.
[46] BCG (2016), 'Digitizing the Netherlands'.

Dé CSP'er bestaat niet en is statistisch onvindbaar. Van Lakerveld e.a. (2014)[47] wijzen erop dat CSP een verzamelbegrip is, variërend van een technisch dominante specialistische CSP'er, zoals een software-tester of ethical hacker, tot niet-technisch dominante functies met cyberveiligheid als onderdeel, zoals een functionaris voor gegevensbescherming. Het is verder lastig om het tekort aan CSP'ers cijfermatig te duiden, omdat CSP'ers in de meeste arbeidsmarktstatistieken onder de bredere groep van ICT'ers vallen. Daarbij komt dat CSP'ers vaak vanuit een generieke opleiding, zoals een studie informatica, wiskunde of criminologie bij een organisatie aan de slag gaan en via werkervaring en trainingen cyberveiligheidsexpertise opdoen. In deze paragraaf kijken we om deze praktische én inhoudelijke redenen grotendeels naar de ontwikkeling van de arbeidsmarkt voor ICT'ers.

Tekorten op de lange termijn zijn onhoudbaar: vragers en aanbieders zullen zich aanpassen. Een organisatie met een onvervulde vacature voor een CSP (de vrager) kan zich aanpassen door een hoger loon te bieden of een lagere kwaliteit te accepteren, zoals door de vereiste kwalificaties aan te passen. Aankomende studenten of afgestudeerden (de aanbodzijde) kunnen reageren op de vraag door te kiezen voor een studie met een sterke cyberveiligheidscomponent of door het volgen van een training of postdoctorale opleiding. Vanwege deze aanpassingsmechanismen is overheidsingrijpen in principe niet zinvol, tenzij de overheid als werkgever optreedt of er bepaalde omstandigheden zijn waardoor het marktmechanisme niet goed werkt.[48]

Het ene aanpassingsmechanisme is efficiënter dan het andere. Een verhoging van het salaris is een snellere en mogelijk goedkopere oplossing dan het aantrekken van buitenlandse CSP's, als voor buitenlandse CSP'ers behalve een marktconform loon ook reis- en verblijfskosten moeten worden betaald. De relevante vraag is daarom in hoeverre de arbeidsmarkt voor CSP'ers/ICT'ers efficiënt reageert op de tekorten. De analyse hieronder suggereert dat de markt efficiënt reageert via een stijging van het arbeidsaanbod in Nederland.

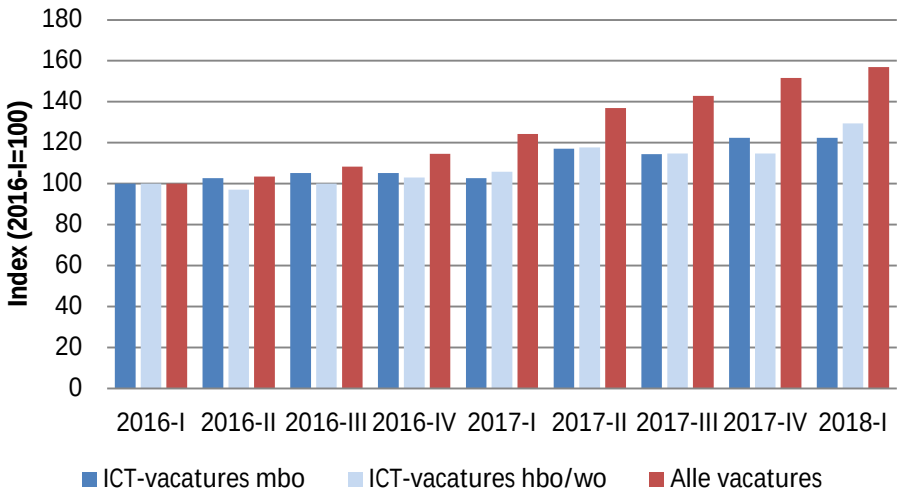
Er zijn verschillende aanwijzingen dat de krapte op de markt voor ICT'ers de laatste jaren toeneemt. Het UWV (2018) schat in dat het aantal vacatures voor ICT'ers in de afgelopen twee jaar is toegenomen met bijna 25 procent (figuur 8). De vraag naar ICT'ers op mbo-niveau is in vergelijkbare mate gegroeid als de vraag naar ICT'ers op hbo/wo-niveau. De krapte op de rest van de arbeidsmarkt lijkt nog sterker te zijn toegenomen: daar nam het aantal vacatures met 57 procent toe. Het aantal vacatures kan een onderschatting zijn van de vraag, als een vacature voor meerdere posities is of als organisaties via andere kanalen (zoals een headhunter) zoeken. Het kan ook een overschatting zijn, als een organisatie een poging doet om tegen niet-

[47] Van Lakerveld e.a. (2014), 'Arbeidsmarkt voor cyber security professionals'.
[48] Zie ook CPB (2013), 'Economische analyse van korte- en langetermijnknelpunten op de arbeidsmarkt'.

marktconforme voorwaarden een positie te vervullen. SEO (2018)[49] laat zien dat ICT'ers relatief snel een substantiële baan vinden: afgestudeerden van de studies Computer Science en Informatiekunde vinden gemiddeld[50] binnen drie maanden een werkgever, dat is twee maanden sneller dan afgestudeerde economen.

Het aantal ICT'ers is sterk toegenomen in de afgelopen jaren, waardoor de tekorten lijken mee te vallen. Van Lakerveld e.a. (2014) verwachtten een toename van de vraag naar CSP'ers. Dialogic, in een studie uit hetzelfde jaar, voorzag voor de periode tot 2019 een toename van de vraag naar ICT'ers van 18 procent. De tekorten lijken uiteindelijk mee te vallen, aangezien in de afgelopen tien jaar het aantal ICT'ers in Nederland met 28 procent is gestegen. Dit komt neer op een toename van ruim honderdduizend ICT-banen. In internationaal perspectief heeft de Nederlandse arbeidsmarkt veel ICT'ers; vijf procent van alle banen in Nederland is een ICT-baan, tegen 3,7 procent gemiddeld in de EU (figuur 9). Vergeleken met andere digitaal ontwikkelde landen scoort Nederland hierop gemiddeld.

Figuur 8 **Groei aantal ICT-vacatures lager dan op gehele arbeidsmarkt**



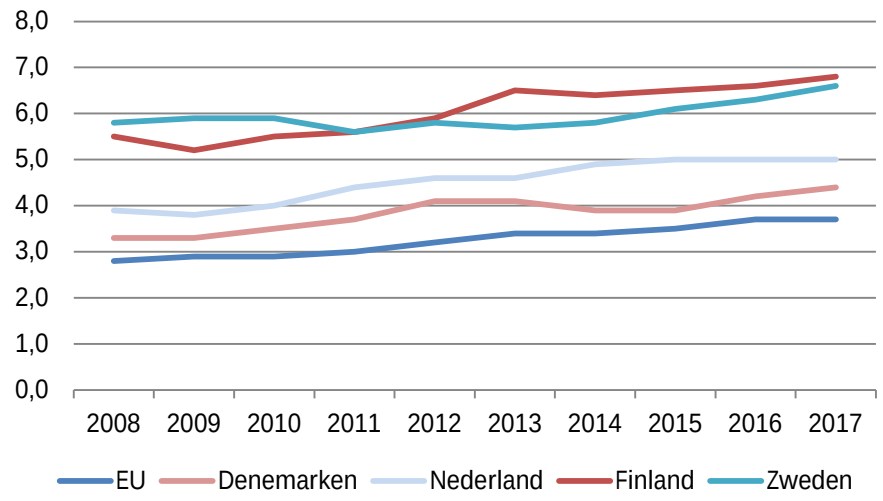
Bron: UWV (2018). Noot: aantal vacatures is geïndexeerd (2016-I=100).

Het aantal studenten dat een ICT-opleiding volgt, stijgt relatief nog harder dan het aantal ICT'ers. Tussen 2013 en 2017 nam het aantal ingeschreven ICT-studenten op hbo- of wo-niveau toe met bijna vijftig procent (figuur 10), tegen gemiddeld zeven procent voor alle studies. Kennelijk reageren aankomende studenten op de voorspelde krapte op de arbeidsmarkt. Onderwijsinstellingen reageren ook op de behoefte aan CSP'ers. Inmiddels zijn er in het hoger onderwijs ongeveer negentien

[49] SEO (2018), 'Studie & Werk 2018'.
[50] Preciezer: de mediane student.

verschillende cyberveiligheidsopleidingen, zowel op master- als bachelorniveau en voltijd en deeltijd, waarvan meer dan de helft opgestart zijn in 2013 of later.[51]

Figuur 9 **ICT'ers als percentage van totale werkgelegenheid**

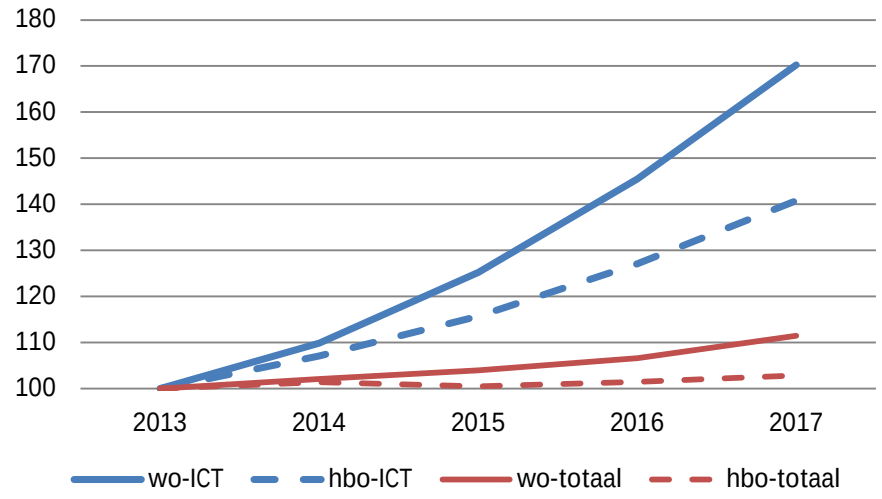


Bron: Eurostat.

