Rathenau Instituut

Een nooit gelopen race

Over cyberdreigingen en versterking van weerbaarheid

Rapport

Een nooit gelopen race

Over cyberdreigingen en versterking van weerbaarheid

Geert Munnichs, Matthijs Kouw & Linda Kool

Een nooit gelopen race
Over cyberdreigingen en versterking van weerbaarheid

Geert Munnichs, Matthijs Kouw & Linda Kool

Rathenau Instituut
Anna van Saksenlaan 51
Postadres: Postbus 95366
2509 CJ Den Haag
Telefoon: 070-342 15 42
E-mail: info@rathenau.nl
Website: www.rathenau.nl
Uitgever: Rathenau Instituut

Redactie: Redactie Dynamiek

Bij voorkeur citeren als:
Geert Munnichs, Matthijs Kouw & Linda Kool, *Een nooit gelopen race - Over cyberdreigingen en versterking van weerbaarheid*. Den Haag, Rathenau Instituut 2017

Het Rathenau Instituut heeft een Open Access beleid. Rapporten, achtergrondstudies, wetenschappelijke artikelen, software worden vrij beschikbaar gepubliceerd. Onderzoeksgegevens komen beschikbaar met inachtneming van wettelijke bepalingen en ethische normen voor onderzoek over rechten van derden, privacy, en auteursrecht.

Voorwoord

De studie *Een nooit gelopen race – Over cyberdreigingen en versterking van weerbaarheid* maakt duidelijk dat Nederland, als een van de meest ICT-intensieve economieën ter wereld, een aantrekkelijk doelwit is voor cybercriminelen, cyberspionnen en andere hackers.

De titel van de studie, *Een nooit gelopen race,* wijst op de continue wedloop tussen aanvaller en doelwit. We zullen in die wedloop verwikkeld blijven. De race zal nooit gelopen zijn.

Moeten we dan maar helemaal stoppen met de race? Nee, natuurlijk niet. We kunnen onze weerbaarheid tegen cybercriminaliteit versterken. Het rapport doet daarvoor aanbevelingen. Zo moet er een onafhankelijk kennis- en adviescentrum voor mkb-bedrijven komen. Daarnaast moeten vitale sectoren, bijvoorbeeld die op het gebied van energie, telecom en financiën, afspraken maken over een jaarlijkse hacktest. Bovendien moet er gekeken worden of de huidige toezichthouders zoals de Autoriteit Consument en Markt en het Agentschap Telecom binnen hun huidige mandaat kunnen optreden tegen onveilige producten. Tot slot zou de overheid, die in Nederland circa 30 procent van de beveiligingsproducten en beveilingsdiensten afneemt, nadrukkelijker een voorbeeldrol kunnen vervullen als '*launching customer'*.

Het Rathenau Instituut deed dit onderzoek op verzoek van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) en de Algemene Inlichtingen- en Veiligheidsdienst (AIVD). Het instituut verrichtte een literatuurstudie, interviewde meer dan 25 deskundigen en stakeholders en hield twee workshops.

In 2016 heeft de Tweede Kamer wetten aangenomen die de bevoegdheden voor opsporingsdiensten en inlichtingendiensten verruimen. Bij deze wetten is de bescherming van de rechtspositie van de burger een belangrijk aandachtspunt. We moeten als samenleving in de gaten houden of de ingebouwde '*checks and balances*' afdoende zijn en of onze publieke waarden en mensenrechten voldoende zijn beschermd.

Nederland bevindt zich in een mooie positie. Ons land loopt in de ICT-ontwikkeling op veel terreinen voor. Dat kan alleen zo blijven als gebruikers, bedrijven en overheid alerter worden. Daarbij geldt wat mij betreft dat cybersecurity niet alleen gaat over veiligheid. Het gaat ook om onze gezondheid, om onze autonomie, om gelijke behandeling en om eerlijke informatie. Kortom, het gaat om de samenleving die we met hulp van digitale technologie met elkaar willen vormgeven.

Dr. ir. Melanie Peters
Directeur Rathenau Instituut

Inhoudsopgave

1 Inleiding

1.1 Groeiende afhankelijkheid van ICT

De Nederlandse samenleving digitaliseert in hoog tempo. Ook hoort Nederland tot een van de meest gedigitaliseerde landen ter wereld. Bijna iedereen heeft een computer en meer dan 90 procent van alle huishoudens en bedrijven maakt gebruik van het internet. Digitalisering dringt nagenoeg door tot elk aspect van het leven. Voorbeelden hiervan zijn het toenemend gebruik van internetbankieren, webwinkels, *wearables*, streamingdiensten als Spotify of Netflix of de opkomst van *smart homes* en zelfrijdende auto's.

Daarnaast is de Amsterdam Internet Exchange (AMS-IX) het grootste het internetknooppunt ter wereld en beschikt Nederland over snelle breedband telecomnetwerken. ICT-bedrijvigheid levert een substantiële bijdrage aan de Nederlandse economie. Volgens cijfers van Dialogic droeg ICT in de periode 1990–2013 voor circa 36 procent bij aan de groei ervan (Dialogic 2014).

Nederland is ook een belangrijke vestigingsplaats voor ICT-gerelateerde bedrijvigheid. Volgens Verhagen kan de digitale infrastructuur worden gezien als de derde mainport van het land, naast Schiphol en de Rotterdamse haven (Verhagen 2016).

De Nederlandse samenleving en economie worden daarom steeds afhankelijker van een goed functionerende ICT-infrastructuur en -dienstverlening. De verwachting is dat digitalisering steeds meer analoge producten en processen zal verdringen. Het door de Belastingdienst aangekondigde afscheid van 'de blauwe envelop' die plaats moet maken voor de online belastingaangifte is hiervan een voorbeeld. Door de opkomst van het Internet of Things worden steeds meer apparaten aan het internet gekoppeld. En de opkomst van het 5G-netwerk maakt het mogelijk om nog grotere hoeveelheden data in nog kortere tijd te versturen.

1.2 Nieuwe kwetsbaarheden

Het toegenomen belang van ICT heeft als keerzijde dat uitval ervan direct gevolgen heeft voor maatschappelijke en bedrijfsprocessen. Het wijdverbreide gebruik van pinbetalingen en internetbankieren brengt met zich mee dat als het online betalingsverkeer enkele uren platligt, een groot deel van de Nederlandse economie daar hinder van ondervindt. En naarmate de digitalisering van allerlei processen voortschrijdt, worden ze een aantrekkelijker doelwit voor cybercriminelen, cyberspionnen en andere hackers. Virussen, phishing mails en DDoS-aanvallen bedreigen de cyberveiligheid van burger, overheid en bedrijfsleven. ICT vergemakkelijkt niet alleen in veel opzichten het dagelijkse leven van de Nederlandse burger, ambtenaar en ondernemer, maar ook dat van kwaadwillende partijen.

Recente hacks tonen deze kwetsbaarheid die gepaard gaat met de groeiende afhankelijkheid van ICT. Zo demonstreerde de cybersecurity-deskundige Mary-Jo de Leeuw voor een verbouwereerd

gezelschap van hoge militairen hoe gemakkelijk de met het internet verbonden, pratende speelgoedpop Cayla valt te hacken door de pop doodswensen uit te laten slaan (Het Financieele Dagblad 2016). Een hack kan ook grote maatschappelijke gevolgen hebben. Dat blijkt uit het laten lekken van intern e-mailverkeer binnen de Amerikaanse Democratische Partij, wat door de Amerikaanse veiligheidsdiensten werd toegeschreven aan Russische hackers, met als oogmerk beïnvloeding van de uitslag van de presidentsverkiezingen. En de aanval in 2016 op de Amerikaanse inlichtingen- en veiligheidsdienst National Security Agency (NSA), waarbij digitale spionagewapens werden ontvreemd, laat zien dat geen enkele partij aan deze kwetsbaarheid lijkt te kunnen ontsnappen (Nakashima 2016).

1.3 Onderzoeksvragen

Bovenstaande voorbeelden roepen de vraag op hoe het gesteld is met het vermogen van de Nederlandse samenleving om dit soort nieuwe bedreigingen, die samenhangen met de digitalisering van de samenleving, het hoofd te bieden. Tegen deze achtergrond hebben de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) en de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) het Rathenau Instituut gevraagd om onderzoek te doen. De belangrijkste vragen daarbij luiden: Welke ontwikkelingen in cyberdreigingen kunnen voor de komende jaren – tot 2020 – worden beschreven? Hoe staat het met de weerbaarheid van de Nederlandse samenleving hiertegen? Behoeft deze weerbaarheid versterking, en zo ja, welke maatregelen moeten hiervoor worden genomen?

Daarbij komen ook andere vragen aan de orde. Welke kansen biedt cybersecurity voor de Nederlandse economie? Kunnen op basis van bestaand cijfermateriaal trends worden waargenomen in de geschetste ontwikkelingen? Welke positie neemt Nederland in ten opzichte van andere landen als het gaat om cybersecurity? Waarin onderscheidt Nederland zich, en waarin niet?

De aanbevelingen die uit dit onderzoek voortvloeien, zijn in belangrijke mate, maar niet uitsluitend, gericht aan de Nederlandse overheid en politiek. Het onderzoek strekt zich daarbij niet uit tot cyberdreigingen in openlijke conflict- of oorlogssituaties.

1.4 Aanpak

Door middel van literatuuronderzoek en interviews met deskundigen en betrokken maatschappelijke partijen zijn inzichten verzameld over cyberdreigingen, weerbaarheid en eventueel te nemen maatregelen. Het merendeel van de interviews is afgenomen door Bertruke Wein en Rob Willems, beiden verbonden aan de Radboud Universiteit. De trendanalyse op basis van bestaand cijfermateriaal en de internationale vergelijking zijn gemaakt door Jasper Veldman, Leonie Hermanussen, Tommy van der Vorst en Reg Brennenraedts, allen werkzaam bij Dialogic.

De voorlopige bevindingen van het literatuuronderzoek en de interviews, inclusief benodigde maatregelen om de weerbaarheid tegen cyberdreigingen te versterken, zijn besproken tijdens twee opeenvolgende workshops met deskundigen en betrokken maatschappelijke partijen. Deze

workshops hebben plaatsgevonden op 13 december 2016 en 10 januari 2017. De namen van de deelnemers aan de interviews en de workshops staan vermeld in Bijlage 1 en Bijlage 2.

Deze studie beschrijft de bevindingen van de onderzoeksactiviteiten en de workshops. Ook zijn hierin de belangrijkste bevindingen van de trendanalyse en de internationale vergelijking verwerkt. De trendanalyse als geheel is opgenomen in Bijlage 3.

1.5 Leeswijzer

De volgende hoofdstukken beschrijven de opbrengst van het onderzoek. Hoofdstuk 2 beschrijft de belangrijkste cyberdreigingen gericht op de Nederlandse samenleving. Hoofdstuk 3 brengt in kaart hoe het is gesteld met de weerbaarheid van de Nederlandse samenleving tegen deze dreigingen. Hoofdstuk 4 bespreekt de mogelijke maatregelen om de weerbaarheid tegen cyberdreigingen te versterken en beschrijft ook de kansen die dit biedt voor de Nederlandse economie, evenals de positie van Nederland in het internationale speelveld. Hoofdstuk 5 is te lezen als samenvatting van het rapport. Het zet de belangrijkste conclusies op een rij en formuleert aanbevelingen. Een overzicht van de aanbevelingen is te vinden in paragraaf 5.6.

Dit rapport verwijst verschillende keren naar ‘gesprekspartners’. Hiermee zijn de deelnemers bedoeld aan de interviews of aan de workshops.

2 Cyberdreigingen

2.1 Cyberdreigingen niet meer weg te denken

Alles waar ICT in zit, valt in beginsel te hacken. ICT is inherent onveilig. Computerprogramma's bestaan uit vele, soms miljoenen regels code, waar onvermijdelijk fouten en onvolkomenheden in sluipen. Deze kwetsbaarheden – die niet alleen voorkomen in software, maar ook in hardware – komen vaak pas aan het licht als hiervan door kwaadwillende partijen misbruik is gemaakt.

In hoofdstuk 1 is er al op gewezen dat ICT niet alleen het alledaagse leven van de gewone burger vergemakkelijkt, maar ook dat van criminelen, spionnen en andere kwaadwillende partijen. Dit hoofdstuk beschrijft de belangrijkste dreigingen die samenhangen met de voortschrijdende digitalisering van de samenleving. Uit de gevoerde gesprekken komt naar voren dat deze dreigingen niet meer weg te denken zijn uit onze samenleving. De dreigingen die we uit de fysieke wereld kennen – vandalisme, criminaliteit, spionage, terrorisme – doen zich ook voor in het digitale domein. En net als in de fysieke wereld zijn de motieven van de aanvallers divers van aard. Criminelen zijn uit op financieel gewin, spionage is gericht op het verkrijgen van hoogwaardige informatie en terroristen zijn uit op verstoring. Maar een cyberaanval kan ook voortvloeien uit een conflict tussen werknemer en werkgever of uit baldadigheid van een puber.

In vergelijking met traditionele vormen van criminaliteit en spionage kunnen cybercriminelen en cyberspionnen gemakkelijker op grote schaal en over landsgrenzen heen opereren. Het internet kent geen grenzen, en één aanval kan vele duizenden of zelfs miljoenen slachtoffers maken. Bovendien is lang niet altijd en eenvoudig te achterhalen wie achter een bepaalde aanval zit en is bewijs daarvoor lastig hard te maken. Dat maakt vervolging moeilijk (AIVD 2016; 2017).

De grootte van de dreiging hangt daarnaast samen met de vaardigheden van de aanvallers en de middelen die hun ter beschikking staan. Zoals ook uit dit hoofdstuk zal blijken, hebben de gemiddelde middelbare scholier of kleine crimineel minder digitale vaardigheden en slagkracht dan de georganiseerde misdaad of inlichtingendiensten van buitenlandse mogendheden. De ene dreiging is kortom de andere niet – hoewel ook een hack van een middelbare scholier aanzienlijke maatschappelijke of economische schade kan veroorzaken.

Dit hoofdstuk beschrijft de diverse dreigingen in volgorde van de mate van complexiteit van de aanval en de vaardigheden van de betrokken hackers: van *scriptkiddies* met beperkte digitale vaardigheden en middelen tot statelijke actoren, die in staat zijn tot zeer geavanceerde hacks. Ook gaat dit hoofdstuk in op de maatschappelijke en economische schade als gevolg van cybercrime en cyberspionage.

2.2 Scriptkiddies

Cybervandalen en scriptkiddies zijn vaak minderjarig en plegen aanvallen uit baldadigheid of om de eigen vaardigheden aan te tonen. Het kennisniveau van cybervandalen varieert, dat van scriptkiddies is doorgaans laag. Volgens het Cybersecuritybeeld Nederland 2016 neemt de dreiging die van hen uitgaat toe. Deze wordt veroorzaakt door de groeiende beschikbaarheid van laagdrempelige middelen voor digitale aanvallen. Zo voeren cybervandalen en scriptkiddies steeds gemakkelijker *destributed denial of service* (DDoS)-aanvallen uit, waarmee een website kan worden platgelegd. Zij kunnen daarvoor gebruikmaken van diensten die op ondergrondse marktplaatsen worden aangeboden (*DDoS-as-a-service*). Ook met weinig geld en kennis kan hierdoor een effectieve aanval worden uitgevoerd (NCSC 2016). Volgens Scott en Spaniel kost het laten uitvoeren van een 24 uur durende aanval tegen een doelwit gemiddeld tussen de 25 en 150 dollar (Scott & Spaniel 2016).

Deze laagdrempelige toegang tot middelen om een DDoS-aanval uit te voeren past in een algemener patroon. Aanvalsmiddelen die in eerste instantie alleen ter beschikking staan van geavanceerde hackers, vinden na verloop van tijd hun weg naar partijen die over minder kennis en vaardigheden beschikken, zoals kleinere criminelen of (zelfs) scriptkiddies.

2.3 Terroristen

Terroristische groeperingen lijken nog onvoldoende ICT-vaardigheden in huis te hebben om serieuze cyberaanvallen te kunnen plegen, maar dit lijkt slechts een kwestie van tijd.

De digitale activiteiten van de islamitische terreurgroep ISIS worden wel meer offensief en gericht van aard. Zo publiceert ISIS vaker persoonsgegevens van westerse militairen en overheidspersoneel (*doxing*), met als doel hen als potentiële doelwitten van aanslagen te benoemen (AIVD 2016).

Daarnaast slaagt ISIS – of slagen sympathisanten ervan – er vaker in websites te hacken en de tekst van de originele webpagina te vervangen door een ideologische boodschap (*defacing*). Dergelijke aanvallen worden op zich niet gezien als terroristische activiteiten, maar als propaganda (NCSC 2016).

2.4 Cybercriminelen

Cybercriminaliteit ontwikkelt zich steeds meer tot een vorm van georganiseerde misdaad. Cybercriminelen worden professioneler, de door hen gebruikte methoden complexer en hun verdienmodel winstgevender. Malware infecties nemen in aantal toe, botnets worden beter verhuld en steeds vaker wordt gebruikgemaakt van *spear* phishing. Deze geavanceerde vorm van phishing richt zich op individuele internetgebruikers en maakt gebruik van persoonlijke informatie, die bijvoorbeeld door het doelwit zelf op Facebook of LinkedIn is geplaatst. Zo kan een op het oog

onschuldig attachment bij een e-mail die afkomstig lijkt te zijn van een bekende, tot nare verrassingen leiden (NCSC 2014; 2015).