De salarissen van ICT'ers lijken, ondanks de ervaren krapte, in Nederland niet structureel gestegen. In gesprekken zeggen bedrijven dat ze hogere lonen moeten bieden om CSP'ers of ICT'ers aan te trekken. In specifieke gevallen, zoals een ervaren CSP'er met aantoonbare expertise op meerdere technische onderwerpen, is dat goed mogelijk, maar er zijn geen aanwijzingen dat het gros van de ICT'ers momenteel grote loonsprongen maakt.[52] ICT'ers vanuit Computer Science of Informatiekunde uit het cohort 2006/2007 verdienden in de eerste baan gemiddeld iets minder dan afgestudeerde economen (figuur 11). Tien jaar later is het salarisverschil tussen economen en werknemers in Computer Science verder toegenomen. Pas afgestudeerde hbo'ers ICT of informatica verdienen in loondienst wel meer (11 procent) dan afgestudeerden Commerciële Economie.[53] Deze bevindingen suggereren dat de krapte op de markt voor ICT'ers niet groter is dan voor andere beroepsgroepen.

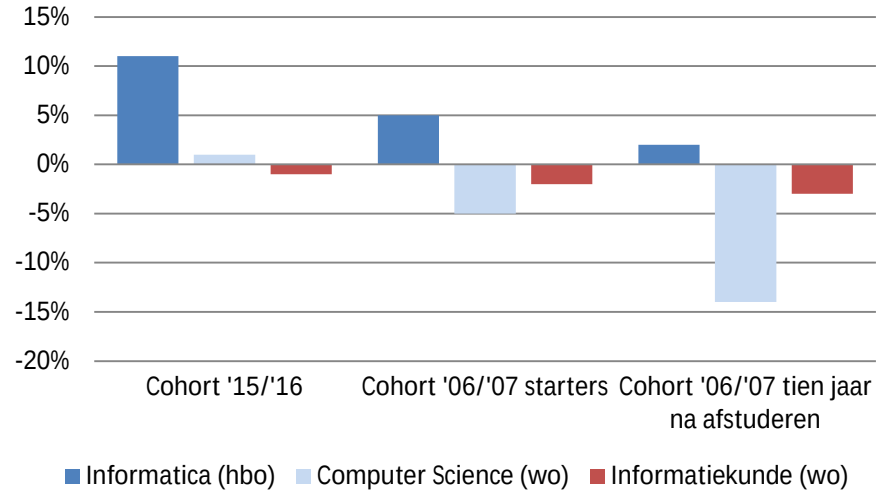
[51] Bron: dcypher (link).
[52] Zie https://www.bnr.nl/nieuws/financieel/10345781/loonontwikkeling-it-blijft-achter anekdotisch bewijs.
[53] Net afgestudeerde docenten of fysiotherapeuten verdienen overigens 30 procent meer en verloskundigen zelfs 60 procent meer dan bij commerciële economie.

Figuur 10 Aantal studenten ICT-opleiding stijgt relatief hard (2013=100)



Bron: DUO.

Figuur 11 Salarissen ICT-afgestudeerden t.o.v. afgestudeerde economen



Bron: SEO (2018). NB: Salarisverschillen t.o.v. Commerciële Economie (hbo) of Economie (wo).

De arbeidsmarkt voor ICT'ers is internationaal. De vaardigheden van ICT'ers zijn waarschijnlijk goed inzetbaar in het buitenland. Hierdoor kunnen ICT'ers waarschijnlijk eenvoudiger in een ander land aan de slag dan bijvoorbeeld een leraar. Anekdotisch bewijs suggereert dan ook dat Nederlandse studenten ICT relatief vaak voor een buitenlands avontuur kiezen en, omgekeerd, dat Nederlandse bedrijven ICT'ers over de grens zoeken.[54] Onderzoek van De Graaf e.a. (2007)[55] concludeert dat buitenlands arbeidsaanbod (in dit geval bèta's) een remmende werking lijkt te hebben op lonen voor bèta's in Nederland. In hoeverre buitenlands aanbod van CSP'ers in Nederland de lonen beïnvloedt, is nog onbekend.

Organisaties met moeilijk te vervullen vacatures kunnen hogere salarissen bieden, de kwaliteit van het werk verbeteren, cyberveiligheid meer automatiseren, buitenlandse CSP's aantrekken of genoegen nemen met lagere kwalificaties. Een organisatie die het cyberveiligheidsniveau wil verbeteren, kan dit doen door meer CSP'ers aan te nemen. Een directe manier om iemand aan te trekken is door het bieden van een aantrekkelijk salaris. Een tweede, indirecte, manier is om de beloning te verhogen door gunstiger arbeidsvoorwaarden te bieden. Ook kan de niet-financiële waardering verbeteren door een 'statusverhoging', misschien door cyberveiligheid dicht bij het bestuur te plaatsen. Ten derde kan een organisatie ervoor kiezen om lagere kwalificaties te vereisen voor nieuwe CSP'ers en deze met extra bedrijfstrainingen op niveau te brengen. De vierde optie is het werven van buitenlandse CSP'ers. Hier komen extra kosten bij voor reis- en verblijfkosten en mogelijk juridische kosten voor een werkvergunning. Ten slotte kan een organisatie het cyberveiligheidsniveau verbeteren door inzet van meer 'kapitaal' in plaats van 'arbeid', zoals door het uitbesteden van systemen aan sterk geautomatiseerde dienstverleners of het gebruik van duurdere maar veiliger veiligheidssoftware.

Beleidsopties

Overheidsbeleid moet gericht zijn op het laten werken van de arbeidsmarkt. Zoals hierboven beschreven zijn er op de arbeidsmarkt verschillende aanpassingsmechanismen die ervoor zorgen dat tekorten op de lange termijn verdwijnen. Hier hoeft de overheid niet direct op te sturen. Wel kunnen sommige aanpassingsmechanismen onnodig inefficiënt zijn vanwege overheidsbeleid. Beperkingen op het in dienst nemen van buitenlandse werknemers kunnen de markt frustreren. De overheid zou kunnen onderzoeken of het proces voor werkvergunningen efficiënter kan of dat (ICT-)diploma's internationaal beter vergelijkbaar kunnen worden. De overheid kan verder zorgen voor objectieve informatie over de arbeidsmarktperspectieven van opleidingen. Dit helpt aankomende studenten bij het maken van een geïnformeerde studiekeuze.

[54] Zie bijvoorbeeld dit FD-artikel.
[55] De Graaf e.a. (2007), 'De arbeidsmarkt van hoger opgeleide bèta's', *SEO Rapport*, 992.

Voorkom dat arbeidsaanbod ICT'ers beperkt wordt door numerus fixus bij opleidingen. Bij enkele universiteiten is voor de studies technische informatica en kunstmatige intelligentie een numerus fixus ingesteld[56], omdat ze de snelle groei van het aantal studenten dat deze studies willen volgen niet aan kunnen. Het beperken van de instroom is onwenselijk in een situatie waarin er nog steeds een tekort op de arbeidsmarkt is. Door onderwijsinstellingen te ondersteunen in het opleiden van een groeiend aantal studenten kan het aanbod blijven reageren op de behoefte vanuit de markt.

3 Dreigingen en manifestaties

3.1 Datalekken

Kern

- Data zijn steeds waardevoller. Organisaties blijven daarom op grote schaal persoonsgegevens verzamelen, met datalekken als bijgevolg.
- De directe kosten van datalekken lopen op tot 1,1 procent van de marktwaarde van het bedrijf.
- De AVG maakt organisaties bewuster van de verantwoordelijkheid om data te beschermen, maar verhoogt compliance-kosten en mogelijk de toetredingskosten voor uitdagers van Facebook of Google.

Ook in het afgelopen jaar kwam een groot aantal datalekken[57] aan het licht. In september 2017 maakte Equifax, een Amerikaanse consumentenkredietbeoordelaar, bekend dat van 145 miljoen mensen persoonsgegevens waren gestolen bij een hack. Bij Uber zouden van 57 miljoen klanten en chauffeurs gegevens zijn buitgemaakt. De meest spraakmakende zaak is die van Cambridge Analytica – dit bedrijf zou al in 2015 persoonsgegevens van 87 miljoen Facebookgebruikers hebben verzameld en gebruikt voor politieke campagnes. Dit najaar kwam een nieuw datalek bij Facebook naar boven: 50 miljoen accounts zouden zijn gehackt, waarvan 5 miljoen in Europa.

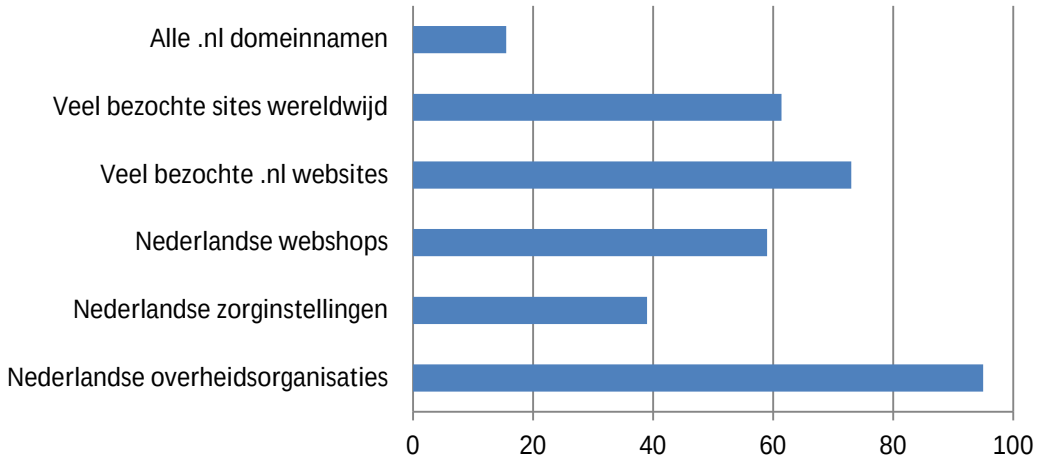
De AVG maakt organisaties bewuster van de verantwoordelijkheid om persoonsgegevens te beschermen. Op 25 mei 2018 trad de Algemene Verordening Gegevensbescherming (AVG) in werking. Dit is de privacywetgeving die voor de gehele EU van toepassing is. Organisaties die persoonsgegevens verwerken, zijn verplicht om aan te tonen dat ze daar toestemming voor hebben en daarvoor is een meldplicht datalekken van toepassing. De bedoeling van deze wet is om burgers en

[56] Bron: Studiekeuze123.nl.
[57] Bij een datalek worden persoonlijke en zakelijke gegevensgegevens vernietigd, gewijzigd of heeft een onbevoegd persoon onbedoeld inzage.

hun persoonsgegevens beter te beschermen. Het lijkt erop dat sommige organisaties sindsdien bewuster omgaan met persoonsgegevens,[58] maar of de AVG echt zal slagen is nog onzeker; veel gebruikers lijken meestal 'blind' voorwaarden te accepteren en maken zo nog geen bewuste afweging.