Vooral het gebruik van ransomware heeft de afgelopen jaren een grote vlucht genomen. Zowel burgers en bedrijven, maar ook ziekenhuizen, krijgen steeds vaker te maken met malware die computerbestanden versleutelt en daarmee ontoegankelijk maakt, waarbij voor ontsleuteling van de bestanden losgeld wordt gevraagd. Bedrijven zijn bij een ransomware-infectie overigens vaak bereid om het gevraagde losgeld te betalen vanwege de continuïteit van de bedrijfsvoering. Toch is het nog maar de vraag of de versleuteling bij betaling van het losgeld daadwerkelijk ongedaan wordt gemaakt. Ransomware lijkt voor criminelen een succesvol verdienmodel te zijn geworden. Volgens het Centraal Planbureau (CPB) varieert de geschatte omzet van criminelen bij het gebruik van ransomware tussen de € 70.000 en € 1.500.000, terwijl de kosten ervan beperkt zijn (CPB 2016).

Van ransomware zijn geavanceerdere vormen in opmars. Ongerichte besmettingen met ransomware worden meer en meer vervangen door op de persoon of organisatie gerichte phishing e-mails. Ook de aard van de ransomware verandert. Zo worden de laatste tijd back-ups – die juist bescherming moeten bieden tegen aanvallen met ransomware – versleuteld (NCSC 2016).

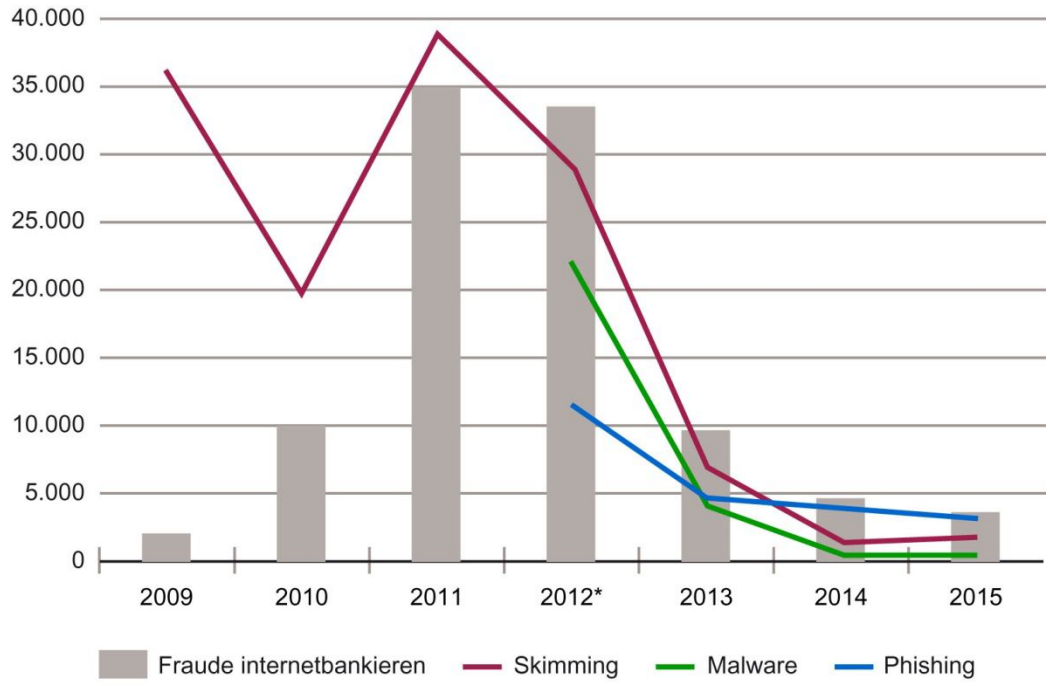
De laatste jaren is tevens een professionele criminele dienstensector ontstaan op het gebied van cybercrime. Met behulp van deze diensten (*cybercrime-as-a-service*) kunnen ook minder vaardige criminelen aanvallen uitvoeren – zoals ook al bij de scriptkiddies duidelijk werd. Het gaat hierbij onder andere om gestolen creditcardgegevens, gegevens over e-mailaccounts, kant-en-klare malware (waaronder ransomware) en DDoS-aanvallen. Sommige aanbieders hiervan hebben zelfs een helpdesk waarmee tijdens kantooruren of 24 uur per dag ondersteuning kan worden geboden. De opkomst van digitale valuta zoals de bitcoin vergemakkelijkt deze criminele dienstverlening (NCSC 2014; 2016).

Bankensector gewild doelwit

De bankensector is in verschillende opzichten een interessante case. Banken vormen al langer een gewild doelwit van cybercriminelen, onder andere vanwege de snelle groei die internetbankieren de afgelopen jaren heeft doorgemaakt. Zoals figuur 1 laat zien, is tussen 2009 en 2011 de fraude met internetbankieren sterk toegenomen. In 2011 bedroeg de daardoor veroorzaakte schade 35 miljoen euro. Maar na 2012 neemt de schade ook weer snel af. In 2015 bedroeg de schade 3,7 miljoen euro (NVB 2016).

Deze afname is gevolg van door de financiële sector getroffen maatregelen, waaronder voorlichtingscampagnes gericht op het voorkomen van fraude en het traceren van verdachte transacties. In reactie op deze succesvolle maatregelen hebben criminelen hun doelwit inmiddels verschoven. In plaats van (grote groepen) particuliere rekeninghouders proberen zij nu (zakelijke) klanten en medewerkers van banken te treffen (NCSC 2016).

Figuur 1: Schade door fraude met internetbankieren (x 1.000 euro).



* Sinds 2012 wordt in de frauderapportage een onderscheid gemaakt tussen phishing, malware en overige fraudevormen.

Bron: Nederlandse Vereniging van Banken (2016), 'Factsheet Veiligheid en Fraude'.

Dit voorbeeld laat niet alleen zien dat er succesvol opgetreden kan worden tegen cybercrime, maar ook dat criminelen steeds op zoek zijn naar nieuwe mogelijkheden om hun slag te slaan. Als gewone phishing e-mails niet meer volstaan om mensen geld afhandig te maken, schakelen ze over op meer geavanceerde methoden als spear phishing. En als banken op particuliere rekeninghouders gerichte fraude onder controle lijken te krijgen, richten ze hun pijlen op de financiële instellingen zelf.

2.5 Cyberspionage door statelijke actoren

Naast cybercriminelen zijn statelijke actoren – buitenlandse inlichtingendiensten en daaraan gelieerde groeperingen – buitengewoon actief in het digitale domein. Vooral Russische en Chinese inlichtingendiensten verzamelen in westerse landen informatie over politieke, militaire, wetenschappelijke en technologische onderwerpen. Zo verzamelen Russische inlichtingendiensten politieke informatie over standpunten van westerse landen in geopolitieke kwesties. Het gaat hierbij om zeer professionele diensten die over een grote operationele slagkracht beschikken. Landen als Rusland en China zetten op dagelijkse basis wereldwijd naar schatting meer dan honderdduizend personen in voor spionagedoeleinden. Maar ook andere landen, waaronder Iran, zijn actief op dit gebied. Nederlandse overheidsinstellingen zijn structureel doelwit van omvangrijke en geavanceerde digitale spionage-aanvallen. Digitale aanvallen door statelijke actoren vormen daarmee een continue dreiging voor de nationale veiligheid (AIVD 2016; MIVD 2016).

Behalve op politieke doelen vindt omvangrijke spionage plaats op economische doelen. Vooral de Chinese inlichtingendiensten richten zich op bedrijven met economisch gevoelige informatie, om daarmee economisch voordeel te behalen. Daarbij gaat het onder andere om bedrijven die deel uitmaken van de Nederlandse topsectoren. Volgens de AIVD zijn aanvallers daarbij op zoek naar specialistische technologie, en soms zelfs naar experimentele technologie die zijn marktwaarde nog moet bewijzen (AIVD 2016). Economische spionage kan dan ook leiden tot omvangrijke schade voor de getroffen organisaties.

Statelijke actoren beschikken over zeer geavanceerde methoden die structureel bestaande beveiligingsmaatregelen omzeilen en vaak lastig te detecteren zijn. Vanwege het geavanceerde karakter van de aanvallen is het ook niet altijd mogelijk om met zekerheid vast te stellen wie er achter een aanval zit. Veel van deze aanvalscampagnes maken gebruik van spear phishing om een netwerk binnen te komen. Eenmaal binnen kunnen spionageactiviteiten maanden tot jaren onopgemerkt blijven (NCSC 2015). Aangevallen bedrijven zijn zich vaak niet bewust van spionageactiviteiten, terwijl de aanvallers vaak kunnen beschikken over de hoogste toegangsrechten tot de digitale infrastructuur van het doelwit (Verhagen 2016). Een aanvallende partij kan heer en meester zijn op het binnengedrongen netwerk en de nieuwe beveiligingsmaatregelen die de getroffen organisatie neemt, steeds een stap voorblijven.

De kwaliteit en bandbreedte van de Nederlandse ICT-infrastructuur zorgt ervoor dat deze ook op grote schaal door partijen van buitenaf wordt gebruikt voor DDoS-aanvallen of cyberspionage gericht op andere landen (AIVD 2016).

2.6 Schade door cybercrime en cyberspionage

Cybercrime kan leiden tot grote maatschappelijke en economische schade. Volgens cijfers van het CBS is in 2015 ongeveer 11 procent van de Nederlanders slachtoffer geweest van cybercrime (CBS 2016). En uit onderzoek van PwC en de Vrije Universiteit Amsterdam kwam naar voren dat meer dan 20 procent van de Nederlandse bedrijven en instellingen rapporteerde de laatste twee jaar last te hebben gehad van cybercrime. De daadwerkelijke cijfers liggen volgens de onderzoekers ‘zeer waarschijnlijk’ hoger (PwC & VU 2014).

Volgens schattingen van Deloitte kost cybercriminaliteit de Nederlandse economie per jaar circa 10 miljard euro (Deloitte 2016). Verhagen noemt een bedrag van circa 15 miljard euro, waarin ze verdisconteert dat lang niet alle schade als gevolg van cybercrime bekend is (Verhagen 2016).

Dergelijke cijfers kenmerken zich echter door grote onzekerheden die het moeilijk maken om harde uitspraken te doen over de daadwerkelijke schade (Overvest & Straathof 2015; Hendriks et al. 2016). Zo wijst het CPB erop dat zowel het belang van cyberveiligheid voor de economie als de economische schade als gevolg van cybercriminaliteit moeilijk zijn te kwantificeren. Schattingen daarvan zijn volgens het CPB doorgaans gebaseerd op *best guesses* van experts en ‘ondoorzichtige methodologieën’ (CPB 2016).

Voor cyberspionage gericht op economische doelen is nog moeilijker vast te stellen wat daarvan de schade is, omdat die mogelijk pas op langere termijn duidelijk wordt (NCSC 2016).

Cybercrime en cyberspionage vormen serieuze bedreigingen. Als het Nederlandse bedrijfsleven op grote schaal te duchten heeft van cybercriminaliteit, en buitenlandse inlichtingendiensten kennis weten te achterhalen over technologische innovatie – een belangrijke pijler van de Nederlandse economie –, kan dat op den duur het innovatie- en concurrentievermogen van het Nederlandse bedrijfsleven ondergraven (Verhagen 2016).

2.7 Manipulatie van informatie

Statelijke actoren kunnen digitale middelen ook inzetten om de publieke opinie, de politieke stabiliteit of het politieke besluitvormingsproces van een ander land te beïnvloeden (NCSC 2016). Manipulatie van informatie vormt daarmee een bedreiging voor het functioneren van het democratisch bestel.

De opzettelijke verspreiding van nepnieuws valt hieronder. Evenals het reeds genoemde voorbeeld van de (vermoedelijk) Russische hack en openbaarmaking van het e-mailverkeer binnen de Democratische Partij, met als verondersteld doel beïnvloeding van de Amerikaanse presidentsverkiezingen van 2016. Ook andere westerse landen maken zich grote zorgen over manipulatie van berichtgeving door buitenlandse mogendheden. In Duitsland speelt dit met het oog op de verkiezingen voor de Bundestag in 2017. Zo is er misleidende informatie over criminele activiteiten van migranten verspreid, wat de populariteit van eurosceptische partijen als Alternative für Deutschland in de hand zou kunnen werken. Volgens de Duitse inlichtingen- en veiligheidsdiensten maakt deze vorm van manipulatie deel uit van een langlopende Russische cyberaanval op Duitsland (*Deutsche Welle* 2016a; 2016b).

Met het oog op propaganda die uit Rusland afkomstig is, heeft de Europese Unie de East StratCom Task Force ingesteld. Volgens deze taskforce zijn Russische hackers buitengewoon actief en is er sprake van een grote, georganiseerde desinformatiecampagne, gericht op de Europese Unie (Alonso 2017).

2.8 Cybersabotage

Ook cybersabotage vormt een groot risico. Een doelbewuste verstoring van vitale sectoren, zoals energiecentrales, de drinkwatervoorziening of het betalingsverkeer kan tot grote economische schade en maatschappelijke ontwrichting leiden (Verhagen 2016). Het internet zelf kan eveneens als een vitale infrastructuur worden beschouwd. Als bijvoorbeeld door een DDoS-aanval het internet wordt platgegooid, heeft dat grote gevolgen voor het functioneren van de economie en samenleving.

Buitenlandse militaire inlichtingendiensten leggen zich in toenemende mate toe op het binnendringen van industriële controlesystemen (SCADA-systemen), die onder andere worden

gebruikt door bedrijven in vitale sectoren. Manipulatie van of het toebrengen van schade aan dergelijke systemen zouden een belangrijke rol kunnen gaan spelen in toekomstige conflictsituaties (MIVD 2016).

Voor zover bekend hebben zich in Nederland nog geen situaties voorgedaan waarbij actoren van buitenaf succesvol sabotage hebben gepleegd (NCSC 2016). Maar in het buitenland hebben wel degelijk ernstige vormen van sabotageaanvallen plaatsgevonden. Zo kreeg Estland in 2007 te maken met een reeks zware DDoS-aanvallen van vermoedelijk Russische makelij. De aanvallen legden onder andere een aantal nieuwswebsites en overheidswebsites en -diensten plat en leidden ertoe dat de grootste bank van Estland meer dan een uur offline was. De bank leed daardoor voor meer dan 1 miljoen dollar aan schade. Mogelijk zaten Russische hackers achter de aanvallen, als vergelding voor het verplaatsen van een WO-II standbeeld van een Russische soldaat (Landler & Markoff 2007; Davis 2007; Traynor 2007).

In 2015 kwamen in Oekraïne bij een aanval op elektriciteitsbedrijven ongeveer een miljoen mensen zonder stroom te zitten. De daders, vermoedelijk een Russisch hackerscollectief, hadden de ICT-systemen van de elektriciteitsbedrijven gehackt waarna ze de werking ervan konden dwarsbomen. Het duurde zes uur voordat de stroomvoorziening weer was hersteld (NCSC 2016; Trend Micro 2016).

2.9 Het Internet of Things & DDoS

Een vrij recente ontwikkeling die de impact van diverse cyberdreigingen danig kan veranderen, is de opkomst van het Internet of Things. Steeds meer apparatuur, waaronder huishoudelijke apparaten, wearables, televisies, zelfrijdende auto's en ook medische apparatuur, wordt met het internet verbonden. De beveiliging van deze *smart devices* is vaak niet op orde. Bijvoorbeeld omdat er met standaard wachtwoorden wordt gewerkt, de software niet eenvoudig kan worden geüpdatet of de leverancier na een bepaalde tijd stopt met het onderhouden ervan.

Met de enorme groei die het aantal smart devices doormaakt, wordt het aanvalsvlak voor cybercriminelen met de dag groter. Dat geldt niet alleen voor netwerken van individuele gebruikers thuis, maar ook voor die van bedrijven en overheidsinstanties. Eén zwakke schakel in een netwerk, in de vorm van een onvoldoende beveiligd apparaat, kan hackers al toegang verlenen tot dat netwerk, inclusief andere daarop aangesloten apparaten. En dat kan leiden tot het stelen, misbruiken of manipuleren van persoonlijke gegevens of andere belangrijke informatie.

Gehackte apparaten kunnen ook worden ingezet als onderdeel van een groot aanvallend netwerk waarmee DDoS-aanvallen kunnen worden uitgevoerd. Er zijn de afgelopen tijd aanvallen gesignaleerd die gebruikmaken van honderdduizenden of zelfs miljoenen aan het internet gekoppelde apparaten. DDoS-aanvallen nemen daardoor enorm in kracht toe. En als zo'n aanval maar zwaar genoeg is, zal uiteindelijk elk ICT-systeem dat met het internet is verbonden, platgaan.

Een recent voorbeeld van een grote DDoS-aanval vond plaats in oktober 2016 en trof het cloud- en netwerkinfrastructuurbedrijf Dyn (Hilton 2016). Dyn kreeg te maken met drie DDoS-aanvallen. De

eerste aanval trof de Dyn-datacentra in Chicago, Washington DC en New York. Vooral gebruikers aan de oostkust van de Verenigde Staten ondervonden hiervan hinder. Populaire websites als Twitter, Netflix, Spotify en GitHub waren twee uur lang onbereikbaar. De tweede en derde aanval troffen Dyn-datacentra wereldwijd en hielden enkele uren aan. Voor de aanvallen werd gebruikgemaakt van gehackte digitale videorecorders, printers en andere apparaten met internettoegang. Mogelijk waren bij de aanval 100.000 geïnfecteerde apparaten betrokken (Hendrikman 2016). De hackergroepen Anonymous evenals New World Hackers claimden achter de aanval te zitten, maar bewezen is dit niet. Een beveiligingsbedrijf verdenkt scriptkiddies hiervan, omdat een deel van de gebruikte aanvalsinfrastructuur werd ingezet om een gamebedrijf aan te vallen (Security.nl 2016).

DDoS-aanvallen kunnen, evenals ransomware, ook voor andere doelen worden ingezet, zoals afpersing. De aanvaller voert dan een kleine DDoS-aanval uit en laat aan de getroffen organisatie weten dat een grotere aanval uitblijft als de organisatie betaalt. Managed service providers geven aan dat ze wekelijks te maken hebben met dergelijke pogingen tot afpersing. Vooralsnog zijn er geen gevallen bekend waarbij het uitblijven van betaling tot een grotere aanval heeft geleid (NCSC 2016).

Tijdens een internationale expertmeeting die door de Cyber Security Raad (CSR) werd georganiseerd, werd geconcludeerd dat de opkomst van het Internet of Things een van de meest disruptieve hedendaagse ontwikkelingen is en een grote uitdaging vormt op het gebied van cybersecurity (CSR 2016).

3 Digitale weerbaarheid

3.1 Gemak boven veiligheid

De cyberdreigingen die in hoofdstuk 2 zijn beschreven, roepen de vraag op hoe het is gesteld met de weerbaarheid van de Nederlandse samenleving. Kort gezegd is de weerbaarheid van de burger, het bedrijfsleven en de overheid in veel gevallen onvoldoende. Cybersecurity krijgt in de praktijk vaak nog weinig prioriteit. ICT-toepassingen worden vooral beoordeeld op hun functionaliteit; gemak gaat boven veiligheid.

Dat wil niet zeggen dat er geen besef is van mogelijke risico's van het steeds grootschaliger gebruik van ICT. Krantenkoppen over datalekken in de zorg, de Russische hack van de Amerikaanse Democratische Partij en de onthullingen door Edward Snowden over de inlichtingenpraktijken van de Amerikaanse NSA dragen bij aan dat besef. Tegelijkertijd hebben burgers, bedrijven en overheden onvoldoende kennis van en inzicht in de precieze risico's die ze lopen en in de mogelijkheden om daar iets aan te doen. Risico's blijven vaak ongrijpbaar, en de noodzaak om maatregelen te nemen onderbelicht, tot het moment dat het daadwerkelijk misgaat. Zo was de hack in 2011 van Diginotar, een bedrijf dat verantwoordelijk was voor de beveiliging van overheidswebsites, een belangrijke wake-upcall voor de overheid.

Niet iedereen vormt een even waarschijnlijk doelwit voor een cyberaanval. Ook verschillen de risico's tussen diverse doelwitten. De doorsnee burger of kleine middenstander zal over het algemeen weinig te duchten hebben van digitale spionage of sabotage door buitenlandse inlichtingendiensten, en mocht dat wel het geval zijn, dan zal het hem of haar ten enenmale aan middelen ontbreken om zich daartegen te verweren. Omgekeerd zullen grote organisaties die over veel kennis en middelen beschikken, over het algemeen minder te vrezen hebben van aanvallen door scriptkiddies of kleine criminelen.

De weerbaarheid van de diverse doelwitten wordt hieronder besproken in volgorde van het vermogen van de (beoogde) doelwitten om zich tegen cyberdreigingen te verweren: van burgers, consumenten en kleinere bedrijven met beperkte digitale vaardigheden en middelen tot grote ondernemingen en organisaties met veel weerstandsvermogen.

3.2 Beperkte weerbaarheid burger

Nederlandse burgers lopen internationaal voorop in de adoptie van ICT in hun dagelijkse leven. Maar hun digitale vaardigheden houden daar, zeker als het gaat om cybersecurity, geen gelijke tred mee. Volgens de jaarlijkse Alert Online monitor scoren Nederlanders een krappe voldoende als het gaat om veilig gedrag.

Veruit de meest gebruikte maatregel waarmee burgers zich beschermen tegen cyberincidenten is antivirussoftware. Uit een kwantitatief onderzoek door Gfk naar online gedrag van onder andere

burgers wordt duidelijk dat 71 procent gebruikmaakt van automatische software-updates. Andere basismaatregelen worden echter veel minder gebruikt, zoals het maken van back-ups, sterke wachtwoorden of apparaten zo instellen dat ze niet automatisch verbinding maken met WiFi-netwerken (Gfk 2015). Juist deze maatregelen zijn van belang met het oog op de toenemende inzet van ransomware door cybercriminelen en het toenemende aantal apparaten dat met het internet verbonden is en door consumenten wordt verkocht.

Burgers zijn alerter wanneer het gaat om phishing mails. De overgrote meerderheid zegt verdachte mails direct te verwijderen en niet op links te klikken die men niet vertrouwt. Ook denkt de helft van de respondenten in het Gfk-onderzoek phishing mails meteen bij ontvangst te herkennen. Maar relatief nieuwe technieken die cybercriminelen inzetten, zoals ransomware en spear phishing, zijn minder bekend. Zo heeft 65 procent van de Nederlanders nog nooit van de term ransomware gehoord (Gfk 2015).

Toch kan niet worden gesteld dat burgers online gevaren onderschatten. Zo voelt slechts 43 procent van de ondervraagden zich beschermd tegen gevaren op het internet en is de helft van mening dat kwaadwillenden toch wel zullen slagen in hun opzet. Ze schatten dan ook in dat ze zich eigenlijk niet kunnen verweren tegen grote gevaren.

De opkomst van het Internet of Things leidt tot nieuwe risico's voor burgers. Vanwege het gebrek aan beveiliging van veel aan het internet verbonden apparaten – waaronder veel consumentenelektronica – wordt een gebruiker niet alleen kwetsbaar voor datalekken en ransomware, maar ook voor het manipuleren of onklaar maken van apparatuur. Zo zijn er voorbeelden bekend van gehackte insulinepompen waardoor de dosis insuline van buitenaf kon worden beïnvloed en gehackte auto's waarvan de remmen op afstand onklaar waren gemaakt (Greenberg 2015; Keijzer 2016).

Daarnaast kunnen geïnfecteerde apparaten, zoals in hoofdstuk 2 is beschreven, ook onderdeel uitmaken van een botnet om DDoS-aanvallen mee uit te voeren. De bezitter van zo'n apparaat hoeft daar zelf niets van te merken, maar kan, zonder zich daarvan bewust te zijn, wel bijdragen aan een aanval en daardoor veroorzaakte schade. Onbeveiligde apparaten vormen dus niet alleen een risico voor een individuele eindgebruiker, maar ook een potentieel gevaar voor het functioneren van een (vitale) ICT-infrastructuur. Hacks van onvoldoende beveiligde apparatuur kunnen dan ook ernstige gevolgen hebben. Ze kunnen zowel leiden tot maatschappelijke ontwrichting – bij een aanval op vitale sectoren – als tot een dodelijke afloop voor gebruikers, zie de gehackte insulinepomp of autoremmen.

Hoewel er vraagtekens kunnen worden geplaatst bij de vanzelfsprekendheid waarmee allerlei consumentenproducten – tot koelkasten en broodroosters aan toe – aan het internet worden gekoppeld, is de verwachting dat deze trend moeilijk te keren valt. Consumenten hebben ook lang niet altijd meer een keuze. Overheden en energiemaatschappijen willen alle huishoudens uitrusten met een slimme energiemeter en de standaard televisie is tegenwoordig een smart TV. Voor de doorsnee burger lijkt het echter onbegonnen werk om de beveiliging van dit soort apparaten voor zijn rekening te nemen.

Marktfalen

Een probleem hierbij is dat op dit moment de economische prikkels voor ICT-leveranciers ontbreken om de beveiliging van ICT-apparatuur substantieel te verbeteren. De prijsconcurrentie voor deze apparaten is hoog, en voor een lage prijs kunnen de bedrijven geen goede beveiliging leveren. De consument vraagt er bovendien niet naar. Omdat de beveiliging van ICT-apparaten maatschappelijk gewenst is, kan dit worden beschouwd als een vorm van 'marktfalen' (CPB 2016).

3.3 Ondersteuning nodig voor midden- en kleinbedrijf

Voor het midden- en kleinbedrijf (MKB) geldt een vergelijkbaar verhaal als voor de burger. Vooral kleinere bedrijven hebben over het algemeen maar een beperkt inzicht in de risico's die ze lopen. Ze hebben daarnaast onvoldoende middelen, kennis of toegang tot kennis om passende maatregelen te nemen (Verhagen 2016). Weliswaar worden door ICT-leveranciers allerlei beveiligingsproducten en -diensten aangeboden, maar mkb-bedrijven zijn vaak onvoldoende in staat geboden oplossingen op waarde te schatten en te beoordelen of die producten en -diensten voor hun situatie een goede oplossing bieden. Het CPB spreekt in dit verband van een kennisasymmetrie tussen ICT-leveranciers en -gebruikers. En omdat bedrijven niet weten wat ze aan beveiligingsmaatregelen moeten vragen, wordt de prijs vaak doorslaggevend (CPB 2016).

Binnen het MKB is de basisbeveiliging vaak niet op orde. Er worden geen sterke wachtwoorden gebruikt, beveiligingssoftware wordt onregelmatig geüpdatet, en er worden onvoldoende back-ups van belangrijke bestanden gemaakt. Het kan overigens ook voorkomen dat bedrijven zich laten verleiden tot de aanschaf van een in hun ogen innovatieve ICT-oplossing, zonder dat zij beschikken over de kennis om de software naar behoren te gebruiken of voldoende hebben nagedacht over de eigenlijke dreigingen waaraan ze blootstaan. Dat kan leiden tot schijnzekerheid.

Bovendien brengt technologie alleen vaak niet de oplossing. De werknemer achter de laptop, pc of tablet is vaak de zwakste schakel. Mensen laten zich door spear phishing e-mails gemakkelijk verleiden tot het aanklikken van geïnfecteerde weblinks. Een probleem dat hierbij meespeelt, is dat op ICT-gebied werk en privé vaak door elkaar lopen. Malware op de privé-computer of tablet kan ook de werkomgeving besmetten.

Binnen het MKB bestaat grote behoefte aan onafhankelijke advisering en ondersteuning ten aanzien van te nemen beveiligingsmaatregelen, die ook passend moeten zijn. Omdat het MKB bestaat uit een grote en zeer diverse groep bedrijven, variërend van zelfstandigen zonder personeel tot bedrijven met 250 werknemers, hangen de benodigde maatregelen af van het type bedrijf en de specifieke sector waarbinnen dat bedrijf werkzaam is. Ongeveer 97 procent van het bedrijfsleven maakt deel uit van het MKB. Daarmee vormt het gebrek aan weerbaarheid een serieus probleem.

3.4 Meer bewustzijn bij grotere bedrijven

Grotere bedrijven zijn zich over het algemeen meer bewust van de risico's die ze lopen op het gebeid van cyberveiligheid en zijn in staat om gespecialiseerde securitykennis in huis te halen om

de organisatie te beveiligen. Wel kan het voor deze bedrijven een probleem zijn om de bedrijfstop te overtuigen van benodigde investeringen in veiligheidsmaatregelen. Investeringen worden al snel als ‘negatieve investeringen’ gezien, omdat ze geen directe baten opleveren. Hierbij speelt mee dat cyberrisico’s vaak lastig te kwantificeren zijn.

Ook zijn de getroffen maatregelen niet altijd even effectief. Beveiligingsinspanningen zijn vaak vooral gericht op het voorkomen dat aanvallers ICT-netwerken binnendringen. Dergelijke inspanningen voorkomen echter niet dat volhardende of meer geavanceerde hackers toch een manier weten te vinden om binnen te komen. En als ze eenmaal binnen zijn, kunnen ze langere tijd in een netwerk actief zijn zonder te worden opgemerkt. Beveiligingsmaatregelen die zich richten op het detecteren van activiteiten van indringers, krijgen vaak echter weinig aandacht (AIVD 2016; 2017).

3.5 Vitale infrastructuur vraagt aandacht

Uitval van vitale sectoren als de energievoorziening, het betalingsverkeer of de drinkwatervoorziening kan leiden tot ontwrichting van het maatschappelijke en economische verkeer. Om dit risico te verkleinen, om dreigingen te onderkennen en het hoofd te bieden, ondersteunt het Nationaal Cyber Security Centrum (NCSC) de vitale sectoren.

De vitale sectoren zijn overigens divers van aard en verschillen in hun weerbaarheidsniveau. De energie-, telecom- en financiële sector lijken hun weerbaarheid redelijk goed op orde te hebben. De Nederlandse bankensector geldt – ook internationaal – zelfs als een innovatieve sector op dit gebied. Eerder is al genoemd dat de banken succesvol maatregelen hebben weten te nemen tegen aanvallen door criminelen op particuliere rekeninghouders. Daarnaast hebben de banken de afgelopen jaren flink geïnvesteerd in maatregelen tegen DDoS-aanvallen, onder meer door diensten van bedrijven in te kopen die bescherming bieden tegen deze aanvallen (*cybersecurity-as-a-service*). Hoewel deze maatregelen duur zijn, zijn ze inmiddels ‘business as usual’ (NCSC 2016).

Maar ook in de vitale infrastructuur blijft de mens achter de computer of tablet vaak de zwakke schakel, zijn basale veiligheidsmaatregelen niet altijd op orde en wint gebruiksvriendelijkheid het nog regelmatig van veiligheid.

Volgens een van onze gesprekspartners wordt in de vitale sectoren te langzaam voortgang gemaakt met het ontwikkelen van noodscenario’s, bijvoorbeeld bij een grootschalige aanval. Er zijn nog te weinig back-upvoorzieningen voorhanden die ervoor moeten zorgen dat vitale processen in noodsituaties blijven draaien. Hierbij doet zich een spanning voor tussen de kosten van een noodvoorziening die vanuit commercieel perspectief weinig aantrekkelijk zijn, en het publieke belang, dat gebaat is bij de continuïteit van vitale processen.

In vitale infrastructuren spelen daarnaast ook ketenafhankelijkheden. Wanneer betrokken organisaties identieke hard- en software gebruiken, kunnen kwetsbaarheden ontstaan. Gebruik van één dienst of één dienstverlener door meerdere organisaties kan leiden tot een *single point of failure*. Wanneer problemen ontstaan met die gezamenlijk gebruikte dienst of dienstverlener, en

meerdere organisaties in de keten met dezelfde uitval te maken krijgen, kan uitval minder goed worden opgevangen. Voster en De Bruijn pleiten er in dit verband ook voor om afhankelijkheden van bepaalde diensten in kaart te brengen en prioriteiten te stellen voor die gebieden waar risico's het grootst zijn (Voster & De Bruijn 2016).

3.6 Beperkte weerbaarheid tegen cyberspionage

Cyberspionage door statelijke actoren vormt zowel voor de vitale sectoren als voor de Rijksoverheid een belangrijk aandachtspunt. De AIVD is in staat om spionageaanvallen te signaleren door onder andere afwijkende patronen in het dataverkeer binnen ICT-netwerken te detecteren. Als de AIVD spionageaanvallen signaleert, informeert de dienst waar mogelijk het getroffen doelwit hierover en geeft het advies over de aanpak ervan. Deze aanpak kan er bijvoorbeeld uit bestaan het getroffen systeem van het internet te ontkoppelen en op te schonen. Als de besmetting diep in het systeem doorgedrongen is, kan dat overigens betekenen dat alle fysieke hardware moet worden vervangen. Dat laatste was het geval bij een grootscheepse aanval op de Duitse Bundestag in 2015 (Die Welt 2015).

De AIVD richt zich bij de signalering van en bescherming tegen cyberspionage vooral op de Rijksoverheid en een deel van de vitale infrastructuur. Vanwege beperkte capaciteit is de AIVD niet in staat om het gehele veld te overzien en alle spionageaanvallen te signaleren, noch om alle gesignaleerde incidenten af te handelen. De waargenomen aanvallen zijn slechts 'het topje van de ijsberg' (NCSC 2016). Ook heeft de dienst onder de huidige wetgeving beperkte bevoegdheden om het internetverkeer te monitoren.

3.7 Te weinig regie door overheid

De Rijksoverheid lijkt zich over het algemeen redelijk bewust van de risico's die spelen op het gebied van cybersecurity. Evenals de vitale sectoren wordt ze daarin bijgestaan door het NCSC en de AIVD. Voor de informatiebeveiliging bij het Rijk wordt de Baseline Informatiebeveiliging Rijksdienst (BIR) gehanteerd. Dit normenkader, dat in 2012 is verschenen, bestaat uit een lijst met verplichte standaarden en (niet-verplichte) best practices. De BIR moet het mogelijk maken om binnen het Rijk op een veilige manier samen te werken en gegevens uit te wisselen (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties 2012).

Dat wil niet zeggen dat de beveiliging ook altijd op orde is. De overheid heeft lang niet altijd voldoende expertise in huis. Dat leidt onder andere tot een 'gefragmenteerde' inkoop van cybersecuritydiensten (Hendriks et al. 2016). Ook zijn er problemen met het uitfaseren van verouderde computerprogramma's. De Algemene Rekenkamer stelt dat de ministeries de afgelopen tijd weliswaar beter zicht hebben gekregen op beveiligingsrisico's en plannen hebben opgesteld om risico's tot een 'aanvaardbaar niveau' terug te brengen, maar dat informatiebeveiliging bij het Rijk de komende jaren nog veel aandacht vraagt (Algemene Rekenkamer 2016a).

In 2015 werd bijvoorbeeld voor het derde jaar op rij gesignaleerd dat het authenticatiesysteem DigiD, dat burgers in staat moet stellen om veilig te communiceren met overheidsinstanties en zorginstellingen, niet voldeed aan de beveiligingsnormen voor webapplicaties van het NCSC (Algemene Rekenkamer 2015a). Het jaar daarop constateerde de Algemene Rekenkamer opnieuw dat DigiD, ondanks diverse verbeteringen, niet voldeed aan de informatiebeveiligingseisen. Verdere acties blijven volgens de Rekenkamer dan ook nodig (Algemene Rekenkamer 2016b).

Ook bij Rijkswaterstaat werden risico's geconstateerd met betrekking tot bruggen, wegen en sluizen. De waterkeringen, de meest risicovolle systemen, leken wel adequaat te zijn beveiligd (Algemene Rekenkamer 2015c). In 2016 zijn de problemen bij Rijkswaterstaat afgeschaald naar een 'aandachtspunt' (Algemene Rekenkamer 2016c).