Nederlandse websites lijken relatief zorgvuldig om te gaan met persoonsgegevens. Mogelijk vanwege de komst van de AVG maken veelbezochte .nl-sites en Nederlandse webshops gebruik van SSL, waarmee het verkeer tussen de browser en de server versleuteld wordt (figuur 12). 73 Procent van de Nederlandse veelbezochte websites gebruiken SSL, tegen 61 procent wereldwijd.

Figuur 12 Percentage websites met SSL-certificaat



Bronnen: SIDN, Forum Standaardisatie, Cybersprint, Qualys SSL Labs (scan van 3 augustus 2018), Pulse (scan van 7 augustus 2017).

Risico's

Met de voortschrijdende digitalisering worden steeds meer data verzameld en neemt de kans op datalekken toe. De hierboven genoemde datalekken betreffen big data, die verzameld zijn vanwege hun commerciële waarde. De gegevens van Equifax geven waardevolle informatie over kredietwaardigheid; de data van Uber helpen programmeurs om de app te optimaliseren en de Facebookgegevens maken gerichte politieke advertenties mogelijk. Door de opkomst van kunstmatige intelligentie (AI) kunnen data op steeds meer verschillende en onverwachte manieren gebruikt worden – organisaties zullen daarom voorlopig nog wel doorgaan met het verzamelen van data. Negentien procent van de Nederlandse bedrijven analyseerde op enige manier big data in 2016 – ruim meer dan het Europees gemiddelde van tien procent.[59] De ervaring laat zien dat datalekken het gevolg kunnen zijn van onbedoelde (menselijke) fouten. In 2017 was bijna de helft van de

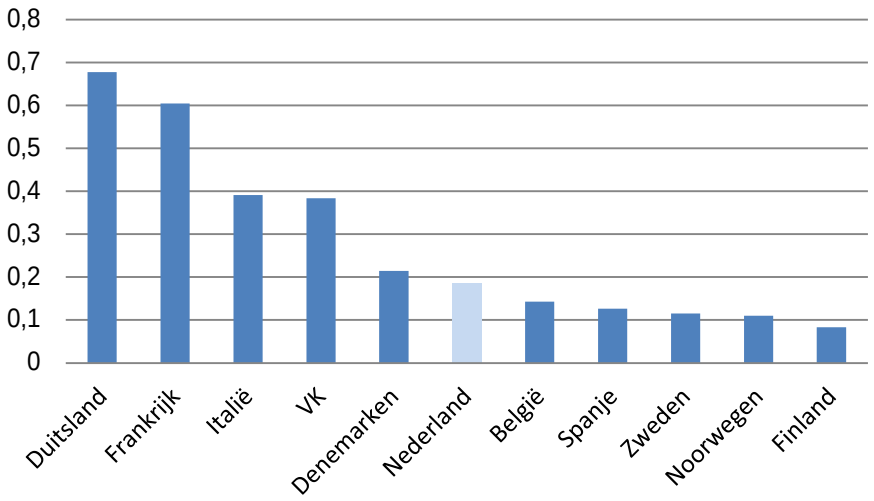
[58] Zo plaatsten Europese nieuwssites minder cookies van derden zonder toestemming sinds de AVG (bron).
[59] Bron: Eurostat.

10.009 meldingen bij de Autoriteit Persoonsgegevens (AP) veroorzaakt doordat gegevens aan de verkeerde ontvanger verstuurd waren.[60] Hacks komen ook vaak voor. De AP registreerde daarvan zo'n 600 in 2017 (6 procent van het totaal aan datalekken).

Datalekken bevatten soms gegevens die direct misbruikt kunnen worden. Dit is vooral zo bij financiële gegevens als creditcardinformatie. In een empirische studie over 188 Amerikaanse datalekken in de periode 2005 tot 2014 laten Kamiya e.a. (2018) zien dat een datalek een significant negatieve impact heeft op de beurswaarde van een onderneming als daarbij financiële informatie van consumenten is gestolen.[61] Na een lek van financiële consumentengegevens daalt de waarde gemiddeld met 1,1 procent: voor het gemiddelde bedrijf een verlies van 607 miljoen dollar per aanval.

Gestolen wachtwoorden en andere persoonsgegevens kunnen jaren later nog gebruikt worden voor identiteitsfraude. Als iemand hetzelfde wachtwoord voor verschillende systemen gebruikt, dan zijn al deze systemen kwetsbaar. Ook buitgemaakte bijzondere persoonsgegevens kunnen hergebruikt worden in een doelgerichte phishingaanval. Volgens een zoekmachine van gelekte wachtwoorden gaat het in Nederland om 3,1 miljoen accounts, exclusief web-based e-mailadressen van bijvoorbeeld Gmail die niet gekoppeld zijn aan een land. Omgerekend naar aantallen internetgebruikers komt dit in ons land neer op één gehackt account per vijf gebruikers. Dit is in dezelfde orde van grootte als de aantallen in Denemarken en Zweden – landen met vergelijkbaar digitaliseringsniveau (figuur 13).

Figuur 13 Aantal gehackte accounts per internetgebruiker (2017)

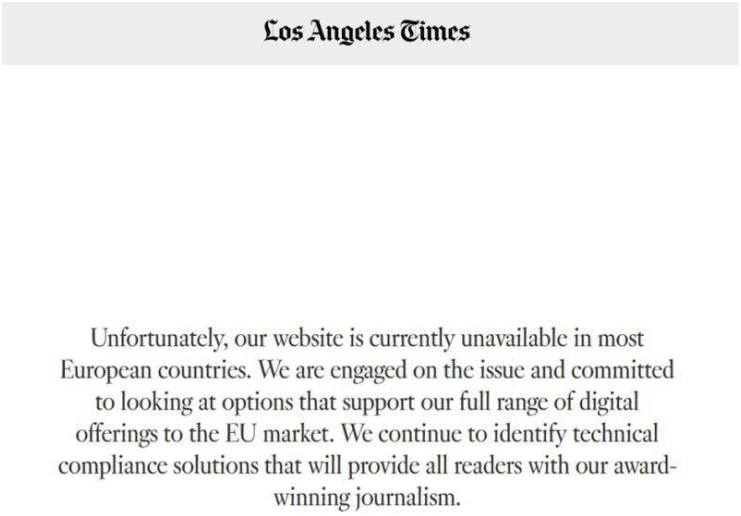


Bron: Gelekte accounts: https://gotcha.pw. Internetgebruik: Eurostat, omvang bevolking: Wereldbank. Alle cijfers zijn voor 2017.

[60] Bron: jaarrapportage Autoriteit Persoonsgegevens 2017.
[61] Kamiya e.a. (2018), 'What is the impact of successful cyberattacks on target firms?', *NBER Working Paper*, 24409.

De AVG leidt tot hogere compliance-kosten en kan het gebruik van big-data-analyses onnodig afremmen. Gemiddeld kosten het melden en verwerken van een datalek bij Nederlandse gemeenten 32 uur, met een totale kostenpost van 4,6 miljoen euro.[62] Voor twee derde van de Amerikaanse bedrijven schat PwC de totale compliance-kosten in op 1 tot 10 miljoen dollar.[63] Deze compliance-kosten kunnen in het voordeel van tech-giganten als Google en Facebook uitpakken, als de toetredingsbarrière voor nieuwe uitdagers hoger wordt.[64] Sommige Amerikaanse nieuwssites zijn onbereikbaar geworden vanuit Europa na de inwerkingtreding van de AVG (figuur 14). Tot slot bestaat het risico dat organisaties te terughoudend worden bij het slim gebruiken van data.[65] Een kenmerk van big data is dat deze op onverwachte manieren toegepast kunnen worden – toepassingen waarvoor mogelijk geen toestemming vooraf is gevraagd. Dit is niet een strikt hypothetisch risico: Miller en Tucker (2009) laten zien dat ziekenhuizen minder vaak een elektronisch patiëntendossier gebruiken in staten met privacywetgeving.[66]

Figuur 14 Toetredingsbarrières door AVG?



Bron: www.latimes.com, bezocht op 11 september 2018.

De AVG lijkt opsporing van cybercriminaliteit te bemoeilijken.
Opsporingsdiensten maken bij hun onderzoek vaak gebruik van WHOIS-data. WHOIS-data zijn gegevens over o.a. de namen, adressen en telefoonnummers van contactpersonen voor domeinen. In mei van dit jaar oordeelde de ICANN (de

[62] Bron: Binnenlands Bestuur (link).
[63] Bron: Guardian (link).
[64] Zie dit stuk in *Wall Street Journal* (link).
[65] Zie bijvoorbeeld Agrawal e.a. (2018), 'Economic policy for artificial intelligence', *Voxeu.org* (link).
[66] Miller en Tucker (2009), 'Privacy protection and technology diffusion: the case of electronic medical records', *Management Science*, 55(7), p. 1077-1093.

organisatie die uiteindelijk verantwoordelijk is voor WHOIS) dat de data niet voldoen aan de AVG. Europol ziet dit als een inperking van hun onderzoekmethoden.[67]

Beleidsopties

De Autoriteit Persoonsgegevens kan overwegen om meldingen openbaar te maken en/of burgers standaard te informeren wanneer hun persoonsgegevens gelekt zijn. Het is niet aannemelijk dat van de markt voldoende prikkels uitgaan om datalekken te beperken: het hergebruik van gestolen persoonsgegevens op de langere termijn vergroot de negatieve externe effecten en beursgenoteerde ondernemingen kunnen een prikkel hebben om een datalek niet te melden. Dit zorgt ervoor dat een incident niet of pas veel later aan het licht komt en asymmetrische informatie over de beveiliging van persoonsgegevens blijft op die manier intact. Door een datalek bekend te maken verbetert de informatiepositie van burgers en dit kan een disciplinerende werking hebben. Daarnaast vergroten sancties na zeer ernstige datalekken de geloofwaardigheid van het toezicht**.**

Betrek bij de evaluatie van de AVG ook de effecten op compliance-kosten, concurrentie en big-datatoepassingen. De AVG zal uiterlijk in 2020 geëvalueerd worden (Artikel 97 van de AVG). Omdat de AVG ook mogelijk onvoorziene gevolgen kan hebben op compliance-kosten, toetredingsdrempels en het gebruik van big data, is het aan te bevelen om deze aspecten mee te nemen in de evaluatie. Onderzocht kan worden of het toezicht en de regels voldoende aansluiten bij de grootte van organisaties en of, net als in het mededingingstoezicht, mogelijkheden bestaan voor richtlijnen of vrijstellingen om organisaties meer houvast te geven.