In de zorg bestaat vaak een gebrek aan bewustwording en beveiligingsmaatregelen. Bij een phishingonderzoek door Deloitte onder 65.000 medewerkers van 28 ziekenhuizen klikte gemiddeld 17 procent van de medewerkers door vanuit de mail en liet een meerderheid daarvan (12 procent) onder andere persoonsgegevens achter op de website waarnaar deze medewerkers werden doorgestuurd (Van Beurden 2016). Ook kampt de zorgsector met een hoog aantal lekken van privacygevoelige informatie (Van Lonkhuyzen 2016).

In algemene zin lijkt binnen de overheid het belang van cybersecurity nog vaak te worden ondergewaardeerd en wordt beveiliging als sluitpost gezien. Bij aanbestedingen is de prijs vaak doorslaggevend. Daarbij speelt mee dat de verantwoordelijkheid bij de overheid op het gebied van cybersecurity bij verschillende ministeries is belegd, waardoor het ontbreekt aan eenduidige politieke coördinatie en sturing (Verhagen 2016). Diverse gesprekspartners wijzen er bovendien op dat de verschillende ministeries verschillende belangen hebben en dat het de overheid daardoor ontbreekt aan een integrale afweging en regie.

Voor de lagere overheden geldt nog sterker dat informatiebeveiliging aandacht behoeft. Zo heeft in 2016 bijna twee derde van de gemeenten een datalek van persoonlijke gegevens van burgers gemeld, en heeft 15 procent van de gemeenten te maken gehad met een datalek als gevolg van een aanval door cybercriminelen (Van Lonkhuyzen 2017).

3.8 Ketenafhankelijkheden

Steeds meer ICT-toepassingen zijn met elkaar zijn verbonden. Bedrijven, (semi-)overheden en beheerders van vitale infrastructuur nemen vaak netwerkgebaseerde producten of diensten (hardware, software, cloud services, dataopslag) af van andere partijen. Geen enkele organisatie is meer in staat om alle taken zelf uit te voeren. De kwetsbaarheid die deze afhankelijkheid van andere bedrijven en dienstverleners met zich meebrengt, wordt vaak onderschat. De zwakste schakel in de keten kan namelijk voor verstoringen van functies verderop in de keten zorgen. Bij vitale sectoren kan dat leiden tot vergaande uitval en maatschappelijke ontwrichting.

De ketenafhankelijkheid en de daarmee gepaard gaande kwetsbaarheden gelden ook voor digitale diensten voor kleinere gebruikers, zoals webwinkels of mkb-bedrijven. Voor hun digitale

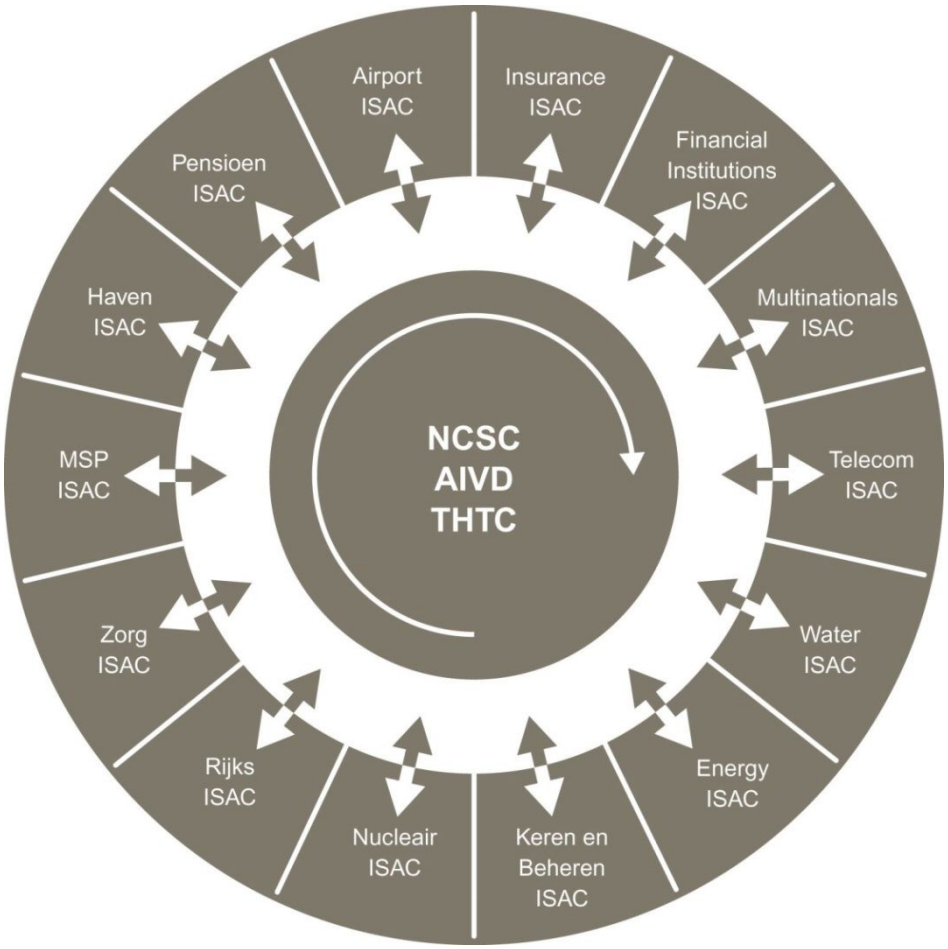
dienstverlening zijn ze vaak afhankelijk van meerdere partijen (datacenters, cloud services, internet service providers), waarvan ze niet of moeilijk kunnen beoordelen hoe veilig de aangeboden diensten zijn. Bovendien is onduidelijk waar verantwoordelijkheden liggen als er ergens iets fout gaat. Verantwoordelijkheden liggen nu nog te vaak bij de eindgebruiker.

3.9 Bestaande maatregelen ter bescherming van vitale sectoren en overheid

ISAC's

Om de weerbaarheid van de vitale sectoren tegen cyberdreigingen te versterken, zijn in Nederland zeventien Information Sharing and Analysis Centres (ISAC's) opgericht. Hierbij speelt het NCSC een ondersteunende rol. Het betreft de volgende sectoren: financiële sector, multinationals, telecombedrijven, watervoorziening, energievoorziening, keren en beheren oppervlaktewater, nucleaire installaties, Rijksoverheid, zorgsector, managed service providers, haven, pensioenen, luchthaven en verzekeringen (zie figuur 2).

Figuur 2: Overzicht Information Sharing and Analysis Centres (ISAC's).



Bron: https://www.ncsc.nl/samenwerking/isacs.html

ISAC's zijn publiek-private samenwerkingsverbanden waarin bedrijven onderling informatie en ervaringen uitwisselen over cybersecurity. De bedoeling hiervan is dat bedrijven in een vertrouwde omgeving van elkaar kunnen leren en elkaar bijstand kunnen verlenen als zich problemen voordoen. Deze samenwerkingsverbanden maken het mogelijk om complexe aanvallen het hoofd te bieden, wat voor individuele bedrijven vaak niet haalbaar is (Verhagen 2016). De bereidheid van betrokken partijen om vertrouwelijke informatie uit te wisselen, is hierbij cruciaal (ENISA 2015). Nederland loopt met de aanpak door middel van ISAC's internationaal voorop.

Het NCSC informeert de organisaties die bij de ISAC's zijn aangesloten over kwetsbaarheiden en voorziet hen van advies. Het NCSC ziet het niet als zijn taak te controleren of de organisaties de adviezen ook opvolgen en kwetsbaarheiden verhelpen. Dit behoort tot de verantwoordelijkheid van de organisaties zelf. Een controlerende rol zou volgens het NCSC de vertrouwensrelatie niet ten goede komen; organisaties zouden daardoor mogelijk minder informatie delen. Deze rolopvatting van het NCSC wordt gedeeld door de betrokken organisaties (Inspectie Veiligheid en Justitie 2015).

De beveiligingsadviezen van het NCSC hebben een gezaghebbende status. Dat helpt betrokkenen om hun management te overtuigen van de noodzaak om maatregelen te nemen. Een onafhankelijke partij als het NCSC is ook van belang omdat leveranciers van ICT-producten en -diensten hun eigen, commerciële belangen hebben (Inspectie Veiligheid en Justitie 2015).

De eigen verantwoordelijkheid van betrokken organisaties om gebleken kwetsbaarheden te verhelpen, houdt ook risico's in. De beveiliging bij de vitale sectoren is, zoals duidelijk is geworden, niet altijd op orde. Volgens diverse gesprekspartners is dat reden voor een meer actieve en leidende rol van de overheid.

Netwerkscheiding

Om vitale sectoren en de Rijksoverheid te beschermen, wordt in de Nationale Cyber Security Strategie 2 gesproken over invoering van gescheiden ICT-netwerken. Hierbij zijn verschillende varianten denkbaar. Gebruikersscheiding houdt in dat een selecte groep gebruikers wordt geautoriseerd om toegang te krijgen tot bepaalde ICT-voorzieningen van een organisatie. In aanvulling hierop kan gebruik worden gemaakt van terminalscheiding: alleen geautoriseerde computers en mobiele apparaten krijgen toegang tot ICT-voorzieningen. Daarnaast kunnen organisaties gebruikmaken van toegangsnetwerkscheiding, bijvoorbeeld door een eigen draadloos netwerk aan te leggen. In de meest veilige variant wordt het eigen netwerk niet alleen losgekoppeld van het internet, maar wordt tevens de ICT-infrastructuur vanaf de individuele componenten ontworpen en gebouwd.

In de praktijk zijn gedeeltelijke scheidingsvormen bij veel organisaties gemeengoed. De keuze voor een van de varianten vergt een afweging tussen het gewenste veiligheidsniveau en de daarvoor benodigde inzet van middelen. Zowel de financiële als de praktische haalbaarheid van ketenscheiding neemt af naarmate de veiligheid dieper in het netwerk gegarandeerd moet worden (PwC 2014).

DigiNetwerk is een voorbeeld van gedeeltelijke netwerkscheiding. Via dit netwerk kunnen overheden op een veilige manier gegevens uitwisselen met andere overheden. Diginetwerk verbindt bestaande netwerken van overheidsorganisaties met elkaar, waaronder de Haagse Ring, die op zijn beurt weer als een virtueel gescheiden netwerk draait op het glasvezelnetwerk van het Netherlands Armed Forces Integrated Network (NAFIN) (PwC 2014).

Het bedrijf TenneT, dat het Nederlandse en een deel van het Duitse hoogspanningsnet beheert, heeft een vergaande vorm van netwerkscheiding doorgevoerd. TenneT maakt voor zijn primaire proces – levering van betrouwbare en ononderbroken elektriciteitsvoorziening aan circa 41 miljoen eindgebruikers – gebruik van een eigen ICT-netwerk dat is losgekoppeld van het internet. Dit proces komt niet in gevaar als er een grootschalige DDoS-aanval plaatsvindt op Nederland. Toegang tot dit netwerk kan alleen van binnenuit. Voor optimalisering van het primaire proces, waarvoor continu contact nodig is met de elektriciteitsproducenten, maakt TenneT wel gebruik van het internet. Dat geldt ook voor het functioneren van de bedrijfsorganisatie. Daarmee zijn deze processen wel gevoelig voor bijvoorbeeld uitval van het internet. Om zich tegen hacks te beschermen heeft TenneT overigens, als een van de weinige bedrijven, de veiligheidsmaatregel ingevoerd dat werknemers privé-mail niet op hun werklaptop mogen ontvangen.

3.10 100 procent veilig bestaat niet

Aanvallen veranderen van gedaante

Hoofdstuk 2 liet zien dat cyberdreigingen voortdurend van gedaante veranderen. Cybercriminelen zijn continu op zoek naar nieuwe verdienmodellen en maken gebruik van een diversiteit aan aanvalsmiddelen; statelijke actoren ontwikkelen steeds geavanceerdere methoden om bestaande beveiligingsmaatregelen te omzeilen. Wat vandaag als veilig wordt beschouwd, kan morgen alweer achterhaald zijn.

Vanwege de snelle technologische veranderingen in combinatie met de vele wederzijdse afhankelijkheden tussen organisaties onderling en tussen organisaties en ICT-leveranciers, en de inherente onveiligheid van ICT, is nauwelijks te voorspellen welke nieuwe vormen cyberdreigingen aannemen. Zo zijn ransomware en spear phishing relatief nieuwe aanvalsmethoden. Veel ICT-gebruikers zijn hierop onvoldoende bedacht, en zijn hier dus ook onvoldoende tegen bestand. En terwijl de afgelopen jaren de beschermingsmaatregelen tegen DDoS-aanvallen succes begon af te werpen, vormen de recente DDoS-aanvallen die gebruikmaken van botnetten bestaande uit honderdduizenden met het internet verbonden apparaten, een belangrijke nieuwe uitdaging.

Wedloop tussen aanvaller en doelwit

Dreiging en weerbaarheid hangen met elkaar samen. De dreiging die van een bepaalde aanvalsmethode uitgaat, hangt af van de mate waarin het beoogde doelwit zich tegen die aanval kan verweren. Dit krachtenspel kan worden gezien als een continue wedloop – een *rat race* – tussen aanvaller en doelwit. De inventiviteit van de aanvallende partij, die op zoek is naar nieuwe kwetsbaarheden en gebruikmaakt van nieuwe aanvalsmethoden, staat hierbij tegenover het vermogen van het getroffen doelwit om hierop snel te kunnen reageren. Voor beide partijen geldt

hierbij een kosten-batenanalyse: hoeveel expertise, tijd en geld hebben partijen ervoor over om bepaalde baten te behalen (financieel gewin, hoogwaardige informatie) of schade te voorkomen?

Wat is veilig en weerbaar?

Maximale veiligheid is meestal niet – of eigenlijk nooit – haalbaar, omdat de kosten daarvan niet opwegen tegen de baten. Investeringsbeslissingen rond cyberveiligheid worden dan ook gemaakt op basis van een kosten-batenanalyse (CPB 2016). Dat geldt zowel voor bedrijven als overheden. Vergaande beveiligingsmaatregelen zoals het eigen ICT-netwerk van TenneT, zullen voor de meeste organisaties financieel onhaalbaar zijn. Maar zelfs een dergelijk netwerk biedt geen 100 procent veiligheid.

Het Stuxnet virus – waarmee naar vermoeden de Amerikaanse en Israëlische geheime diensten Iraanse uraniumverrijkingscentrifuges ontregelden – liet zien dat zo'n 'air gap' kan worden overbrugd door, in dit geval, gebruik te maken van een besmette usb-stick (Zetter 2014).

Een van de gesprekspartners stelt dan ook de vraag wat onder 'veilig' en 'weerbaar' moet worden verstaan. Risico's op het gebied van cyberveiligheid worden vaak als niet-acceptabel beschouwd. Maar net als in de fysieke wereld zijn risico's in het digitale domein nooit volledig uit te bannen. Het streven naar een bepaald niveau van cyberweerbaarheid betekent dat bepaalde risico's zullen moeten worden geaccepteerd. En de vraag die hierdoor wordt opgeroepen, is welke risico's en daaruit voortvloeiende schade we als samenleving bereid zijn te accepteren.

4 Maatregelen

Tijdens de twee workshops die zijn gehouden in het kader van dit onderzoek, is uitvoerig ingegaan op mogelijke maatregelen om de weerbaarheid van de Nederlandse samenleving tegen cyberdreigingen te versterken. In dit hoofdstuk passeren deze maatregelen de revue. Daarbij worden verschillende soorten maatregelen onderscheiden: maatregelen om mediawijsheid te vergroten; maatregelen met het oog op de beveiliging van burgers, bedrijven, vitale sectoren en overheid; wettelijke maatregelen; en maatregelen op het gebied van expertise, capaciteit en budget. Dergelijke maatregelen vragen (financiële) investeringen van met name de overheid. Dit hoofdstuk gaat daarnaast in op de kansen die deze investeringen bieden voor de Nederlandse economie. Ook beschrijft dit hoofdstuk de positie van Nederland in het internationale speelveld en relevante internationale afspraken om cyberaanvallen te kunnen weren.

4.1 Mediawijsheid vergroten

Uit het vorige hoofdstuk werd duidelijk dat burgers vaak onvoldoende inzicht hebben in de risico's die ze lopen door nieuwe aanvalsmethoden van criminelen als ransomware en spear phishing. Daarnaast maken ze onvoldoende gebruik van basale beveiligingsmaatregelen als sterke wachtwoorden en back-ups.

Om burgers 'mediawijs' te maken – het bewustzijn op cyberrisico's en daartegen te nemen maatregelen te vergroten – lijkt er veel voor te zeggen om in het onderwijs meer aandacht te besteden aan cybersecurity en digitale vaardigheden. Verhagen pleit er bijvoorbeeld voor om digitale geletterdheid, inclusief aandacht voor cybersecurity, zo snel mogelijk op te nemen in het kerncurriculum voor basis- en voortgezet onderwijs (Verhagen 2016). Anderen onderkennen weliswaar de behoefte aan mediawijsheid van – vooral – jongeren, maar waarschuwen ervoor het onderwijs hier al te veel mee te belasten.

Een tweede mogelijkheid om burgers mediawijs te maken, is gebruik te maken van voorlichtingscampagnes. Die voorlichtingscampagnes kunnen zowel door de overheid worden gevoerd als door het bedrijfsleven of een organisatie als de Consumentenbond. Zo heeft de Betaalvereniging Nederland met de voorlichtingscampagne 'Hang op! Klik weg! Bel uw bank!' klanten bewuster gemaakt van de risico's op fraude met internetbankieren en hoe zij daarmee kunnen omgaan (NVB 2016).

Maar er kan niet te veel worden verwacht van de digitale vaardigheden van de burger. Veel burgers hebben nu al moeite om hun computer en smartphone adequaat te beveiligen. Beveiliging van de stroom aan niet of slecht beveiligde slimme apparaten die met de opkomst van het Internet of Things de markt overspoelen, zal voor de meeste burgers te veel zijn gevraagd.

In dit verband is de vraag van belang of het wel zo nodig en – uit veiligheidsoogpunt – zo verstandig is om allerlei huishoudelijke en andere apparatuur uit te rusten met een internetverbinding.

4.2 Beveiligingsmaatregelen

4.2.1 Basisbeveiliging op orde brengen

De eerste stap voor het versterken van de weerbaarheid tegen cyberaanvallen is het op orde brengen van de basisbeveiliging. Dat geldt niet alleen voor burgers, maar ook voor het bedrijfsleven, de overheid en de vitale infrastructuur. Naast reeds genoemde maatregelen als het tijdig installeren van software-updates, het gebruik van sterke wachtwoorden en het maken van back-ups van belangrijke bestanden, kan worden gedacht aan het gebruik van zogeheten tweefactor-authenticatie of versleuteling van belangrijke data.

Het MKB zou voor het nemen van beveiligingsmaatregelen gebruik kunnen maken van door ICT-leveranciers aangeboden clouddiensten. Deze leveranciers bieden een totaalpakket aan maatregelen aan waarmee de ondernemer de zorg voor veiligheid uit handen wordt genomen. Clouddiensten kunnen innovatieve en gemakkelijk toegankelijke security-oplossingen bieden, waarbij rekenkracht, security-applicaties en kennis over cyberdreigingen worden gebundeld (PwC 2016). Ze zijn een voorbeeld van security-as-a-service.

Het uitbesteden van beveiligingsmaatregelen vraagt wel om een kosten-risicoafweging door het betreffende bedrijf. En dat vraagt weer om voldoende inzicht in de eigen bedrijfsprocessen, in de daarvoor essentiële data, in de risico's die een bedrijf loopt bij een hack en of het pakket aan maatregelen voldoende is toegesneden op de specifieke situatie van het bedrijf. Het bedrijf moet daarnaast voldoende vertrouwen hebben in de aanbieder van de diensten om daaraan de beveiliging van cruciale bedrijfsgegevens te delegeren (PwC 2016).

Cyberveiligheid bestaat niet alleen uit het nemen van technische maatregelen, maar is tevens een organisatorische aangelegenheid. Zo is het van belang dat binnen een bedrijf of organisatie een open meldcultuur bestaat, zodat medewerkers zonder angst voor represailles veiligheidsincidenten kunnen melden (KPMG 2013).

4.2.2 Aandacht voor detectie en respons

Alleen het treffen van maatregelen die aanvallers buitenhouden, volstaat in veel gevallen niet. Een volhardende of geavanceerde hacker lukt het vroeg of laat om binnen te komen. Daarom is het noodzakelijk om te weten welke processen en informatie essentieel zijn voor de bedrijfsvoering en om hiervoor specifieke maatregelen te treffen.

Om afwijkende patronen te kunnen detecteren en in te grijpen als dat nodig is, moeten bedrijven aandacht geven aan de monitoring van kritische processen. Banken hebben bijvoorbeeld de fraude met internetbankieren fors kunnen terugdringen door in te zetten op snelle detectie van verdachte transacties.

Ook is van belang dat bedrijven weten hoe ze moeten reageren als ze bijvoorbeeld te maken krijgen met een besmetting met ransomware of een DDoS-aanval, en wat ze in een dergelijke situatie moeten doen om de bedrijfsvoering zo snel mogelijk te herstellen.

4.2.3 Opzetten van Digital Trust Centrum

Een belangrijke vraag is welke beveiligingsmaatregelen voor welk bedrijf of voor welk type bedrijf passend zijn. De bakker op de hoek werkt met andersoortige data en loopt andere risico's dan bedrijven die werken met hoogwaardige technologie of bedrijven met een volledig internetgebaseerde bedrijfsvoering, zoals webwinkels. Maar, zoals eerder duidelijk werd, veel bedrijven hebben niet de kennis en vaardigheden in huis om te weten welke beveiligingsmaatregelen nodig zijn of welke cloud- of andere diensten voor hen het meest geschikt zijn. Ze hebben dan ook grote behoefte aan een onafhankelijk advies.

Meerdere gesprekspartners pleiten voor meer publiek-private samenwerking en informatie-uitwisseling. In dit verband wordt vaak verwezen naar de ondersteunende en adviserende rol die het NCSC binnen het kader van de ISAC's biedt aan bedrijven en organisaties die vitale infrastructuur beheren. Maar het is de vraag of de aanpak met ISAC's wel geschikt is voor mkb-bedrijven. Regelmatig overleg in een vertrouwelijke setting lijkt meer te passen bij sectoren met een beperkt aantal grotere bedrijven, zoals in de financiële of energiesector het geval is, dan met grote aantallen kleinere bedrijven.

Vanuit het MKB wordt dan ook gepleit voor een Digital Trust Centrum. Dit kenniscentrum zou een adviserende en ondersteunende functie kunnen vervullen voor het MKB. Het centrum zou gebruik moeten kunnen maken van de expertise van het NCSC. Vanwege het grote aantal mkb-bedrijven zouden de brancheorganisaties hierbij een schakelfunctie kunnen vervullen, zodat de specifieke informatie die van toepassing is op verschillende branches, kan worden doorgegeven aan de brancheleden. Omdat brancheorganisaties over het algemeen kleine organisaties zijn, zou de overheid hierin een stimulerende en faciliterende rol moeten spelen. Ook het grotere bedrijfsleven dat geen deel uitmaakt van de vitale sectoren, zou gediend kunnen zijn met zo'n expertise- en adviescentrum.

4.2.4 Versterking weerbaarheid vitale infrastructuur

De overheid zou volgens diverse gesprekspartners een actievere rol kunnen spelen bij het versterken van de weerbaarheid van de vitale infrastructuur tegen cyberdreigingen. Die weerbaarheid blijkt immers niet altijd op orde en de vitale sectoren dienen wel een breder, publiek belang. Aanvallen op de vitale infrastructuur kunnen immers leiden tot ernstige maatschappelijke en economische ontwrichting.

Daarbij is de vraag hoe de overheid die actievere rol moet invullen. Volgens verschillende gesprekspartners zal een dwingende aanpak met specifieke, voorgeschreven veiligheidsnormen, niet werken. De sectoren zijn daarvoor te divers en de normen zijn nooit specifiek genoeg. Er lijkt dan ook meer te zeggen voor lichtere maatregelen, zoals het maken van afspraken over jaarlijks uit

te voeren hacktesten. Daarin kunnen ook de nieuwste inzichten over actuele cyberdreigingen worden meegenomen.

4.2.5 Voorbeeldrol overheid

Ook de overheid moet de basisbeveiliging op orde hebben. Bovendien is de overheid als afnemer van beveiligingsproducten en -diensten een belangrijke speler in het veld. Ze neemt in Nederland circa 30 procent van de beveiligingsproducten en -diensten af. Vanwege deze sleutelpositie is het van groot belang dat de overheid op een goede manier inkoopt, en daarmee een voorbeeldrol vervult (CPB 2016; Ministerie van Economische Zaken 2016).

Dat laatste is niet altijd het geval. De overheid heeft de basisbeveiliging niet altijd op orde en cyberveiligheid is nog te vaak een sluitpost op de begroting. Diverse gesprekspartners pleiten dan ook voor een ambitieuzere overheid, die zich sterker laat gelden als vernieuwer en *launching customer*. De inkoop van de overheid op het domein van cybersecurity kan bijvoorbeeld sterker worden gebundeld. Dat leidt zowel tot meer kennisopbouw in huis als tot het ‘uitdagen’ van marktpartijen tot meer innovatie (Hendriks et al. 2016). Ook kan de overheid een duidelijker integrale strategie uitzetten en sterker regie voeren op het nemen van adequate beveiligingsmaatregelen. Wel veronderstelt dit dat de overheid voldoende eigen expertise heeft.

Om tot meer coördinatie en daadkracht binnen de overheid te komen, hebben de gesprekspartners verschillende suggesties gedaan. Deze reiken van aanstelling van een hoge functionaris of aparte minister voor cybersecurity tot meer interdepartementale samenwerking tot de instelling van een ministerieel topteam onder leiding van de minister-president. Tijdens de tweede workshop werd opgemerkt dat recentelijk, onder andere naar aanleiding van het rapport van Verhagen (2016), de eerste stappen in deze richting worden gezet, door sterker in te zetten op interdepartementale samenwerking.

4.3 Wettelijke maatregelen

4.3.1 Uitbreiding bevoegdheden inlichtingen- en opsporingsdiensten

Om beter op te kunnen treden tegen cyberspionage en manipulatie van informatie door statelijke actoren pleit de AIVD voor ruimere bevoegdheden om het internetverkeer te kunnen onderscheppen. Daarmee kunnen verdachte patronen eerder worden gesignaleerd. Het voorstel voor deze modernisering van de Wet op de inlichtingen- en veiligheidsdiensten (Wiv) is in december 2016 besproken in de Tweede Kamer. In februari 2017 stemde de Tweede Kamer in met het wetsvoorstel en de Nota van wijzigingen (Kamerstukken II 2016-2017a). De wet moet nog door de Eerste Kamer worden behandeld.

Volgens Ronald Prins, directeur van beveiligingsbedrijf Fox-IT, is de voorgestelde uitbreiding van de bevoegdheden van de Nederlandse inlichtingen- en veiligheidsdiensten ‘bittere noodzaak’ (NOS 2015). De AIVD speelt een belangrijke rol bij de verdediging tegen digitale spionage door statelijke actoren. Met de modernisering van de Wiv zou volgens Prins de slagkracht tegen cybercriminaliteit

en -spionage aanzienlijk winnen (Prins 2016). Ook Verhagen is van mening dat de huidige wettelijke bevoegdheden van de inlichtingen- en veiligheidsdiensten tekortschieten om cybersecurity in Nederland goed op peil te krijgen, en dat uitbreiding ervan nodig is (Verhagen (2016).

Maar er klinkt ook kritiek op het wetsvoorstel, bijvoorbeeld door de Raad van State en de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD). Hoewel beide organisaties de noodzaak onderkennen van uitbreiding van de bevoegdheden van de inlichtingendiensten, uiten ze kritiek op de wijze van toezicht op de uitoefening van die bevoegdheden, zoals deze in het wetsvoorstel is vastgelegd. De Raad van State uit 'ernstige twijfels' over de effectiviteit van het toezicht (RVS 2016). De CTIVD geeft aan dat het wetsvoorstel weliswaar betere waarborgen kent dan de huidige wet, waaronder voorafgaande toestemmingsverlening, maar dat deze waarborgen niet toereikend zijn gezien de reikwijdte van de nieuwe bevoegdheden. De Nota van wijziging biedt op dit punt wel verbeteringen, maar die zijn in de ogen van de CTIVD nog steeds onvoldoende. Het wetsvoorstel biedt te weinig toetsbare normen, hetgeen effectief toezicht bemoeilijkt (CTIVD 2016; 2017).

De CTIVD is daarnaast bezorgd over de rechtspositie van de burger met het oog op informatie-uitwisseling met buitenlandse diensten. De toezichthouder beschouwt dit als een 'ernstig hiaat' in de rechtsbescherming van burgers (CTVID 2017). Dit punt kwam ook naar voren tijdens een expertmeeting van de Eerste Kamer over cyberintelligence in 2014. Het is niet altijd duidelijk of gegevens van Nederlandse burgers bij samenwerkingsrelaties met buitenlandse diensten voldoende zijn beschermd. Ook is het voor burgers moeilijk om zich te verweren tegen onterechte verdenkingen door inlichtingendiensten (Rathenau Instituut 2014; Kamerstukken I 2013-2014).

Het wetsvoorstel is in februari 2017 door de Tweede Kamer aangenomen met een amendement en een aantal moties. De regering wordt in de moties verzocht om de CTIVD de risico's van gegevensuitwisseling met buitenlandse inlichtingendiensten te laten onderzoeken, en de CTIVD te laten rapporteren over de gevolgen van een bewaartermijn voor gegevens van drie jaar voor de bescherming van de persoonlijke levenssfeer (Kamerstukken II 2016-2017d; Kamerstukken II 2016-2017e). Ook wordt de regering gevraagd om een zo gericht mogelijke inzet van de verruimde bevoegdheden (Kamerstukken II 2016- 2017f).

Behalve de inlichtingendiensten willen ook de opsporingsdiensten ruimer toegang krijgen tot communicatie via het internet. Maar de toenemende versleuteling van het internetverkeer vormt daarvoor een belemmering. De diensten willen dan ook gebruik kunnen maken van *zero-days.* Een *zero-day* is een kwetsbaarheid in soft- of hardware die ontdekt is, maar waarvoor nog geen beschermingsmaatregelen zijn getroffen. De opsporingsdiensten kunnen met behulp van deze zero-days in computers van verdachten inbreken ('terughacken').

Het wetsvoorstel Computercriminaliteit III moet dit terughacken mogelijk maken. In december 2016 is dit wetsvoorstel in de Tweede Kamer behandeld en, met enkele aanpassingen, aangenomen (Kamerstukken II 2015-2016). Ook dit voorstel is niet onomstreden. Critici hebben erop gewezen dat zolang deze zero-day kwetsbaarheden niet worden gemeld bij de softwareproducent, ook andere partijen hiervan gebruik kunnen maken, zoals cybercriminelen. Om aan deze kritiek

tegemoet te komen, is een amendement van de Kamerleden Recourt en Tellegen aangenomen. Het amendement regelt dat de officier van justitie het gebruik van zero-days door opsporingsdiensten moet melden bij de softwareproducent en die melding alleen in geval van een ‘zwaarwegend opsporingsbelang’ mag uitstellen (Kamerstukken II 2016-2017c). Ook is een motie aangenomen van het Kamerlid Recourt waarin aan de regering wordt gevraagd om zero-days alleen ‘in het uiterste geval’ te gebruiken (Kamerstukken II 2016-2017b).

4.3.2 Handhaving en toezicht

Hoofdstuk 2 beschreef hoe met de opkomst van het Internet of Things steeds meer apparaten op de markt komen die met het internet worden verbonden, van routers tot babyfoons en slimme poppen. De beveiliging hiervan is vaak niet op orde. De producten zijn bijvoorbeeld uitgerust met een standaardwachtwoord of er is überhaupt geen wachtwoord nodig.

In de praktijk ligt de verantwoordelijkheid voor de beveiliging van deze apparaten daardoor bij de consument. Ze worden bijvoorbeeld geacht het standaardwachtwoord direct te veranderen, consequent updates uit te voeren en wachtwoorden regelmatig aan te passen. In de praktijk doen burgers dit lang niet altijd. Dit probleem wordt alleen maar groter naarmate consumenten meer ‘slimme’ apparaten aanschaffen (Eskens et al. 2016).

Een veelgenoemde optie die zou moeten voorzien in deze beveiligingslacune, is invoering van een keurmerk voor veilige apparaten. Daarmee zouden onveilige apparaten van de markt kunnen worden geweerd. Maar een wettelijk opgelegd keurmerk zal waarschijnlijk niet werken. Wetgevingstrajecten nemen namelijk te veel tijd in beslag en de technologische ontwikkelingen op het gebied van ICT gaan te snel. Voordat een wet van kracht is geworden, zijn daarin omschreven veiligheidseisen alweer achterhaald. Ook de grote hoeveelheid nieuwe ICT-producten die wekelijks op de markt komen, maken de uitvoerbaarheid van een keurmerk lastig.

Meer kans van slagen heeft de mogelijkheid om in wetgeving een minimumbeveiligingsniveau als ‘open norm’ vast te leggen, in combinatie met actief toezicht om dit minimumniveau in de praktijk nader invulling te geven en te handhaven. Een dergelijke open norm wordt vaker gebruikt in wetgeving. Zo is in de Wet bescherming persoonsgegevens een open norm voor de beveiliging van persoonsgegevens vastgelegd. Organisaties die persoonsgegevens verwerken, moeten ‘passende technische en organisatorische maatregelen’ nemen om persoonsgegevens te beveiligen tegen verlies of onrechtmatige verwerking. Het College Bescherming Persoonsgegevens (CBP) heeft ook richtsnoeren uitgebracht voor de beveiliging van persoonsgegevens en ziet toe op de naleving daarvan (CBP 2013). Recent wees de Autoriteit Persoonsgegevens (AP; de opvolger van het CBP) ziekenhuizen erop dat de beveiliging van veel patiëntenportalen tekortschoot (AP 2016). Omdat voor medische gegevens het hoogste betrouwbaarheidsniveau is vereist, moeten ziekenhuizen gebruikmaken van zogeheten tweefactor-authenticatie. Het AP heeft laten weten ervan uit te gaan dat ziekenhuizen hier gevolg aan geven. Zo niet, dan zal het AP handhavende maatregelen nemen.

In Amerika is de Amerikaanse Federal Trade Commission (FTC) een voorbeeld van actief toezicht op het gebied van ICT. De FTC besloot in 2015 om privacy en veiligheid van met het internet

verbonden apparaten tot speerpunt te maken en publiceerde daartoe richtlijnen voor de beveiliging van apparaten (FTC 2015). Op basis van een wettelijk verbod op misleidende en oneerlijke handelspraktijken klaagde de FTC drie bedrijven aan bij de rechter. De FTC kon namelijk aantonen dat deze bedrijven redelijke stappen en algemeen bekende beveiligingsmaatregelen niet hadden genomen, terwijl de fabrikanten de producten aanprezen als veilig. Het bedrijf ASUS, producent van computeronderdelen, kreeg op grond hiervan door de FTC een audit opgelegd van twintig jaar (FTC 2016).

Het voorbeeld van de FTC roept de vraag op of Nederlandse toezichthouders op een vergelijkbare manier handhavend zouden kunnen optreden tegen onvoldoende beveiligde ICT-apparatuur. Kunnen de Autoriteit Consument en Markt (ACM) of het Agentschap Telecom vanuit hun huidige mandaat optreden tegen onveilige producten? In Nederland kennen we net als in de Verenigde Staten een wet die toeziet op ‘oneerlijke handelspraktijken’. De ACM ziet daarop toe. Hieronder vallen bijvoorbeeld zaken als het maken van misleidende reclame, het niet vermelden van alle bijkomende kosten of het agressief werven van nieuwe klanten. De ACM kan een boete of een last onder dwangsom opleggen, of een combinatie daarvan.