3.2 Financieel gemotiveerde malware

Kern

- Grote ransomware-uitbraken waren het afgelopen jaar beperkt. Er lijkt een verschuiving gaande naar andere vormen van malware.
- Het gebruik van cryptojacking nam sterk toe met de toegenomen populariteit van cryptomunten. In tegenstelling tot ransomware levert cryptojacking geld op voor criminelen zonder monetaire overdracht van slachtoffer naar crimineel.
- Toenemende professionalisering van cybercriminelen kan zorgen voor een grotere betaalbereidheid bij slachtoffers van ransomware.

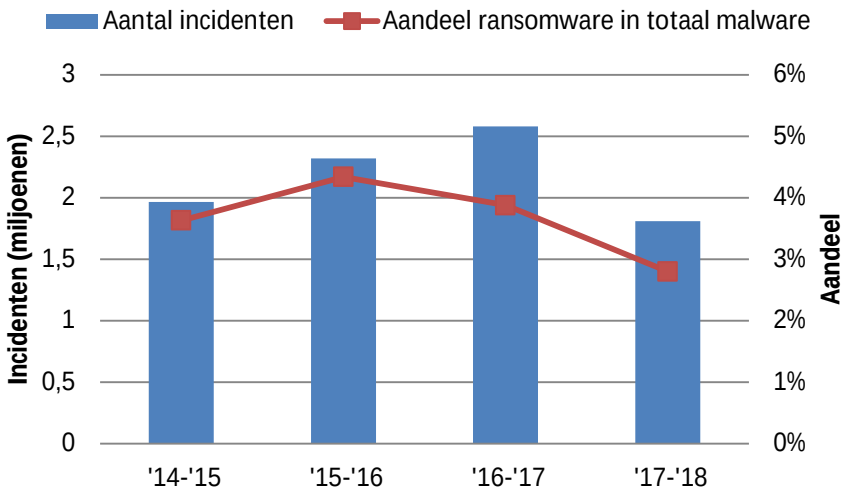
Ontwikkelaars van financieel gemotiveerde malware richtten zich afgelopen jaar minder op ransomware om geld te verdienen. Dit is onder andere te zien aan het feit dat het relatieve aantal ransomware-incidenten is afgenomen: zie het aantal incidenten als percentage van de totale hoeveelheid malware (figuur 15, rood). Ook is het absolute aantal aanvallen van ransomware gedaald (figuur 15, blauw).

[67] Europol (2018), 'Internet organised crime threat assessment (IOCTA)', blz. 60.

Vermoedelijk spelen de hoge ontwikkelkosten van ransomware hierin een belangrijke rol – het aantal nieuwe ransomwarefamilies in 2017 is teruggekeerd op een niveau vergelijkbaar met 2014 en 2015 (figuur 16). 2016 lijkt een eenmalige uitschieter. Desondanks blijven zich (kleinschalige) incidenten met ransomware voordoen.[68,69,70]

Cryptojacking is in toenemende mate het nieuwe verdienmodel van cybercriminelen. Bij cryptojacking gebruikt men de processorkracht van (onwetende) computergebruikers om cryptomunten te delven (*mining*). De gedolven munten worden vervolgens op legale wisselkantoren omgezet in standaardvaluta. Het aantal gebruikers dat last heeft van cryptojacking is in de periode 2012-2017 vertienvoudigd[71]. Daarbovenop noteerde beveiligingsbedrijf McAfee in het eerste kwartaal van 2018 bij gebruikers zelfs een kwartaalstijging van ruim 600 procent[72]: van 400 duizend incidenten tot bijna 3 miljoen. De illegale opbrengsten van cryptojacking hangen sterk samen met de waarde van cryptomunten. Het risico hiervan zal dus vermoedelijk sterk correleren met de waardeontwikkeling van cryptomunten. Browserontwikkelaars nemen wel beschermingsstappen tegen cryptojacking. Google laat sinds april 2018 Chrome-extensies die cryptocurrency delven niet meer toe[73]. Innovatie waardoor geen extensies meer nodig zijn, heeft inmiddels plaatsgevonden – met Coinhive als meest bekende voorbeeld[74].

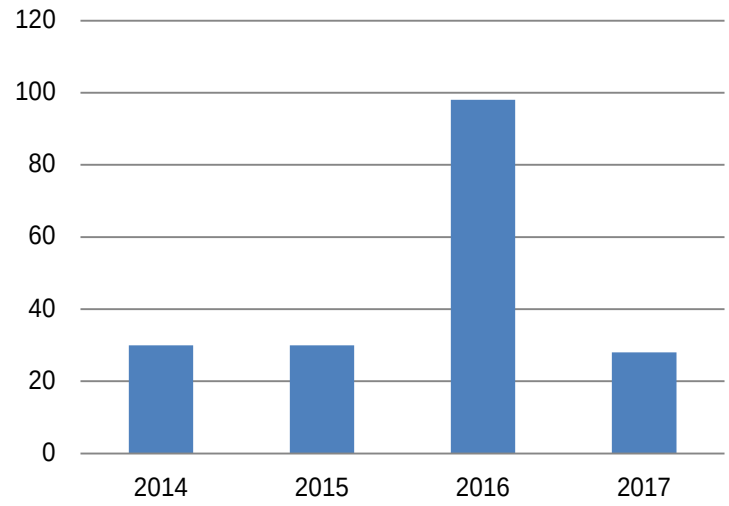
Figuur 15 **Omvang ransomware nam af in afgelopen jaar**



Noot: De gebroken jaren op de horizontale as lopen van april tot en met maart. Bron: Kaspersky, KSN Report: Ransomware and malicious cryptominers 2016-2018 & https://securelist.com/pc-ransomware-in-2014-2016

[68] Zie hier.
[69] Zie bijvoorbeeld deze lijst.
[70] Begin oktober 2018 maakt ook ransomware GrandCrab slachtoffers in Nederland (zie hier).
[71] https://securelist.com/miners-on-the-rise/81706/.
[72] https://www.ft.com/content/d355e206-795d-11e8-8e67-1e1a0846c475.
[73] https://blog.chromium.org/2018/04/protecting-users-from-extension-cryptojacking.html.
[74] Zie dit nieuwsbericht.

Figuur 16 **Aantal nieuwe ransomwarefamilies afgenomen**



Bron: Symantec ISTR Vol.23 & ISTR Ransomeware 2017.

Risico's

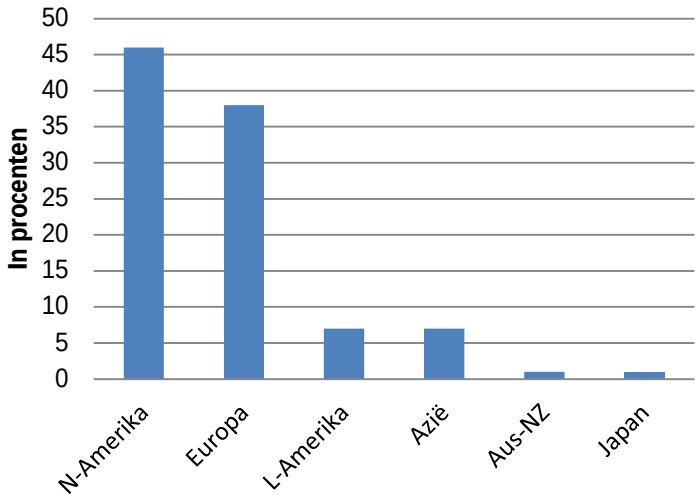
In ontwikkelde landen bestaat het meeste risico op ransomware voor gebruikers. Infecties met ransomware leveren alleen geld op voor criminelen wanneer slachtoffers betalen. Het is dan ook niet verbazingwekkend dat in Noord-Amerika en Europa de meeste slachtoffers zitten (figuur 17). Vanuit maatschappelijk oogpunt is betaling echter ongewenst. Een betaling beloont crimineel gedrag en versterkt het gehanteerde businessmodel. In dit opzicht is het positief dat een recent gelanceerde verzekering[75] tegen cyberschade betalingen van losgeld niet vergoedt.

Procesinnovatie moet slachtoffers verleiden tot betaling. Vanwege koopkrachtverschillen tussen verschillende landen variëren criminelen het losgeld voor slachtoffers (met hulp van de Big-Mac index[76]). Ook bieden criminelen na onderhandelingen soms lagere prijzen aan[77]. Daarnaast worden specifieke bedrijven als doelwit uitgekozen die vermoedelijk bereid zijn veel te betalen. Een webhoster uit Korea betaalde één miljoen dollar na besmet te zijn met specifiek op hen gerichte ransomware[78].

Productinnovaties zorgen voor nieuwe vormen van waardeoverdracht van slachtoffer naar crimineel. In het geval van cryptojacking is deze waardeoverdracht zelfs ongezien**.** Het is immers het gebruik van processorkracht waar de crimineel winst mee maakt. Als dit de werkzaamheden van het slachtoffer niet significant vertraagt, zal deze het misbruik van capaciteit niet doorhebben. Er is dus een groot risico dat het misbruik ongemerkt aanwezig blijft.

[75] https://www.unive.nl/zorgeloosonline/vergoeden.
[76] https://www.recordedfuture.com/fatboy-ransomware-analysis/.
[77] Zie deze berichtgeving.
[78] Zie dit nieuwsbericht.

Figuur 17 **Sterke concentratie van ransomware-aanvallen in Noord-Amerika en Europa**



Bron: 2018 SonicWall Annual Threat. Zie hier. Data gaan over 2017.