De Consumentenbond heeft eind 2016 de ACM, het AP en de Nederlandse Voedsel- en Warenautoriteit (NWVA) geïnformeerd over onveilige slimme poppen die in de schappen lagen (Consumentenbond 2016d). De poppen hebben een internetverbinding en kunnen terugpraten als kinderen iets tegen ze zeggen. Uit onderzoek van de Noorse consumentenbond bleek dat iedereen met een mobiele telefoon met bluetooth in de buurt van de poppen de gesprekken kon afluisteren en de pop iets kon laten zeggen. De toezichthouders hebben nog niet gereageerd op de actie van de Consumentenbond. Wel heeft Blokker Holding (eigenaar van Bart Smit en Intertoys) de poppen ondertussen uit de schappen gehaald.

4.3.3 Zorgplichten en aansprakelijkheidswetgeving

Een andere mogelijkheid om beter beveiligde producten op de markt te krijgen, is door middel van zorgplichten en aansprakelijkheidswetgeving. De huidige wetgeving kent meerdere zorgplichten toe aan bedrijven ten aanzien van een goede beveiliging. Het gaat hierbij onder andere om bepalingen uit de Wet bescherming persoonsgegevens, het Wetboek van Strafrecht en het Burgerlijk Wetboek. Bedrijven zijn echter vaak onvoldoende op de hoogte van de zorgplichten die gelden en hoe deze in de praktijk invulling krijgen. De Cyber Security Raad publiceert daarom binnenkort een handleiding over zorgplichten op het gebied van cybersecurity. Zo moeten bedrijven die ICT-producten of -diensten aanbieden, ervoor zorgen dat deze voldoen aan relevante beveiligingsstandaarden en dat deze van software-updates kunnen worden voorzien (CSR, nog te verschijnen).

Een andere belangrijke zorgplicht voor bedrijven die ICT-apparaten verkopen is dat producten ‘veilig genoeg’ zijn om normaal te worden gebruikt. In de praktijk is echter niet altijd duidelijk wat dit betekent. Ten tijde van de verkoop van een product mogen er geen bekende beveiligingslekken bestaan. Maar of de klant mag verwachten dat kwetsbaarheden die later aan het licht komen binnen een redelijke tijd worden gerepareerd, hangt af van de omstandigheden (CSR, nog te verschijnen).

De Consumentenbond is inmiddels een rechtszaak tegen Samsung begonnen omdat de fabrikant veel van zijn Android-telefoons niet, of maar voor een korte periode, van updates voorziet. Dat is onrechtmatig, volgens de Consumentenbond. De bond eist dat Samsung minimaal vier jaar na de introductie, of twee jaar na aankoop van een smartphone, updates uitgeeft om de software actueel en veilig te houden (Consumentenbond 2015; 2016a; 2016b).

In Europa is momenteel een Richtlijn in voorbereiding over de 'levering van digitale inhoud'. De voorgestelde richtlijn beoogt uniforme regels op te stellen ten aanzien van consumentenrechten voor digitale diensten en producten. Het voorstel maakt expliciet dat veiligheid, toegankelijkheid en continuïteit, inclusief updates en security patches, onder de plicht vallen rondom 'veilig genoeg voor normaal gebruik' (European Commission 2015).

De combinatie van wettelijk toezicht op de veiligheid van ICT-producten en -diensten in combinatie met aansprakelijkheidswetgeving leidt er mogelijk toe dat op de markt vormen van certificering of keurmerken zullen ontstaan. Bedrijven zullen immers willen voorkomen dat ze door de toezichthouder of de rechter tot de orde moeten worden geroepen. Ook Verhagen (2016) en Hendriks et al. (2016) wijzen op de mogelijkheid van certificering op basis van zelfregulering.

4.3.4 Aangifte en pakkans cybercrime

Hoewel de Nederlandse politie op nationaal niveau een op cybercrime gespecialiseerd Team High Tech Crime (THTC) in huis heeft, komt de bestrijding van cybercrime op regionaal niveau te weinig van de grond. Het belang daarvan wordt regionaal te weinig gevoeld. Dit komt tot uiting in de moeite die burgers en bedrijven ondervinden om bij de (regionale) politie aangifte te doen van cybercrime. Het ontbreekt vaak aan kennis – bijvoorbeeld over ransomware – en vervolging van cybercriminaliteit krijgt weinig prioriteit.

Meerdere gesprekspartners wijzen erop dat de pakkans en vervolging van cybercriminelen omhoog moet. Misdaad moet niet lonen. Van een verhoogde pakkans en kans op vervolging zou zeker voor scriptkiddies en kleinere criminelen een afschrikwekkende werking uitgaan.

Wanneer de politie het aangiftebeleid serieuzer neemt, kan ook een beter beeld ontstaan van de daadwerkelijke problemen en kan cybercriminaliteit gerichter worden bestreden.

4.4 Expertise, capaciteit en budget

4.4.1 Expertiseontwikkeling en capaciteitsversterking

Nederland beschikt op diverse plekken over veel kennis op het gebied van cybersecurity: bij bedrijven als Deloitte en KPN, kennisinstellingen als TNO en de Radboud Universiteit of overheidsorganisaties als het NCSC of het Team High Tech Crime (THTC) van de politie.

Daarnaast stimuleert de Nederlandse overheid onderzoek en innovatie op het gebied van informatiebeveiliging. Zo heeft de Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO) drie cybersecurityprogramma's aangekondigd voor 2017, onder andere in het kader van de Nationale Cyber Security Research Agenda (NCSRA) (NWO 2017). De programma's sluiten aan bij de tweede Nationale Cyber Security Strategie (NCSS) en het op economische innovatie gerichte topsectorenbeleid.

Maar de vraag naar mensen met expertise op het gebied van cybersecurity is veel groter dan het aanbod. Dat geldt niet alleen voor hoger geschoold personeel, maar ook voor vakmensen met een beroepsopleiding (Verhagen 2016; Hendriks et al. 2016). Er is krapte op de arbeidsmarkt, waardoor de partijen met behoefte aan expertise allemaal in dezelfde vijver vissen. De goed gekwalificeerde specialisten zullen vaker kiezen voor het bedrijfsleven, waar ze een hoger salaris kunnen verdienen. Dat gaat ten koste van de kwaliteit van het personeel bij de overheid.

Ook de politie kampt met een gebrek aan expertise. Doordat de politie een relatief minder goed loopbaanperspectief kan bieden aan cybersecurityspecialisten, raakt ze deze kwijt aan grote bedrijven. Als gevolg hiervan ontbeert de politie data-specialisten die een meer omvattende analyse kunnen maken van cybercrime en de drijvende krachten daarachter. Dat gaat ten koste van een effectieve aanpak van cybercriminaliteit.

De vraag naar expertise zal de komende jaren alleen maar toenemen. Dit hangt samen met de grootte van de cyberdreigingen en de snelheid van de technologische ontwikkelingen. Door de snelheid van die ontwikkelingen valt niet te zeggen welke gedaante de dreigingen in de komende jaren zullen aannemen en wat ervoor nodig is om die het hoofd te bieden. Er is dan ook vooral behoefte aan adaptief vermogen.

Meerdere gesprekspartners geven aan dat het van groot belang is om te investeren in cybersecurity-opleidingen en capaciteitsversterking binnen het bedrijfsleven en de overheid. Als dat niet gebeurt, zal het gebrek aan weerbaarheid tegen cyberdreigingen over enkele jaren nog groter zijn dan nu al het geval is.

Een van de gesprekspartners merkt in dit verband op dat hierbij ook meer gebruik zou kunnen worden gemaakt van de expertise die aanwezig is binnen de Nederlandse hacker community. Dat gebeurt nu nog te weinig.

4.4.2 Verhogen budget cybersecurity

Meer investeren in cybersecurity-opleidingen en capaciteitsversterking betekent dat er meer geld door overheid en bedrijfsleven moet worden besteed aan cybersecurity. Diverse gesprekspartners wijzen erop dat Nederland in vergelijking met andere westerse landen weinig investeert in cybersecurity. Ook Verhagen pleit voor een substantieel hoger budget voor cybersecurity (Verhagen 2016).

Anderen wijzen erop dat de nadruk niet alleen moet liggen op het uitgeven van meer geld. Uitbreiding van publiek-private samenwerkingsverbanden, in het kader van de ISAC's of in de vorm van een Digital Trust Centrum, kunnen de weerbaarheid tegen cyberdreigingen substantieel versterken. Dergelijke maatregelen vragen mogelijk maar een beperkte inzet van menskracht en financiële middelen.

4.5 Economische kansen

Meerdere gesprekspartners geven aan dat de ontwikkelingen op het gebied van cybersecurity ook als een kans voor de Nederlandse economie moeten worden gezien. Nederland beschikt met het grootste internetknooppunt ter wereld over snelle breedband telecomnetwerken en is daarmee een belangrijke vestigingsplaats voor ICT-bedrijvigheid. Door de kwaliteit en veiligheid van de ICT-infrastructuur te waarborgen, kan Nederland zijn aantrekkelijkheid vergroten als vestigingsplaats voor ICT-gerelateerde bedrijvigheid (Ministerie van Economische Zaken 2016; PwC 2016).

Daarnaast biedt de ontwikkeling van beveiligingsproducten en -diensten de cybersecuritysector allerlei kansen. Nederland beschikt over een goede uitgangspositie om zich op dit gebied te profileren. Het heeft daarvoor de benodigde specialistische kennis in huis met bedrijven als Fox-IT en Deloitte Nederland en kennisinstellingen als TNO, de Radboud Universiteit en Universiteit van Amsterdam.

Op dit moment wordt de in Nederland aanwezige kennis nog onvoldoende benut. Daarmee laat Nederland (economische) kansen liggen. Om die kansen te grijpen, zouden bedrijven zich sterker moeten profileren met informatiebeveiliging als 'unique selling point' (PwC & VU 2014).

De cybersecuritysector in Nederland groeit overigens sneller dan de gehele ICT-sector. In 2014 was ongeveer 10 procent van de omzet binnen de ICT-sector gerelateerd aan cybersecurity-activiteiten (Hendriks et al. 2016).

4.6 Internationale context

Cybersecurity is niet alleen een Nederlands probleem. Het internet houdt niet op bij de landsgrenzen; cybercriminelen zijn actief over de hele wereld en onveilige apparatuur komt van fabrikanten overal ter wereld. Cyberaanvallen hebben vaak een internationaal karakter. Landen kunnen zowel het doelwit zijn, ze kunnen als middel fungeren voor een aanval (doordat ze botnets hosten), of de bron zijn van de aanval (Nederlandse cybercriminelen kunnen achter een cyberaanval zitten). Daarom vraagt een effectieve aanpak van cyberaanvallen niet alleen om nationale maatregelen, maar ook om internationale afspraken. Deze paragraaf beschrijft de positie van Nederland in het internationale speelveld en relevante internationale afspraken om cyberaanvallen te kunnen weren.

4.6.1 Positie Nederland

Nederland lijkt met betrekking tot dreigingsbeelden over het algemeen redelijk in de pas te lopen met andere landen zoals Duitsland, het Verenigd Koninkrijk, Frankrijk en de Verenigde Staten. Wel valt op dat Nederland relatief veel malafide websites host en dat Nederlandse internetgebruikers steeds vaker worden geconfronteerd met phishing sites en malware hosting sites. Met betrekking tot maatregelen loopt Nederland op een aantal gebieden voorop. Dat geldt voor de publiek-private samenwerking met de ISAC's en voor de innovatieve aanpak van cybercrime door de Nederlandse bankensector.

Nederland zou op haar beurt kunnen leren van andere landen, bijvoorbeeld bij de toepassing en het up-to-date houden van beveiligingsstandaarden. De International Telecom Unit stipt de maatregelen van de Verenigde Staten op het gebied van beveiligingsstandaarden aan als *good practice* (ITU 2015). Een belangrijk onderdeel van deze aanpak is een nationaal raamwerk bestaande uit een set aanbevolen beveiligingsstandaarden voor de industrie en een verzameling *best practices* (NIST 2014). Het raamwerk vormt een leidraad voor organisaties voor detectie van en respons op cybersecurityrisico's. Het National Institute of Standards and Technology (NIST) draagt zorg voor de implementatie van het raamwerk en het up-to-date houden hiervan. In Europa verzorgt het Network and Information Systems (NIS)-platform de facilitering van standaarden.

In Nederland bestaat geen organisatie die zich uitsluitend richt op cybersecuritystandaarden. Wel onderhoudt het Forum Standaardisatie de verplichte open standaarden voor de publieke sector, zoals geformuleerd in de Baseline Informatiebeveiliging Rijksdienst. Daarnaast geeft het NCSC adviezen over beveiligingsnormen aan de Rijksoverheid en de vitale infrastructuur. Het onderzoeksbureau InnoValor heeft in 2015 in opdracht van het ministerie van Veiligheid en Justitie een overzicht en classificatie van standaarden opgesteld (Hulsebosch & Van Velzen 2015). Dit is een hulpmiddel voor de omgang met risico's, maar biedt geen concrete handvatten, zoals de leidraad in de VS. Een ander aandachtspunt is dat het nu in kaart gebrachte raamwerk, evenals de onderliggende standaarden, onderhouden moeten worden om ook in de toekomst bruikbaar te zijn.

De Verenigde Staten besteden ook expliciet aandacht aan dreigingen gerelateerd aan het Internet of Things. Homeland Security heeft strategische principes voor het beveiligen van het Internet of Things gepubliceerd (US Department of Homeland Security 2016). Het gaat om zes niet-bindende richtlijnen voor de industrie en beleidsmakers, waaronder het meenemen van beveiliging in de ontwerpfase van digitale producten of diensten, het stimuleren van security-updates en terughoudend zijn met het verbinden van producten aan het internet. Zoals eerder besproken, heeft ook de Amerikaanse Federal Trade Commission het Internet of Things tot een van haar speerpunten gemaakt.

Ook op het gebied van certificering zou Nederland van andere landen kunnen leren. In tegenstelling tot Estland, Duitsland en het Verenigd Koninkrijk kent Nederland namelijk geen beleid voor certificering van professionals. Zo heeft in Duitsland de Bundesamt für Sicherheit in der Informationstechnik richtlijnen opgesteld voor certificering van cybersecuritybedrijven en professionals (*IT-Grundschutz*) (BSI 2017). Het certificaat kan opdrachtgevers en klanten helpen inzicht te krijgen in de inspanningen die het bedrijf levert op het gebied van cybersecurity. Estland

heeft deze Duitse richtlijnen overgenomen en verplicht gesteld voor publieke organisaties die databases of registers verwerken (ISE 2016). In Europa wordt verkend of certificeringsprogramma's voor ICT-beveiligingsproducten kunnen worden geharmoniseerd (European Commission 2016). Een ICT-bedrijf moet nu in Europese lidstaten verschillende nationale certificeringsprocessen doorlopen om zijn producten en diensten te kunnen verkopen.

In het Verenigd Koninkrijk zijn bedrijven die meedingen naar bepaalde overheidsopdrachten verplicht om te voldoen aan bepaalde basisbeveiligingsmaatregelen. Het gaat hierbij om opdrachten voor het verwerken van persoonlijke informatie van burgers of ambtenaren of anderszins vertrouwelijke informatie. De maatregelen zijn vastgelegd in het *Cyber Essentials Scheme* (Gov.uk 2014).

4.6.2 Internationale afspraken

Als het ene land maatregelen treft tegen bijvoorbeeld ransomware, zullen criminelen uitwijken naar een ander land waar deze maatregelen niet zijn doorgevoerd. Ook op internationaal niveau vindt een voortdurende wedloop plaats tussen aanvallers en verdedigers. Gezien het 'waterbed'-karakter van deze cyberdreigingen is harmonisatie van afspraken op internationaal niveau van belang. Het European Union Agency for Network and Information Security (ENISA) is daarom voorstander van harmonisering van maatregelen (ENISA 2015).

De Europese Unie heeft recent een aantal initiatieven genomen om de weerbaarheid tegen cyberdreigingen te verbeteren. Zo is in 2016 de Europese richtlijn Netwerk en Informatiebeveiliging (NIB) aangenomen. Het doel van deze richtlijn is om een gemeenschappelijk niveau van netwerkbeveiliging binnen Europa te creëren. Onderdeel hiervan is een betere samenwerking tussen de Cyber Security Incident Response Teams van de verschillende lidstaten (zoals het NCSC in Nederland). Ook verplicht de richtlijn bedrijven die de vitale infrastructuur beheren, inbreuken in hun ICT-systemen te melden. De richtlijn is in augustus 2016 in werking getreden en moet worden geïmplementeerd in nationale wetgeving. De lidstaten hebben daar 21 maanden voor (European Parliament 2016).

Daarnaast is de Algemene Verordening Gegevensbescherming aangenomen. Deze treedt in 2018 in werking. De verordening moet de regels voor omgang met persoonsgegevens harmoniseren. De verordening kent onder andere een verplichte melding van datalekken. Daarnaast krijgen organisaties een documentatieplicht: zij moeten kunnen aantonen dat ze de juiste technische en organisatorische maatregelen hebben genomen om persoonsgegevens te beschermen.

Naast internationale regulering zijn ook internationale kennisontwikkeling en innovaties op het gebied van cybersecurity van belang om cyberdreigingen het hoofd te kunnen bieden. De Europese Commissie maakte in juli 2016 een actieplan op dit gebied bekend. De Commissie steekt 450 miljoen euro in publiek-private samenwerking om innovaties met betrekking tot cybersecurity te stimuleren (European Commission 2016). De verwachting is dat de totale investeringen in 2020 zullen uitkomen op circa 1,8 miljard euro. De financiering komt uit het Europese onderzoeks- en innovatieprogramma Horizon2020.