Beleidsopties

Treffen van maatregelen om de opsporing en bestrijding te verbeteren, investeringen in internationale samenwerking en snelle verzameling van data. Om financieel gemotiveerde malware tegen te gaan moeten de knelpunten rond de bestrijding van cybercriminaliteit en op de markt voor cyberveiligheid worden aangepakt**.** In de paragrafen over deze knelpunten worden de beleidsopties hiervoor toegelicht.

3.3 DDoS-aanvallen

Kern

- Er zijn veel eenvoudig bereikbare websites – *booters* – die DDoS-aanvallen als goedkope dienst verlenen. Met de groei in slecht beveiligde apparaten, die onderdeel uitmaken van de infrastructuur van booters, worden zulke websites een groter probleem.
- De overheid kan de overlast van DDoS-aanvallen beperken door actieve opsporing en/of ondermijning van het verdienmodel van booters.
- Digitale ontwikkelingshulp kan helpen om de netwerkveiligheid van buitenlandse internetserviceproviders te vergroten en daarmee overlast door DDoS-aanvallen te verminderen.

DDoS-aanvallen verminderen de beschikbaarheid van online diensten en veroorzaken overlast voor de samenleving.[79] Zo zorgden in het afgelopen jaar DDoS-aanvallen voor uitval bij diensten als DigiD, de Belastingdienst en verschillende banken. De samenleving vraagt echter om continue beschikbaarheid, zoals blijkt uit Kamervragen over dit onderwerp[80] en uit de beschikbaarheidseis[81] van 99,9 procent[82] voor iDeal-betalingen. Ook streeft de Belastingdienst voor zijn websites naar een beschikbaarheid van 99,9 procent[83].

DDoS-aanvallen die overlast veroorzaken komen in verschillende soorten en maten voor. Het record voor de sterkste DDoS-aanval is het afgelopen jaar meerdere keren `verbeterd'. De sterkst genoteerde[84] aanval tot dit moment is 1,7 terabit per seconde – dit komt overeen met 340 duizend Netflix HD-videostreams[85]. Hoewel zulke grote getallen tot de verbeelding spreken, zijn kleinere aanvallen frequenter. Er zijn aanwijzingen dat in Nederland de duur en grootte van DDoS-aanvallen afneemt, terwijl de vernuftigheid ervan toeneemt[86]. Deze vernuftigheid zit hem vooral in het snel wisselen tussen – en combineren van – verschillende aanvalstechnieken.

Kleinere aanvallen veroorzaakten overlast bij meerdere Nederlandse banken. Als gevolg van een DDoS-aanval met een geschatte grootte[87] van 'slechts' 50 gigabit per seconde werd bij deze banken het online betalingsverkeer[88] enkele uren verstoord. In dit voorjaar zorgden aanvallen op DigiD en de Belastingdienst ook voor problemen met de belastingaangifte[89].

Opvallend aan de aanval op de banken is dat deze voor slechts 40 euro is ingekocht bij een zogeheten *booter* website[90]**.** Zulke *booters* bieden alledaagse gebruikers de mogelijkheid om voor weinig geld een DDoS-aanval te starten. Hierbij maakt de aanvaller gebruik van een systeem van gehackte apparaten die samen een datastroom afvuren. Vanwege het gebruiksgemak wordt de toegenomen hoeveelheid DDoS-aanvallen in de afgelopen jaren deels toegeschreven aan de opkomst van zulke *booters*[91].

---

[79] Zie kader in paragraaf 3.3 voor een uitleg van verschillende typen DDoS-aanvallen.
[80] Zie bijvoorbeeld hier en hier.
[81] Zie de regeling oversight.
[82] De 99,88 procent is het eindstation van een groeipad dat begon met 99,64 procent in 2016. Voor daluren geldt in 2018 een minimum van 98,5 procent.
[83] Zie hier.
[84] https://www.zdnet.com/article/new-world-record-ddos-attack-hits-1-7tbps-days-after-landmark-github-outage/.
[85] Uitgaande van een HD-stream van vijf megabit per second (zie hier).
[86] NBIP DDOS Data Report 2017 & NBIB DDoS Data Report first semester 2018.
[87] https://www.agconnect.nl/artikel/bestaande-ddos-bescherming-niet-toekomstbestendig.
[88] Zie bijvoorbeeld de NOS berichtgeving.
[89] Zie ook dit nieuwsbericht.
[90] Dit wordt ook wel DDoS-*as-a-service* of *stresser* genoemd.
[91] DDoS-as-a-Service: Investigating Booter Websites, PhD Thesis, Jair Santanna, 2017, Universiteit Twente.

Typen DDoS-aanvallen

DDoS-aanvallen komen in verschillende soorten voor. Hier wordt een onderverdeling gemaakt in twee typen.

Volumeaanvallen

Simpele volumeaanvallen sturen zo veel mogelijk verkeer naar een doelwit met als doel de internetverbinding te verzadigen. Een dergelijke aanval springt eruit (want veroorzaakt een hoge piek in verkeer) en kan daarom in principe goed en snel gedetecteerd en gemitigeerd worden zonder dat de doelserver platgaat.

Applicatieaanvallen

Complexer zijn Application Layer Attacks (ALAs), waarbij niet zozeer de internetverbinding wordt verzadigd, maar juist de achterliggende computersystemen in de war worden gestuurd en uitvallen. Hiervoor is weinig verkeer nodig. Vooral nieuwe en dus onbekende ALAs zijn daardoor lastig te detecteren. Het draait in dit laatste geval dan ook vaker om mitigatie nadat er problemen zijn opgetreden, i.e. het verminderen van de tijd dat een server onbereikbaar is.

Risico's

De toenemende beschikbaarheid van hackbare apparaten vergroot de kans op DDoS-aanvallen. De sterke opkomst van consumentenproducten (bijv. lampen, gordijnen en koelkasten) die verbonden zijn met internet – bekend als `Internet of Things (IoT)' – zorgt voor problemen. Zulke apparaten zijn niet altijd goed beveiligd en daardoor vatbaar voor misbruik. Omdat zowel de consument als fabrikant hier niet direct last van heeft is er geen economische prikkel dit probleem op te lossen. Dit is een typisch falen van de markt dat mogelijk met productregulering voorkomen kan worden. Mede hierom pleiten de Nederlandse regering en het Agentschap Telecom voor betere toegangsbeveiliging en (Europese) certificering van IoT-apparatuur[92,93].

Een betere toegangsbeveiliging en/of certificering lost echter maar een deel van het probleem op: het voorkomt geen versterkingsaanvallen. Bij een versterkingsaanval stuurt een kwaadwillende een verzoek naar een bepaald apparaat (bijvoorbeeld een IoT-product). Het antwoord op dit verzoek bevat (veel) meer data. Deze versterkte datastroom kan vervolgens gebruikt worden in een DDoS-aanval. Het is verontrustend dat zulke aanvallen ook mogelijk zijn zonder dat de kwaadwillende toegang heeft verkregen tot de software van een apparaat[94]. Technische maatregelen door (buitenlandse) netwerkbeheerders om dit soort kwaadwillend verkeer te voorkomen zijn er wel[95] maar worden niet door iedereen gebruikt. Het lijkt erop dat DDoS-aanvallen dus ook in de voorzienbare toekomst nog aanwezig blijven.

[92] Zie Agentschap Telecom.
[93] Regeerakkoord Rutte-III, Vertrouwen in de toekomst.
[94] Hierbij wordt vaak gebruik gemaakt van intrinsieke zwakheden in internetprotocollen.
[95] https://www.manrs.org/manrs/.

Beleidsopties

Probeer het businessmodel van *booters* te ondermijnen. De fysieke opsporing van verdachten is ook mogelijk[96] maar dit is zeer tijdrovend. Het actief identificeren[97] van *booter* websites en vervolgens sluiten kan daarom een alternatief zijn. Ook kan het betalingsverkeer naar *booters* worden afgesneden. Dit is effectief gebleken in het verminderen van DDoS-aanvallen[98].

Om versterkingsaanvallen te voorkomen kan de overheid eisen dat professionele beheerders van apparatuur die wordt gebruikt voor versterkingsaanvallen, beschermingsmaatregelen nemen. Een voorbeeld zijn de versterkingsaanvallen via professionele *memcached* servers[99]. De mogelijkheid tot misbruik van zulke systemen is eenvoudig te detecteren en kan eenvoudig worden verholpen. Het feit dat versterkingsaanvallen ondanks beschikbare oplossingen nog steeds voorkomen, laat zien dat organisaties niet altijd de juiste prikkel hebben om zelf oplossingen te implementeren. Deze optie vraagt ook om internationale samenwerking, aangezien de servers vaak over de grens zitten.

Nederland zou digitale ontwikkelingshulp kunnen geven aan buitenlandse internet-serviceproviders. Veel van deze providers hebben weinig economische prikkels om *good practices*[100] te implementeren die veel versterkingsaanvallen kunnen verhinderen. Het gaat hierbij vooral om maatregelen die *spoofing* voorkomen. Het recent door Nederland gestarte *Global Forum on Cyber Expertise* is een omgeving om zulke maatregelen te bespreken.

3.4 De markt voor DDoS-mitigatie

Kern

- De markt voor DDoS-mitigatiediensten (diensten die de impact van een aanval beperken) draait om het verkrijgen van data en het optimaliseren van algoritmes.
- Het delen van DDoS-aanvalsdata is van belang voor het beschermen van competitie en leidt vermoedelijk tot betere mitigatie.
- Stimuleren van een Nederlandse coöperatie gericht op DDoS-mitigatie is vanuit geopolitiek oogpunt interessant: het zorgt voor Nederlandse kennis en voorkomt het ongewild weglekken van data naar het buitenland.

[96] Dit NOS bericht is hier een voorbeeld van.
[97] Historisch zijn er meer dan vijfhonderd bekend. Zie deze lijst, bezocht op 28 juni 2018.
[98] M. Karami *et al,.* Stress Testing the Booters: Understanding and Undermining the Business of DDoS Services, ACM 2016, doi: 10.1145/2872427.2883004.
[99] *Memcached* servers worden gebruikt om websites sneller te maken door tijdelijk externe data op te slaan. Zie hier.
[100] Zie https://www.manrs.org/manrs/.

Organisaties kunnen zelf DDoS-aanvallen mitigeren of dit (deels) uitbesteden aan een derde partij. Deze derden zijn zowel commerciële *cloud-based* partijen (bv. Akamai), non-profit instellingen (bv. NaWas) of internet-serviceproviders (bv. KPN). Het gebruik van permanente bescherming (door *cloud-based* dienstverleners) in Nederland is relatief toegenomen (figuur 18).[101] Gecombineerd met de absolute aantallen komt dit overeen met een toename van permanent anti-DDoS-gebruik onder .nl-domeinnamen van 1,6 procent naar 1,9 procent[102].

Detectie is noodzakelijk om een DDoS-aanval te kunnen mitigeren. Detectie van volumeaanvallen (zie kader in paragraaf 3.3) is relatief eenvoudig. Zulke aanvallen gaan namelijk gepaard met ongebruikelijk hoge pieken in het dataverkeer. Voor *Application Layer Attacks* (ALAs) ligt dit ingewikkelder. Bij een dergelijke aanval is het voornamelijk de inhoud van de data – en niet de hoeveelheid – die voor overlast zorgt. Daardoor is het van de buitenkant minder eenvoudig om te zien dat er iets mis gaat. Detectie van nog onbekende typen ALAs is daarom lastiger en de kans op uitval aannemelijker.

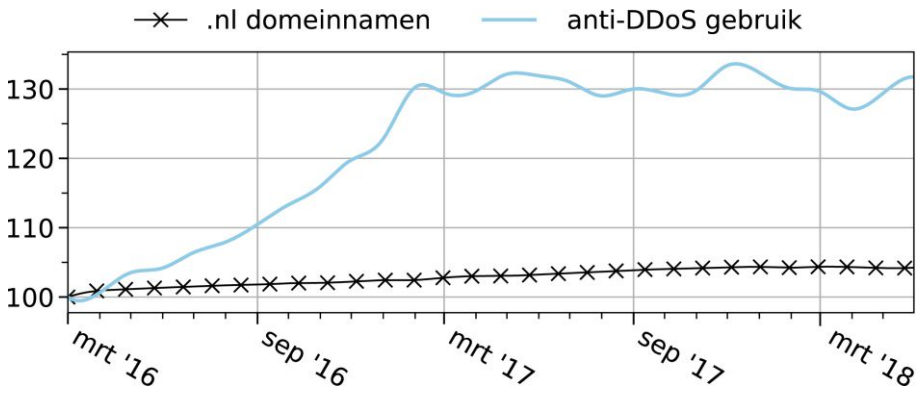
Naast een goed detectiemechanisme draait mitigatie van elk soort DDoS-aanval om het scheiden van goed en slecht verkeer. Het scheiden gebeurt door de mix aan dataverkeer te inspecteren en schoon te wassen. Dit doet het slachtoffer zelf en/of gebeurt door een derde partij[103]. Belangrijk om op te merken is dat controle door een derde partij impliceert dat de datastroom wordt omgeleid naar de systemen van die (externe) partij. De opgeschoonde data worden vervolgens teruggestuurd naar het oorspronkelijke doeladres.

Inzage in dataverkeer is nodig om goed en fout verkeer tijdens een Application Layer Attack (ALA) zoveel mogelijk te scheiden. Bij versleuteld dataverkeer – zoals betalingsopdrachten – is in het dataverkeer kijken alleen mogelijk indien diegene die de mitigatie uitvoert, decryptiesleutels bezit. Bij mitigatie door derden worden decryptiesleutels afgestaan. Er vindt dus een afweging plaats tussen betere bescherming en de vertrouwelijkheid/het delen van gegevens van klanten. Dit is onder voorwaarden, opgesteld door De Nederlandsche Bank in de regeling outsourcing, toegestaan. Daarnaast moet vanwege inzicht in persoonsgegevens in het kader van de AVG ook een bewerkersovereenkomst worden gesloten.

[101] M. Jonker *et al.*, *Measuring the Adoption of DDoS Protection Services*, IMC 2016, November 14- 16, 2016, doi: 10.1145/2987443.2987487.
[102] Dit gaat om permanente bescherming door negen grote dienstverleners en geeft dus geen volledig beeld van het anti-DDoS gebruik in Nederland. Er vindt ook niet-permanente bescherming plaats. Ook bieden de NaWas en internet service providers zoals KPN beschermingsdiensten aan die niet in deze cijfers zijn meegenomen.
[103] De detectie van DDoS-aanvallen kan ook uitbesteed worden. Dit vereist wel dat verkeer ook langs de derde partij gaat wanneer er geen aanval plaatsvindt.

Zowel het detecteren als het opschoonproces gebeurt met algoritmes die beter worden naarmate meer training plaatsvindt. Het proces van DDoS-mitigatie is dus vergelijkbaar met andere markten waarin data en slimme algoritmes een rol spelen: hoe meer (aanvals-)data een partij weet te verzamelen, hoe beter deze in staat is om goed te mitigeren en hoe beter het product is dat men kan aanbieden. Dergelijke bedrijfsmodellen zijn tegenwoordig veel te vinden bij techbedrijven en hebben als bijeffect dat er (grote) kans is op monopolievorming: de koploper wordt steeds dominanter als gevolg van een grotere toegang tot data om algoritmes mee te trainen en te verfijnen.

Figuur 18 **Anti-DDoS-gebruik relatief gegroeid (geïndexeerd, maart 2016 = 100)**



Bron: Mattijs Jonker, Universiteit Twente.

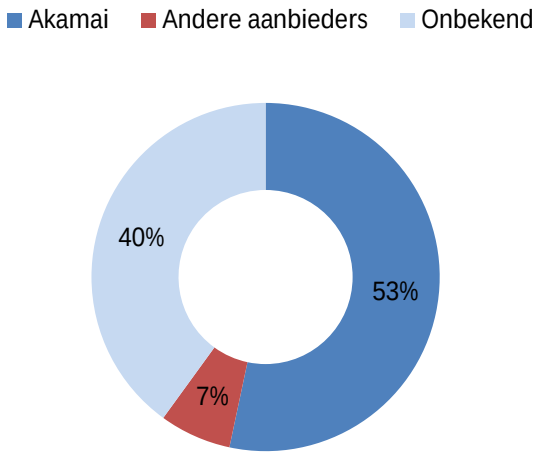
I. Risico's voor de werking van de markt voor DDoS-mitigatie

Marktmacht kan ervoor zorgen dat de markt voor DDoS-mitigatie suboptimaal werkt. Op het eerste gezicht lijkt de markt voor DDoS-mitigatie goed te functioneren: er zijn keuzemogelijkheden. Het aanbod behelst meerdere aanbieders van *cloud-based* beschermingsdiensten, internet service providers bieden mitigatiediensten aan en men kan zich aansluiten bij de NaWas – dat een corporatiemodel hanteert. Dat de markt op grote lijnen functioneert, blijkt ook uit het feit dat – ondanks de bijna dagelijkse aanvallen op vitale processen – er relatief weinig DDoS-aanvallen zijn die tot grote uitval leiden.

Een steekproef onder internationale banken (figuur 19) doet vermoeden dat één partij sterk dominant is. Zolang er lage toetredingsbarrières bestaan, hoeft zulke marktdominantie vanuit puur economisch perspectief echter niet nadelig te zijn. De dreiging om van de troon gestoten te worden blijft immers aanwezig. Dit dwingt de bovenliggende partij tot innoveren en dus tot betere dienstverlening. Vanuit maatschappelijk perspectief kun je wèl de vraag stellen of grote marktconcentratie in dit specifieke geval gewenst is. Immers, valt in dit geval Akamai om (door bijvoorbeeld een grote DDoS-aanval), dan heeft dit potentieel een keteneffect. Dit hoeft zich niet te beperken tot uitval in de bankensector alleen.

Belangrijk is dat in een markt die gekenmerkt wordt door toegang tot data, de toetredingsbarrière hoog is. Nieuwkomers hebben mogelijk onvoldoende toegang tot data om hun algoritmes te optimaliseren. Dit kan weer de prikkel ondergraven voor gevestigde partijen om verder te innoveren. Op deze markt is het daarom de vraag voor het mededingingstoezicht of grote aanbieders een economische machtspositie hebben en of zij deze misbruiken.

Figuur 19 Akamai groot als primaire DDoS-beschermingsdienst onder banken



Noot: Deze data is verkregen via de spiceworks traceroute tool en laat de primaire DDoS-beschermingsdienst zien. Daarnaast maken banken in noodgevallen ook gebruik van andere (secundaire) diensten. We onderzochten de dertig belangrijkste banken wereldwijd – geïdentificeerd door de Financial Stability Board – zoals hier is gepubliceerd.

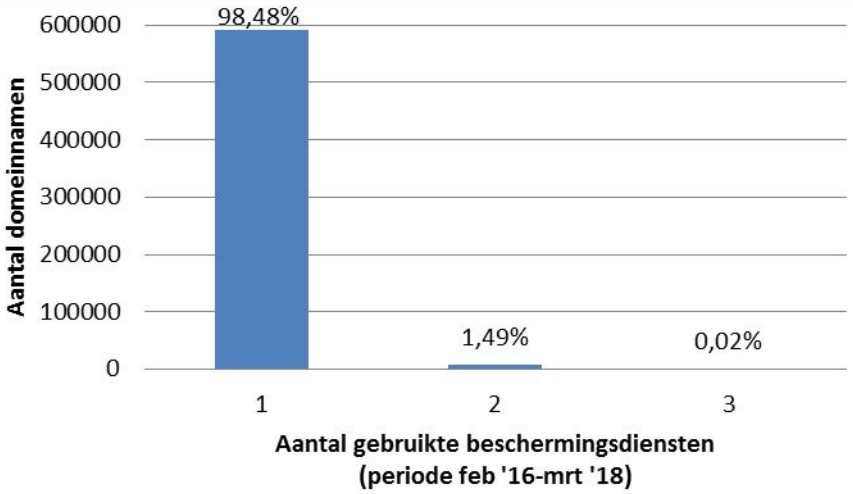
De toegankelijkheid voor nieuwkomers kan verbeterd worden door relevante aanvalsdata van DDoS-aanvallen zo snel mogelijk te delen. Om transparantie en toegankelijkheid te waarborgen ligt een platform dat bepaalde datastandaarden hanteert, voor de hand. Belangrijke data zijn zo voor iedereen beschikbaar en te gebruiken. Recent gestarte initiatieven op dit gebied, zoals het nauwkeurig kenmerken *(fingerprinting)* van aanvallen via booterwebsites, zouden dan ook ondersteund moeten worden[104].