5 Conclusies en aanbevelingen

5.1 Nederland digitaal

Nederland hoort bij de meest gedigitaliseerde landen ter wereld. Bijna iedereen heeft een computer en meer dan 90 procent van alle huishoudens en bedrijven maakt gebruik van het internet. Digitalisering dringt nagenoeg door tot elk aspect van het leven. De fysieke wereld en het digitale domein raken daardoor steeds sterker met elkaar verweven.

De Nederlandse samenleving en economie worden daarmee meer en meer afhankelijk van een goed functionerende ICT-infrastructuur en -dienstverlening. Diefstal of manipulatie van gegevens of uitval van ICT-structuren kunnen grote gevolgen hebben voor het maatschappelijke en economische verkeer. De groeiende afhankelijkheid van ICT maakt de Nederlandse samenleving dan ook kwetsbaar op dit gebied.

Dit roept de vraag welk vermogen de Nederlandse samenleving en economie hebben om cyberbedreigingen het hoofd te bieden. Behoeft deze digitale weerbaarheid versterking en zo ja, welke maatregelen moeten daarvoor worden genomen? Om deze vraag te beantwoorden, gaf hoofdstuk 2 een overzicht van de belangrijkste cyberdreigingen. Hoofdstuk 3 beschreef de mate van weerbaarheid van diverse sectoren tegen deze dreigingen en hoofdstuk 4 schetste mogelijke maatregelen om de dreigingen beter het hoofd te kunnen bieden.

Dit hoofdstuk zet de belangrijkste conclusies op een rij en geeft aanbevelingen op verschillende niveaus aan met name de overheid en het bedrijfsleven.

5.2 Conclusies

5.2.1 Toename van cyberdreigingen

Alles waar ICT in zit, valt in beginsel te hacken. De groeiende afhankelijkheid van ICT maakt digitale producten en processen een aantrekkelijk doelwit voor cybercriminelen, cyberspionnen en andere hackers. Computerprogramma’s bestaan uit vele, soms miljoenen regels code, waar onvermijdelijk fouten en onvolkomenheden in sluipen. Deze kwetsbaarheden kunnen door kwaadwillende partijen worden misbruikt. De motieven daarvoor lopen uiteen: van politiek-gemotiveerde spionage door statelijke actoren tot ransomware-aanvallen door cybercriminelen om geldelijk gewin en hacks uit baldadigheid door puberende scriptkiddies.

De grootste dreiging gaat uit van buitenlandse inlichtingendiensten en daaraan gelieerde hackersgroepen. Vooral Russische en Chinese inlichtingendiensten verzamelen op grote schaal informatie over politieke, militaire en technologische onderwerpen. Ze gaan hierbij zeer professioneel te werk en beschikken over een grote operationele slagkracht. De Rijksoverheid en bedrijven met hoogwaardige technologie zijn structureel doelwit van digitale spionage-aanvallen.

Statelijke actoren richten zich ook meer en meer op manipulatie van informatie, om daarmee bijvoorbeeld de publieke opinie of het politieke klimaat in een ander land te beïnvloeden.

Daarnaast ontwikkelt cybercriminaliteit zich steeds meer tot een vorm van georganiseerde misdaad. Cybercriminelen worden professioneler, de door hen gebruikte methoden geavanceerder en hun verdienmodel winstgevender. Botnets worden beter verhuld en criminelen maken steeds vaker gebruik van spear phishing. Vooral het gebruik van ransomware heeft de afgelopen jaren een grote vlucht genomen. Dit treft zowel burgers en bedrijven, maar ook ziekenhuizen steeds vaker. Cybercrime en economische spionage kunnen op den duur het innovatie- en concurrentievermogen van het Nederlandse bedrijfsleven ondergraven.

Ook kleinere criminelen of scriptkiddies vormen een probleem. Doordat op ondergrondse marktplaatsen laagdrempelige middelen voor digitale aanvallen te koop worden aangeboden (cybercrime-as-a-service), kunnen ook minder geavanceerde hackers bijvoorbeeld een DDoS-aanval uitvoeren en daarmee flinke schade veroorzaken.

5.2.2 Weerbaarheid onvoldoende op orde

Zowel de burger, het bedrijfsleven als de overheid nemen vaak onvoldoende maatregelen om bestaande cyberdreigingen het hoofd te bieden. Basale beveiligingsmaatregelen, zoals het updaten van software, het gebruik van sterke wachtwoorden of het maken van back-ups van belangrijke bestanden, worden vaak niet genomen. Ook ontbreekt het burgers, bedrijfsleven en overheid aan inzicht in de precieze risico's waaraan ze blootstaan en in de mogelijkheden om daar iets aan te doen. Risico's blijven daardoor ongrijpbaar en het belang van cybersecurity krijgt onvoldoende prioriteit totdat het een keer echt misgaat. Zeker voor de burger, het MKB en lagere overheden, zoals gemeenten, geldt dat ze de basisbeveiliging vaak niet op orde hebben.

Bedrijven die de vitale infrastructuur beheren en de Rijksoverheid zijn zich vaak bewuster van de risico's die ze lopen en van de maatregelen die ze daartegen kunnen nemen. De vitale sectoren en de Rijksoverheid worden hierbij ondersteund door het NCSC en de AIVD. Zo heeft het NCSC in samenwerking met het bedrijfsleven Information Sharing and Analysis Centres (ISAC's) opgericht. Binnen deze publiek-private samenwerkingsverbanden wisselen bedrijven onderling informatie en ervaringen uit over cybersecurity. Met deze aanpak loopt Nederland internationaal voorop.

De vitale sectoren verschillen overigens in hun weerbaarheidsniveau. Terwijl de energie-, telecom- en financiële sector hun weerbaarheid redelijk goed op orde lijken te hebben, geldt dat niet voor alle sectoren.

Ook de Rijksoverheid heeft de beveiliging niet altijd op orde. Zo zijn er problemen met het uitfaseren van verouderde computerprogramma's en voldoet het authenticatiesysteem DigiD al enige jaren niet aan de beveiligingsnormen van het NCSC. Daarnaast vormt cybersecurity in aanbestedingsprocedures nog te vaak een sluitpost. Als belangrijke afnemer van beveiligingsproducten en -diensten zou de overheid juist een voorbeeldrol moeten vervullen. De overheid heeft hiervoor echter niet altijd voldoende expertise in huis.

Het Internet of Things versterkt kwetsbaarheid

Door de opkomst van het Internet of Things worden steeds meer ‘slimme’ apparaten met het internet verbonden. De beveiliging van deze smart devices is vaak niet op orde, wat ze kwetsbaar maakt voor cyberaanvallen. En omdat het aantal slimme apparaten dat op de markt verschijnt fors in aantal toeneemt, neemt het aanvalsvlak voor cybercriminelen enorm toe.

Een hack van een met het internet verbonden apparaat houdt niet alleen risico’s in voor de individuele eindgebruiker, bijvoorbeeld omdat persoonlijke gegevens worden gestolen of gemanipuleerd. Wanneer gehackte apparaten worden ingezet voor grootschalige DDoS-aanvallen, kunnen ook overheidsdiensten of de vitale infrastructuur worden platgelegd. Er zijn de afgelopen tijd aanvallen gesignaleerd die gebruikmaken van honderdduizenden of zelfs miljoenen aan het internet gekoppelde apparaten. Als zo’n aanval maar zwaar genoeg is, zal uiteindelijk elk ICT-systeem dat met het internet is verbonden, platgaan.

Marktfalen

Op dit moment ontbreken de economische prikkels voor ICT-leveranciers om de beveiliging van ICT-apparatuur substantieel te verbeteren. De prijsconcurrentie voor deze apparaten is hoog, maar voor een lage prijs kunnen bedrijven geen goede beveiliging leveren. Omdat gehackte apparaten onder andere kunnen worden ingezet voor een grootschalige DDoS-aanval, kan deze situatie tot grote maatschappelijke en economische schade leiden. Het gebrek aan beveiliging kan dan ook worden beschouwd als ernstig ‘marktfalen’.

Huidige maatregelen volstaan niet

Het is verontrustend dat de burger, het bedrijfsleven en de overheid momenteel hun weerbaarheid tegen cyberdreigingen onvoldoende op orde hebben. Dat is eens te meer het geval vanwege de snelle technologische ontwikkelingen en de steeds geavanceerdere methoden waarvan cybercriminelen en statelijke actoren zich bedienen. De bestaande maatregelen op het gebied van cybersecurity volstaan dan ook niet.

5.3 Aanbevelingen om weerbaarheid te versterken

Het treffen van maatregelen om de weerbaarheid tegen cyberdreigingen te versterken, is van groot belang. Deze paragraaf beschrijft de benodigde maatregelen en verbindt hieraan aanbevelingen voor de betrokken partijen, met name voor de overheid.

5.3.1 Aanbevelingen die bijdragen aan veiligheid

Niet van alle burgers, bedrijven en overheden kan eenzelfde niveau aan kennis en digitale vaardigheden worden verwacht. Bovendien vormt niet iedereen een even waarschijnlijk doelwit voor een bepaald type cyberaanval. De gewone burger of kleine middenstander zal over het algemeen

weinig te duchten hebben van digitale spionage door buitenlandse inlichtingendiensten. En mocht dat toch het geval zijn, dan ontbreekt het hun ten enenmale aan middelen om zich daartegen te verweren. Omgekeerd hebben grotere organisaties, die over meer kennis en middelen beschikken, over het algemeen minder te vrezen van aanvallen door scriptkiddies of kleine criminelen. Wel kunnen zij weer het doelwit vormen van geavanceerde aanvallen door statelijke actoren.

De eerste stap voor het versterken van de weerbaarheid tegen cyberaanvallen is het op orde brengen van de basisbeveiliging, door bijvoorbeeld het tijdig installeren van software-updates, het gebruik van sterke wachtwoorden en het maken van back-ups. Dat geldt niet alleen voor burgers, maar ook voor het bedrijfsleven, de vitale sectoren en overheden. Zolang de basisbeveiliging niet op orde is, hebben andere, verdergaande beveiligingsmaatregelen weinig zin.

Bevorder digitale vaardigheden, maar overvraag burger niet

Er valt veel voor te zeggen om in het onderwijs en door middel van voorlichtingscampagnes meer aandacht te besteden aan cybersecurity om digitale basisvaardigheden van consumenten en burgers te bevorderen. Tegelijkertijd mag hier niet te veel van worden verwacht. Veel burgers hebben nu al moeite om hun computer en smartphone adequaat te beveiligen. Beveiliging van de stroom aan slimme apparaten die met de opkomst van het Internet of Things de markt overspoelen, is voor de meeste burgers te veel gevraagd. De verantwoordelijkheid daarvoor moet dan ook door andere partijen worden opgepakt.

Aanbeveling aan de overheid, het bedrijfsleven en andere partijen zoals de Consumentenbond:
Besteed binnen het onderwijs en in voorlichtingscampagnes meer aandacht aan cybersecurity en de daarvoor benodigde digitale vaardigheden van consumenten en burgers.

Investeer in onafhankelijk kennis- en adviescentrum voor bedrijven

Bij mkb-bedrijven bestaat grote behoefte aan onafhankelijke advisering en ondersteuning ten aanzien van te nemen beveiligingsmaatregelen. Ze hebben maar een beperkt inzicht in de risico's die ze lopen en het ontbreekt hun aan kennis om passende maatregelen te treffen. Het treffen van maatregelen om aanvallers buiten te houden, volstaat vaak niet. Vroeg of laat lukt het hackers om binnen te komen. Daarom is het van belang dat bedrijven weten welke processen en informatie essentieel zijn voor hun bedrijfsvoering, zodat zij daarvoor gerichte maatregelen kunnen treffen.

ICT-leveranciers leveren weliswaar allerlei beveiligingsproducten en -diensten aan, maar mkb-bedrijven zijn vaak onvoldoende in staat te beoordelen of die producten en -diensten voor hun situatie een goede oplossing bieden. De bakker op de hoek loopt immers andere risico's dan hightech bedrijven of webwinkels.

Vanuit het MKB wordt dan ook gepleit voor een Digital Trust Centrum. Dit kenniscentrum kan een adviserende en ondersteunende functie vervullen voor het MKB. Daarbij is van belang dat dit centrum gebruik kan maken van de expertise van het NCSC. Vanwege het grote aantal mkb-

bedrijven zouden brancheorganisaties hierbij een schakelfunctie kunnen vervullen. Ook het grotere bedrijfsleven dat geen deel uitmaakt van de vitale sectoren, zou gediend zijn met zo'n onafhankelijk expertise- en adviescentrum.

Aanbeveling aan de overheid en het bedrijfsleven:
Investeer in een onafhankelijk kennis- en adviescentrum voor mkb-bedrijven en grotere bedrijven die geen deel uitmaken van de vitale sectoren.

Bescherm vitale sectoren door hacktest

De bedrijven die de vitale infrastructuur beheren, zijn divers van aard en verschillen in hun weerbaarheidsniveau. Terwijl een bedrijf als TenneT of banken vergaande maatregelen hebben getroffen om hun primaire proces – levering van elektriciteit, geldverkeer – te beveiligen, lijken andere bedrijven hun beveiliging minder op orde te hebben. Hierbij speelt een spanning tussen het commerciële bedrijfsbelang, waardoor investeringen in beveiliging onaantrekkelijk kunnen zijn, en het publieke belang, dat gebaat is bij de continuïteit van vitale processen.

Om de weerbaarheid van achterblijvende vitale sectoren te versterken, lijkt een actievere rol van de overheid wenselijk. Dit hoeft niet te leiden tot een van bovenaf opgelegde aanpak met voorgeschreven, specifieke veiligheidsmaatregelen. Daarvoor verschillen de sectoren te veel van elkaar. Wat de overheid wel kan doen, is sectoren sterker aanspreken op hun verantwoordelijkheid voor een veilige bedrijfsvoering. Ze kan bijvoorbeeld met de sectoren afspraken maken over een jaarlijks uit te voeren hacktest. En als die afspraken niet werken, kan de overheid overgaan tot het wettelijk verplichten van een dergelijke hacktest.

Aanbeveling aan de overheid:
Spreek de vitale sectoren sterker aan op hun verantwoordelijkheid voor een veilige bedrijfsvoering, bijvoorbeeld door afspraken te maken over een jaarlijkse hacktest.

Geef als overheid het goede voorbeeld

Ook de weerbaarheid van de overheid behoeft versterking. De overheid neemt in Nederland circa 30 procent van de beveiligingsproducten en -diensten af en is daarmee een belangrijke speler in het veld. Dit vraagt van de overheid dan ook een ambitieuzere rol. De overheid dient een voorbeeldrol te vervullen door zich sterker te laten gelden als vernieuwer en 'launching customer'. Dat vereist dat de overheid voldoende expertise op het gebied van cybersecurity in huis heeft. Bovendien vereist het een sterkere regie binnen de overheid. De verantwoordelijkheid voor cybersecurity is nu te veel versnipperd. Een sterkere regie maakt het mogelijk om binnen de diverse overheidsorganisaties het beveiligingsniveau te verhogen. Daarbij kan geleerd worden van de ervaringen in bijvoorbeeld de Verenigde Staten of het Verenigd Koninkrijk met beveiligingsstandaarden en certificering van ICT-bedrijven.

Aanbeveling aan de overheid:
Geef het goede voorbeeld als 'launching customer' en stuur binnen de overheid sterker aan op adequate beveiligingsmaatregelen.

5.3.2 Aanbevelingen voor wettelijke maatregelen

De overheid beschikt over diverse wettelijke mogelijkheden om cybercrime en cyberspionage aan te pakken en om onveilige ICT-producten van de markt te weren. Maar het is niet altijd duidelijk hoe ver deze mogelijkheden reiken. Ook zijn ze niet altijd onomstreden.

Verbeter aangiftebeleid en vervolging cybercrime

Op het gebied van aangifte en opsporing kan de overheid winst behalen. Voor burgers en bedrijven is het lastig om een aangifte te doen van cybercrime. Er is weinig kennis aanwezig bij de regionale politie en dergelijke aangiften krijgen vaak geen prioriteit. Betere mogelijkheden voor het doen van aangifte zouden de pakkans en de kans op vervolging verhogen. Zeker voor scriptkiddies en kleinere criminelen kan hiervan een afschrikwekkende werking uitgaan.

Aanbeveling aan de overheid:
Maak meer werk van het aangiftebeleid op regionaal niveau en van vervolging van cybercrime.

Monitor ‘checks and balances’ verruimde bevoegdheden opsporings- en inlichtingendiensten

Om de pakkans en kans op vervolging te verhogen, heeft de regering het wetsvoorstel Computercriminaliteit III ingediend. Het wetsvoorstel moet het voor opsporingsdiensten mogelijk maken om in te breken in computers van verdachten (‘terughacken’). Het voorstel stelt voorwaarden aan het hiervoor benodigde gebruik door opsporingsdiensten van zero-day kwetsbaarheden. Dit laatste heeft de nodige discussie losgemaakt. Ook cybercriminelen kunnen immers van zero-days gebruikmaken om zich toegang te verschaffen tot ICT-systemen. De discussie spitst zich toe op de voorwaarden voor het gebruik door opsporingsdiensten van zero-days. De toekomst moet uitwijzen of de in het wetsvoorstel opgenomen ‘checks and balances’ afdoende zijn.

Aanbeveling aan de overheid:
Monitor of de in het wetsvoorstel Computercriminaliteit III opgenomen voorwaarden voor het gebruik van zero-day kwetsbaarheden door opsporingsdiensten in de praktijk afdoende zijn.

De versterking van de weerbaarheid van vitale sectoren en de Rijksoverheid tegen cyberspionage en manipulatie van informatie door statelijke actoren, vraagt om uitbreiding van de capaciteit en bevoegdheden van de AIVD. Ruimere bevoegdheden geven de dienst de mogelijkheid om het internetverkeer op grotere schaal te monitoren en verdachte patronen te signaleren. Het wetsvoorstel modernisering van de Wet op de inlichtingen- en veiligheidsdiensten moet deze uitbreiding van bevoegdheden mogelijk maken.