Ook transactiekosten kunnen goede marktwerking in de weg staan. Een manier om te bepalen of transactiekosten een beperking vormen is door te kijken naar het aantal overstappers. Figuur 20 laat zien dat de meeste websites die – in een twee jaar durende meting – een DDoS-aanval te verduren hebben gehad tijdens die periode, vaak maar één beschermingsdienst hebben gebruikt. Dit kan komen doordat er één of enkele aanbieders zijn die goede service leveren. Daarentegen is het ook mogelijk dat de transactiekosten om over te stappen hoog zijn en/of dat (de afwezigheid van) vertrouwen een grote rol speelt. De rol van vertrouwen is zeker belangrijk wanneer

[104] Zie DDoS-as-a-Service: Investigating Booter Websites, PhD Thesis, Jair Santanna, 2017, Universiteit Twente

men voor het afslaan van ALAs decryptiesleutels moet delen met een nieuwe derde partij. Transactiekosten zijn in een dergelijk geval zeer waarschijnlijk.

Figuur 20 Anti-DDoS-gebruikers stappen weinig over



Bron: Mattijs Jonker, Universiteit Twente.
Noot: De data bevatten .nl-domeinnamen die ergens in de onderzochte twee jaar zijn belaagd door een DDoS-aanval *en* tijdens minimaal één dagelijkse momentopname gebruik hebben gemaakt van een van de negen geanalyseerde dienstverleners[105].

II. Optimale marktordening voor mitigatiediensten

Naast een concurrentiemodel, op basis van prijs en product, zijn er ook andere organisatievormen mogelijk. Een alternatief is bijvoorbeeld een coöperatie (zonder winstoogmerk) waar sommige experts voorstander van zijn[106]. Een coöperatie kan in sommige gevallen geschikt zijn om in een bepaald product of bepaalde dienst te voorzien, namelijk wanneer de belangen van de deelnemers met elkaar overeenstemmen[107]. In het geval van DDoS-mitigatie lijkt aan deze voorwaarde voldaan. Alle deelnemers streven immers naar optimale DDoS-mitigatie.

[105] Het gaat hierbij niet noodzakelijk om permanente bescherming – tijdelijke bescherming is ook meegenomen. Zie ook:
M. Jonker *et al.* 'Millions of Targets Under Attack: a Macroscopic Characterization of the DoS Ecosystem', in Proceedings of the 2017 ACM Internet Measurement Conference, 2017.
[106] https://www.agconnect.nl/artikel/bestaande-ddos-bescherming-niet-toekomstbestendig.
[107] In *Economics for the common good*, p 180 (Jean Tirole) worden bijvoorbeeld Visa en Mastercard genoemd.

Dutch Continuity Board als antwoord op grote DDoS-aanvallen

Hoe te anticiperen op (doem-)scenario's waarin Nederlandse vitale processen verstoord worden door grootschalige DDoS-aanvallen, en de standaardbeschermingsmethodes niet meer voldoen? In een dergelijk geval is het noodzakelijk om te kunnen terugvallen op werkende verbindingen die kernfuncties bereikbaar houden. Een mogelijkheid om dit te realiseren is door het instellen van een lokaal netwerk dat tijdens een disruptieve aanval tijdelijk is afgesloten van andere (niet vertrouwde) netwerken. Vanwege de intrinsieke openheid van het internet ligt de crux in welke netwerken je in zo' n geval wel of niet toelaat – en welke gevolgen dit heeft voor de betrokken vitale processen. Het vereist namelijk dat de vitale processen uiteraard ook onderdeel zijn van dit vertrouwde netwerk

In Nederland zijn de netwerkbeheerders die in noodsituaties een dergelijk lokaal netwerk nastreven verenigd in de Dutch Continuity Board. Zij stellen voor om tijdens noodsituaties de afsluiting van externe netwerken stapsgewijs te doen. Dit is te vergelijken met het afpellen van een ui: je begint met het afstoten van de buitenste netwerken totdat je alleen die netwerken overhoudt die geen overlast veroorzaken. Gezien het nationale belang is het verstandig dat de overheid actief betrokken is bij de ontwikkeling van de protocollen die tijdens zulke digitale calamiteiten een rol spelen.

In Nederland zijn er twee coöperaties, de NaWas en DCB, actief die DDoS-aanvallen mitigeren. De NaWas[108] is een DDoS-beschermingsdienst van de Nationale Beheersorganisatie Internet Providers met als doel tegenwicht te bieden aan commerciële partijen. De Dutch Continuity Board[109] (DCB, zie kader op vorige pagina) is een samenwerkingsverband van Internet Service Providers. De leden van de DCB willen ervoor zorgen dat telecommunicatiediensten beschikbaar blijven voor zowel vitale processen als voor hun afnemers – ook ten tijde van grootschalige cyberaanvallen.

Vanuit puur economisch perspectief is het lastig hard te maken dat de overheid moet sturen op een coöperatie. Een argument vóór zou kunnen zijn dat vanwege het gebrek aan winstoogmerk een coöperatie de kosten voor DDoS-mitigatie omlaag brengt. Dit kan ervoor zorgen dat goede mitigatie voor iedereen betaalbaar wordt – ook voor bijvoorbeeld beginnende techbedrijven met weinig financiële middelen. Dit verhoogt de toegankelijkheid van de markt. Van goede mitigatie voor iedereen profiteert de samenleving als geheel. Een tegenargument is dat ditzelfde doel wellicht te bereiken valt door het bevorderen van competitie tussen commerciële aanbieders via het eerder bediscussieerde vrijgeven van aanvalsdata.

Door de afhankelijkheid van buitenlandse (lees: Amerikaanse) aanbieders ontstaan er risico's voor de informatieveiligheid van Nederlandse gebruikers. Vanuit dit meer geopolitieke oogpunt zijn er daarom wel argumenten voor stimulering van een nationale (of Europese) coöperatie. Ten eerste zorgt het gebruik van een 'nationale wasstraat' ervoor dat belangrijke kennis over cyberveiligheid binnen de eigen invloedssfeer blijft. Ten tweede voorkomt een nationaal systeem dat vitale datastromen (wellicht ongewild of gedwongen door buitenlandse wetgeving) via een derde partij in handen komen van een buitenlandse statelijke actor.

[108] Voor meer informatie zie https://www.nbip.nl/nawas/.
[109] https://www.dcboard.nl/about-us.

De Amerikaanse CLOUD Act verhoogt het risico op het ongewild weglekken van gevoelige data. Deze wet verplicht Amerikaanse bedrijven om data die zijn opgeslagen in het buitenland, op verzoek met de Amerikaanse autoriteiten te delen. Op dit moment is het nog onduidelijk hoe dit met de recent in werking getreden AVG valt te rijmen[110].

Beleidsopties

Om succesvolle DDoS-aanvallen te voorkomen kan de overheid de toegankelijkheid van – en de competitie in – de markt voor DDoS-mitigatiediensten bevorderen, bijvoorbeeld door deling van DDoS-aanvalsdata te verplichten. Deze overweging is onderdeel van de bredere discussie over het delen van data binnen de digitale economie en moet wellicht breder en op Europees niveau gevoerd worden. In verband met vertrouwelijkheid en misbruik van zulke data is een goede toegangscontrole van belang.

Het stimuleren van binnenlandse of Europese samenwerkingsverbanden is een goede manier om de beschikking te houden over essentiële cyberveiligheidskennis en te zorgen voor informatiebeveiliging. Zeker gezien de sterke afhankelijkheid van Amerikaanse aanbieders en de invloed van de Amerikaanse overheid op het verkrijgen van Nederlandse data via de CLOUD Act. De Rijksoverheid zou in dit opzicht een voortrekkersrol kunnen spelen door DDoS-aanvallen waar mogelijk te laten mitigeren bij de NaWas.

3.5 Social engineering

Kern

- Cybercriminelen gebruiken steeds geraffineerdere technieken om mensen te verleiden persoonsgegevens prijs te geven, malware te installeren, of geld over te maken.
- Het blijft daardoor voor gebruikers lastig om ‘nep’ van ‘echt’ te onderscheiden.
- Het gebruik van technische standaarden om e-mail en websites veiliger te maken neemt toe, maar kan nog vergroot worden.

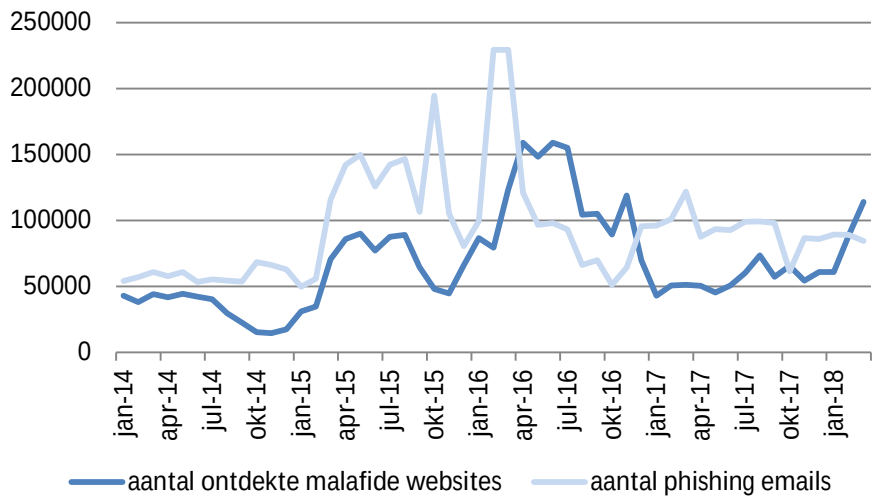
Social engineering is een verzamelterm voor alle aanvallen waarbij de gebruiker wordt gemanipuleerd om informatie te geven of andere voor hem- of haarzelf nadelige acties te ondernemen. Voorbeelden hiervan zijn phishingmails die hengelen naar persoonsgegevens of een link sturen die leidt naar een malafide website, mails die de lezer verleiden een bijlage te openen die malware bevat en mails met nepfacturen. Niet alleen e-mail wordt hiervoor gebruikt, social engineering gebeurt ook onder andere via WhatsApp, SMS, sociale media en valse apps.[111]

[110] Zie bijvoorbeeld deze analyse.
[111] Zie bv. de nieuwsberichten hier, hier, hier en hier.

Bij social engineering maken criminelen misbruik van het feit dat mensen vaak op de automatische piloot snelle beslissingen nemen.[112] Wanneer een mail ogenschijnlijk van een autoriteit afkomstig is (zoals een directeur of een bank) zijn mensen meer geneigd daarop in te gaan. Ook deadlines ('binnen drie dagen verloopt je wachtwoord, klik hier om te resetten') activeren automatische denkpatronen. Weer andere vormen van social engineering (bv. iemand die zich voordoet als familielid in geldnood) doen een beroep op de menselijke neiging bekenden in nood te helpen.

Het aantal phishingmails en malafide websites wereldwijd fluctueert sterk (figuur 21). De maandelijkse aantallen in 2017-2018 lijken wat gedaald ten opzichte van de eerste helft van 2016, maar het is moeilijk een algemene trend te onderscheiden. Financiële instellingen en betaalsystemen zoals Paypal zijn een geliefd doelwit; in het eerste kwartaal van 2018 relateerde 53,6 procent van de phishingmail en malafide websites hieraan.[113]

Figuur 21 Ontwikkeling aantal ontdekte malafide websites en phishingmails wereldwijd

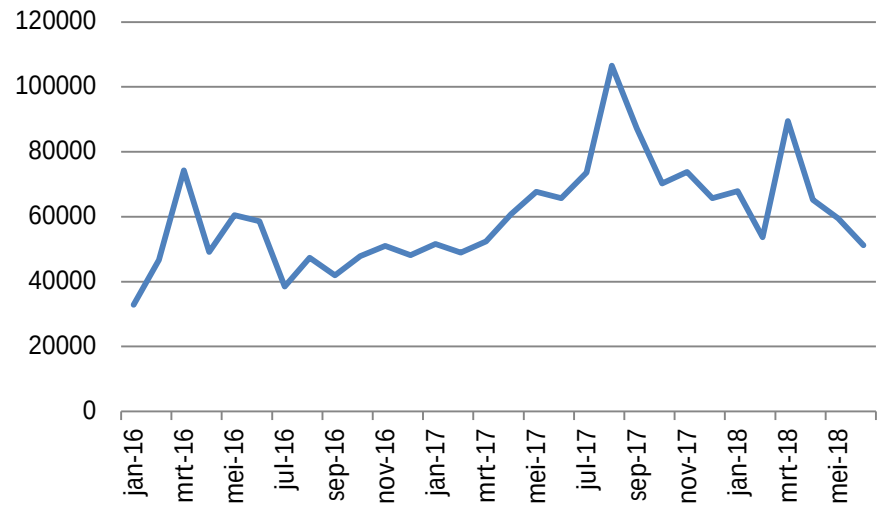


Bron: Anti Phishing Working Group phishing attack trends reports, link.

De Nederlandse Fraudehelpdesk heeft het afgelopen jaar meer meldingen gekregen van valse e-mails (figuur 22). Valse e-mails betreffen zowel phishingmails, als mails die malware verspreiden, mails met valse facturen en andere frauduleuze mails. Hoewel het aantal gemelde e-mails fluctueert over de tijd, is er een stijgende lijn te zien. De toename kan zowel duiden op een toename van activiteit van criminelen, als op een toegenomen bekendheid van het meldpunt.

[112] Zie bv. het boek *Thinking fast and slow* van D. Kahneman of *Infuence* van R. Cialdini.
[113] Zie het Phishing attack trends report Q1 2018 van APWG, te downloaden via https://www.antiphishing.org/resources/apwg-reports/.

Figuur 22 Ontwikkeling aantal gemelde valse e-mails in Nederland



Bron: Fraudehelpdesk.

Gegevens van het CBS laten zien dat in 2017 0,3 procent van de bevolking slachtoffer is geworden van phishing. Dit is gelijk aan 2016, maar een daling ten opzichte van 2012-2015.[114] Voor sommige specifieke vormen van social engineering wordt in 2017 wel meer schade gemeld dan in 2016. Zo rapporteren de Betaalvereniging en Nederlandse Vereniging van Banken dat de schade veroorzaakt door fraude met internetbankieren met bijna 400.000 euro is gestegen tot 1,2 miljoen euro.[115] Het grootste deel van deze schade wordt veroorzaakt door phishing[116]; de schade hiervan was ruim een miljoen in 2017 tegenover 700.000 euro in 2016. Overigens is in historisch perspectief de schade in 2017 nog altijd relatief laag.

Risico's

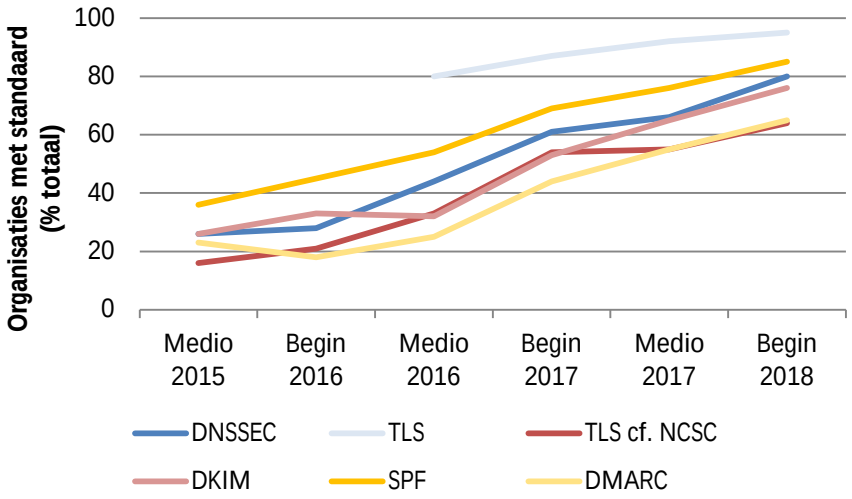
Er is een continue wapenwedloop gaande tussen cybercriminelen enerzijds en bonafide organisaties anderzijds. Cybercriminelen gaan steeds geraffineerder te werk.[117] Eind 2016 gebruikte nog geen 5 procent van de malafide websites het HTTPs protocol, in het eerste kwartaal van 2018 is dat gestegen tot 33 procent.[118] Hoewel HTTPs alleen duidt op een veilige verbinding tussen de browser van de gebruiker en de ontvangende website, lijken veel consumenten HTTPs te interpreteren als signaal voor een veilige website waar een betrouwbare partij achter zit.[119] Het gebruik van HTTPs door cybercriminelen kan een vals gevoel van veiligheid geven en gebruikers verleiden om hun persoonlijke gegevens prijs te geven. Cybercriminelen gebruiken

[114] Bron: CBS Statline.
[115] Bron: dit nieuwsbericht en toelichting door Betaalvereniging Nederland.
[116] Het gaat hier om phishing naar inlogcodes. Phishing naar betaalpassen, waarbij het slachtoffer de pas opstuurt naar een crimineel, valt niet onder internetbankieren.
[117] Hier een recent voorbeeld van een geavanceerde phishing aanval op DigiD met 200 slachtoffers.
[118] APWG Phishing activity trends report Q1 2018.
[119] Zie bijvoorbeeld dit bericht, of een onderzoek van de NOS.

ook steeds vaker andere kanalen dan e-mail, zoals SMS en Whatsapp, of platformen zoals Marktplaats.[120] Opvallend is een sterke toename van fraude via Whatsapp. Hierbij doet een crimineel zich op Whatsapp voor als een familielid of vriend van het slachtoffer en vraagt dringend om geld over te maken. Werden in 2015 t/m 2017 in totaal 60 gevallen gemeld bij de Fraudehelpdesk, in de eerste helft van 2018 zijn er al 180 meldingen gedaan.[121]

Het gebruik van beveiligingsstandaarden om valse e-mails en malafide websites te voorkomen is onder overheidsorganisaties verder gestegen (figuur 23).[122] Het doel om vóór eind 2017 een implementatiegraad van 100 procent te halen is echter niet bereikt. In oktober 2017 bleek dat onbevoegden e-mail konden versturen via de mailserver van de Tweede Kamer omdat het SPF-protocol niet was ingeschakeld.[123] Ook in het algemeen worden beveiligingsstandaarden steeds meer toegepast, maar is volledige implementatie nog niet bereikt. In juni 2018 was 52 procent van de .nl-domeinnamen DNSSEC ondertekend.[124] Wat betreft DNSSEC-validatie bij de eindgebruiker doet Nederland het minder goed. In augustus 2018 gebruikte ruim 28 procent van het internetverkeer DNSSEC-validatie. Dat is iets meer dan het gemiddelde van heel Europa (24 procent) maar wel beduidend minder dan onder andere Noorwegen en Zweden, die beide boven de 80 procent scoren.[125]

Figuur 23 Adoptiegraad technische standaarden overheidsorganisaties



Bron: Stichting Internet Domein Registratie Nederland en Forum Standaardisatie.

[120] Zie bv. hier en hier.
[121] Zie ook dit bericht.
[122] DKIM, SPF en DMARC gaan phishing e-mails, spam en malware e-mails tegen. DNSSEC voorkomt dat verkeer wordt omgeleid naar een malafide website.
[123] Zie dit nieuwsbericht.
[124] Bron: SIDN statistieken, https://stats.sidnlabs.nl/nl/.
[125] Zie deze website, bezocht op 29-08-2018.

Het blijft voor gebruikers lastig om in alle situaties onderscheid te maken tussen bonafide en valse berichten en websites. Naast de directe schade van geslaagde cybercriminaliteit kan er ook indirecte schade optreden als gebruikers wantrouwend worden ten opzichte van legitieme websites en daardoor geen transacties via internet durven doen. Organisaties als de Belastingdienst en banken maken extra kosten om betrouwbare communicatie mogelijk te maken, onder andere door het opzetten van beveiligde berichtenboxen.

Beleidsopties

Treffen van maatregelen om de opsporing en bestrijding te verbeteren, investeringen in internationale samenwerking en snelle verzameling van data. Om social engineering tegen te gaan moeten, net als bij financieel gemotiveerde malware, de knelpunten rond de bestrijding van cybercriminaliteit en op de markt voor cyberveiligheid worden aangepakt**.** In de paragrafen over deze knelpunten worden de beleidsopties hiervoor toegelicht.

Dit is een uitgave van:

Centraal Planbureau
Bezuidenhoutseweg 30
Postbus 80510 | 2508 GM Den Haag
T (088) 984 60 00

info@cpb.nl | www.cpb.nl

Oktober 2018