Ook dit wetsvoorstel is niet onomstreden. Het zou volgens critici onvoldoende voorzien in een afdoende en voldoende onafhankelijk toezicht op het gebruik door de diensten van hun (ruimere)

bevoegdheden. Een ander kritiekpunt is de bescherming van de rechtspositie van de burger. De burger zou over te weinig juridische mogelijkheden beschikken om zich te verweren tegen onterechte verdenkingen. Ook voor dit wetsvoorstel geldt dat de toekomst moet uitwijzen of de opgenomen ‘checks and balances’ afdoende zijn.

Aanbevelingen aan de overheid:
Breid de capaciteit van de AIVD uit, zodat ze beter in staat is om cyberspionage en manipulatie van informatie door statelijke actoren te signaleren en passende maatregelen te (laten) treffen.

Monitor of de ‘checks and balances’ in het wetsvoorstel modernisering van de Wet op de inlichtingen- en veiligheidsdiensten in de praktijk afdoende zijn.

Formuleer ‘open normen’ in wetgeving voor beveiligingseisen producten

Er verschijnen steeds meer onvoldoende beveiligde slimme apparaten op de markt. Vanwege de daarmee gepaard gaande veiligheidsrisico’s wordt regelmatig gepleit voor wettelijke maatregelen om slecht beveiligde apparaten van de markt te weren, bijvoorbeeld door invoering van een keurmerk. Door de snelle technologische ontwikkelingen op het gebied van ICT zullen voorgeschreven beveiligingsvereisten echter al bij invoering achterhaald zijn.

Een minimumbeveiligingsniveau als ‘open norm’ in wetgeving vastleggen, lijkt meer kans van slagen te hebben. Een toezichthouder kan hier nader invulling aan geven en kan op naleving hiervan actief toezien. Een dergelijke open norm wordt vaker gebruikt, bijvoorbeeld door de Nederlandse Autoriteit Persoonsgegevens (AP) of de Amerikaanse Federal Trade Commission (FTC). Zo is in de Wet bescherming persoonsgegevens vastgelegd dat bedrijven en organisaties ‘passende technische en organisatorische maatregelen’ moeten nemen om persoonsgegevens te beveiligen tegen verlies of onrechtmatige verwerking. Op grond van deze norm wees de AP ziekenhuizen erop dat de beveiliging van veel patiëntenportalen tekortschoot. Een dergelijke vorm van toezicht roept de vraag op of andere Nederlandse toezichthouders zoals de Autoriteit Consument en Markt (ACM) of het Agentschap Telecom over voldoende mandaat en capaciteit beschikken om op te kunnen treden tegen het op de markt brengen van onveilige digitale producten.

Een tweede mogelijkheid om onbeveiligde slimme apparaten te weren, is door middel van zorgplichten en aansprakelijkheidswetgeving. De bestaande wetgeving kent meerdere zorgplichten toe aan bedrijven ten aanzien van een goede beveiliging. Bedrijven zijn echter vaak onvoldoende op de hoogte van de zorgplichten die gelden en hoe deze in de praktijk invulling krijgen. Wanneer toezichthouders sterker inzetten op wettelijk toezicht en naleving van zorgplichten kan daarvan wellicht ook een stimulans uitgaan voor marktpartijen om te komen tot een vorm van zelfregulering, waarbij vormen van certificering of keurmerken kunnen ontstaan.

Als het gaat om onveilige producten wordt op dit moment vooral actie ondernomen door de Consumentenbond. De bond heeft bijvoorbeeld diverse toezichthouders geattendeerd op onveilige

met het internet verbonden poppen, waarop de eigenaar heeft besloten om de poppen uit de schappen te halen. Tevens is de bond een rechtszaak begonnen tegen Samsung, omdat deze veel van zijn Android-telefoons niet, of slechts voor een korte periode, van updates voorziet. Het is van belang dat toezichthouders hierop actiever toezien.

Aanbeveling aan het bedrijfsleven:
Stel je op de hoogte van bestaande zorgplichten en houd je hieraan.

Aanbevelingen aan de overheid:
Leg 'open normen' in wetgeving vast om te kunnen toezien op de beveiliging van slimme apparaten. Laat toezichthouders op basis hiervan actief optreden tegen onveilige ICT-producten.

Ga na of de toezichthouders (AP, ACM, Telecom) voldoende mandaat hebben om op te treden tegen onveilige ICT-producten, en of aanpassing van hun mandaat nodig is. Rust toezichthouders uit met voldoende expertise en capaciteit.

Zie toe op naleving van zorgplichten voor veilige producten door fabrikanten en leveranciers, en ga na of de zorgplichten en aansprakelijkheidswetgeving hiervoor aanpassing behoeven.

5.3.3 Aanbevelingen ten aanzien van expertise en capaciteit

Investeer in expertiseontwikkeling en capaciteitsuitbreiding

Vanwege de snelle technologische veranderingen, de vele ketenafhankelijkheden en de inherente onveiligheid van ICT, is niet te voorspellen welke nieuwe vormen cyberdreigingen de komende jaren aannemen. Zo zijn ransomware en spear phishing relatief nieuwe aanvalsmethoden waarop veel ICT-gebruikers momenteel onvoldoende zijn bedacht, en dus onvoldoende weerbaar tegen zijn. En terwijl de afgelopen jaren de beschermingsmaatregelen tegen DDoS-aanvallen succes begonnen af te werpen, vormen de recente DDoS-aanvallen die gebruikmaken van botnetten bestaande uit honderdduizenden met het internet verbonden apparaten, een belangrijke nieuwe uitdaging. Vooral de steeds geavanceerdere methoden waarvan cybercriminelen en statelijke actoren zich bedienen, baren grote zorgen.

Omdat digitale aanvalsmethoden steeds van vorm veranderen en steeds geavanceerder worden, is de rat race tussen aanvaller en doelwit nooit gelopen. De weerbaarheid tegen cyberdreigingen is dan ook nooit af, maar vergt continu aandacht en investeringen.

Het is verontrustend dat de burger, het bedrijfsleven en de overheid momenteel hun weerbaarheid tegen cyberdreigingen onvoldoende op orde hebben. Er is te weinig expertise en capaciteit om cyberdreigingen het hoofd te bieden. Zoals in de vorige paragrafen al is aangegeven, zouden overheid en bedrijfsleven dan ook meer moeten investeren in expertiseontwikkeling en capaciteitsuitbreiding. Dat geldt voor de volle breedte van het spectrum: van uitbreiding van cybersecurity-opleidingen en ondersteuning van het MKB met een onafhankelijk kennis- en

adviescentrum tot het in huis hebben van voldoende expertise en capaciteit bij de overheid, betrokken toezichthouders en de AIVD. Deze investeringen in expertiseontwikkeling en capaciteitsuitbreiding zijn bovendien nodig om het weerstandsvermogen te versterken met het oog op de nieuwe, moeilijk te voorspellen cyberdreigingen die de Nederlandse samenleving en economie de komende jaren te wachten staan.

Aanbevelingen aan de overheid en het bedrijfsleven:
Investeer in cybersecurity-opleidingen.

Investeer in capaciteitsuitbreiding: een onafhankelijk kennis- en adviescentrum voor het MKB en overig bedrijfsleven (niet-vitale sectoren); voldoende expertise en capaciteit binnen de overheid, betrokken toezichthouders en de AIVD.

5.4 Kansen voor economie

De maatregelen die nodig zijn om de weerbaarheid tegen cyberdreigingen te versterken, vergen de nodige investeringen. Tegelijk bieden deze investeringen kansen voor de Nederlandse economie. Een veiligere ICT-infrastructuur vergroot de aantrekkelijkheid van Nederland als vestigingsplaats voor ICT-bedrijvigheid. Ook bieden de beveiligingsmaatregelen nieuwe kansen voor de Nederlandse cybersecuritysector. Om die kansen te verwezenlijken, is wel van belang dat de kennis die aanwezig is bij bedrijven en kennisinstellingen die in cybersecurity gespecialiseerd zijn, beter wordt benut.

5.5 Leren leven met onveiligheid

100 procent veilig bestaat niet. Dat hangt samen met de snelle technologische ontwikkelingen en de continue wedloop die plaatsvindt tussen aanvaller en doelwit. De dreiging die van een bepaalde aanval uitgaat, hangt af van de mate waarin het beoogde doelwit zich tegen die aanval kan verweren. De inventiviteit van de aanvallende partij, op zoek naar nieuwe kwetsbaarheden en gebruikmakend van nieuwe aanvalsmethoden, staat hierbij tegenover het vermogen van het getroffen doelwit om daar snel op te kunnen reageren.

Voor zowel aanvallers als verdedigers geldt daarbij dat ze een kosten-batenanalyse maken: hoeveel expertise, tijd en geld hebben beide ervoor over om bepaalde baten te behalen (geldelijk gewin, hoogwaardige informatie) of schade te voorkomen? Omdat geld en menskracht altijd een beperkende factor zullen blijven, zijn risico’s in het digitale domein nooit volledig uit te bannen. Net als in de fysieke wereld. Het streven naar een bepaald niveau van cyberweerbaarheid betekent dat bepaalde risico’s zullen moeten worden geaccepteerd. En net als in de fysieke wereld betekent dit dat we in het digitale domein zullen moeten leren leven met een bepaalde mate van onveiligheid.

Zoals deze studie laat zien, laat dit besef onverlet dat maatregelen noodzakelijk zijn om de weerbaarheid van de Nederlandse samenleving en economie tegen cyberdreigingen te versterken.

5.6 Overzicht aanbevelingen

De in dit rapport geformuleerde aanbevelingen zijn in deze slotparagraaf kernachtig samengevat.

Versterking weerbaarheid burgers, bedrijven en overheid

Aanbeveling aan de overheid, het bedrijfsleven en andere partijen zoals de Consumentenbond:

1. Besteed binnen het onderwijs en in voorlichtingscampagnes meer aandacht aan cybersecurity en de daarvoor benodigde digitale vaardigheden van consumenten en burgers.

Aanbeveling aan de overheid en het bedrijfsleven:

2. Investeer in een onafhankelijk kennis- en adviescentrum voor mkb-bedrijven en grotere bedrijven die geen deel uitmaken van de vitale sectoren.

Aanbevelingen aan de overheid:

3. Geef het goede voorbeeld als ‘launching customer’ en stuur binnen de overheid sterker aan op adequate beveiligingsmaatregelen.
4. Spreek de vitale sectoren sterker aan op hun verantwoordelijkheid voor een veilige bedrijfsvoering, bijvoorbeeld door afspraken te maken over een jaarlijkse hacktest.

Wettelijke maatregelen

Aanbeveling aan het bedrijfsleven:

5. Stel je op de hoogte van bestaande zorgplichten en houd je hieraan.

Aanbevelingen aan de overheid:

6. Maak meer werk van het aangiftebeleid op regionaal niveau en van vervolging van cybercrime.
7. Monitor of de in het wetsvoorstel Computercriminaliteit III opgenomen voorwaarden voor het gebruik van *zero-day* kwetsbaarheden door opsporingsdiensten in de praktijk afdoende zijn.
8. Breid de capaciteit van de AIVD uit, zodat ze beter in staat is om cyberspionage en manipulatie van informatie door statelijke actoren te signaleren en passende maatregelen te (laten) treffen.
9. Monitor of de ‘checks and balances’ in het wetsvoorstel modernisering van de Wet op de inlichtingen- en veiligheidsdiensten in de praktijk afdoende zijn.
10. Leg ‘open normen’ in wetgeving vast om te kunnen toezien op de beveiliging van slimme apparaten. Laat toezichthouders op basis hiervan actief optreden tegen onveilige ICT-producten.
11. Ga na of de toezichthouders (AP, ACM, Telecom) voldoende mandaat hebben om op te treden tegen onveilige ICT-producten, en of aanpassing van hun mandaat nodig is. Rust toezichthouders uit met voldoende expertise en capaciteit.
12. Zie toe op naleving van zorgplichten voor veilige producten door fabrikanten en leveranciers, en ga na of de zorgplichten en aansprakelijkheidswetgeving hiervoor aanpassing behoeven.

Expertise en capaciteit

Aanbevelingen aan de overheid en het bedrijfsleven:

13. Investeer in cybersecurity-opleidingen.
14. Investeer in capaciteitsuitbreiding: een onafhankelijk kennis- en adviescentrum voor het MKB en overig bedrijfsleven (niet-vitale sectoren); voldoende expertise en capaciteit binnen de overheid, betrokken toezichthouders en de AIVD.

Bibliografie

AIVD (2016). *Jaarverslag 2015*. Den Haag: Algemene Inlichtingen- en Veiligheidsdienst.

AIVD (2017). 'Economische Cyberspionage'. https://www.aivd.nl/onderwerpen/cyberdreiging/inhoud/economische-cyberspionage

Algemene Rekenkamer (2015a). *Resultaten verantwoordings-onderzoek 2014 Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (VII)*. Den Haag: Algemene Rekenkamer.

Algemene Rekenkamer (2015b). *Resultaten verantwoordings-onderzoek 2014 Ministerie van Infrastructuur en Milieu (XII)*. Den Haag: Algemene Rekenkamer.

Algemene Rekenkamer (2016a). *Staat van de rijksverantwoording 2015: Rijksbrede resultaten verantwoordingsonderzoek*. Den Haag: Algemene Rekenkamer.

Algemene Rekenkamer (2016b). *Resultaten verantwoordingsonderzoek 2015 Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (VII)*. Den Haag: Algemene Rekenkamer.

Algemene Rekenkamer (2016c). *Resultaten verantwoordingsonderzoek 2015 Ministerie van Infrastructuur en Milieu (XII)*. Den Haag: Algemene Rekenkamer.

Alonso, S., 'Brussel voert strijd op tegen Russische desinformatie'. In: *NRC Handelsblad* 24 januari 2017.

Autoriteit Persoonsgegevens (2016). 'Brief aan NVZ over patiëntenportalen'. https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/brief-nvz-patientenportalen.pdf

Beek, M. van, 'Rebelleren tegen foute knuffels'. In: *Het Financieele Dagblad* 1 oktober 2016.

Beurden, P. van, (2016). 'Informatieveiligheid is een issue voor de zorg'. https://www.zorgvisie.nl/personeel/nieuws/2016/10/informatieveiligheid-is-een-issue-voor-de-zorg/

BSI (2017). 'IT-Grundschutz Certification process'. https://www.bsi.bund.de/EN/Topics/ITGrundschutz/ITGrundschutzCertification/itgrundschutzcertification_node.html

CBS (2016). *Veiligheidsmonitor 2015*. Den Haag: Centraal Bureau voor de Statistiek.

College Bescherming Persoonsgegevens (2013). *CPB Richtsnoeren. Beveiliging van persoonsgegevens*. Den Haag: College Bescherming Persoonsgegevens.

Consumentenbond (2016a). ‘Dagvaarding bodemprocedure Consumentenbond / Samsung over Android updates’. https://www.consumentenbond.nl/binaries/content/assets/cbhippowebsite/actie-voeren/updaten/dagvaarding-consumentenbond---samsung-11-nov-2016.pdf

Consumentenbond (2016b). ‘Kort geding Consumentenbond versus Samsung’. https://www.consumentenbond.nl/nieuws/2016/kort-geding-consumentenbond-versus-samsung/

Consumentenbond (2016c). ‘Bodemprocedure tegen Samsung van start’. https://www.consumentenbond.nl/nieuws/2016/bodemprocedure-tegen-samsung-van-start

Consumentenbond (2016d). ‘Pratende pop Cayla slecht beveiligd - update 8 december 2016’. https://www.consumentenbond.nl/nieuws/2016/pratende-pop-cayla-slecht-beveiligd

CPB (2016). *Risicorapportage cyberveiligheid economie*. Den Haag: Centraal Planbureau.

CTIVD (2016). ‘Zienswijze van de CTIVD Op het wetsvoorstel Wiv 20..’. https://www.ctivd.nl/binaries/ctivd/documenten/publicaties/2016/11/09/zienswijze/Zienswijze+van+de+CTIVD_november+2016.pdf

CTIVD (2017). ‘Standpunt CTIVD wetsvoorstel wiv 20.. - vervolg op de zienswijze’. https://www.ctivd.nl/binaries/ctivd/documenten/publicaties/2017/01/31/index/Standpunt+CTIVD+Wiv+20..+-+februari+2017.pdf

Cyber Security Raad (2016). *European Foresight Cyber Security Meeting 2016: Public Private Academic Recommendations to the European Commission about Internet of Things and Harmonization of Duties of Care*. Den Haag: Cyber Security Raad.

Cyber Security Raad (nog te verschijnen). *Handreiking zorgplichten*. Den Haag: Cyber Security Raad.

Davis, J. (2007). ‘Hackers Take Down the Most Wired Country in Europe’. https://www.wired.com/2007/08/ff-estonia/

Deloitte (2016). ‘Cyber Value at Risk in the Netherlands’. https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/financial-services/deloitte-nl-fsi-cyber-value-at-risk.pdf

Deutsche Welle (2016a). ‘Merkel warns of Russian cyber attacks in German elections’. http://www.dw.com/en/merkel-warns-of-russian-cyber-attacks-in-german-elections/a-36314197

Deutsche Welle (2016b). ‘Germany's domestic intelligence chief accuses Russia of cyberwarfare’. http://www.dw.com/en/germanys-domestic-intelligence-chief-accuses-russia-of-cyberwarfare/a-19256911

Dialogic (2014). *De impact van ICT op de Nederlandse economie*. Utrecht: Dialogic.

Die Welt (2015). ‘Bundestag muss IT-Netzwerk wohl komplett austauschen’. https://www.welt.de/politik/deutschland/article142298394/Bundestag-muss-IT-Netzwerk-wohl-komplett-austauschen.html

ENISA (2015). *Cyber Security Information Sharing: An Overview of Regulatory and Non-Regulatory Approaches*. Heraklion: ENISA.

Eskens, S., Timmer, J., Kool, L., R. van Est (2016). *Beyond Control. Exploratory Study on the Discourse in Silicon Valley About Consumer Privacy in the Internet of Things*. Den Haag: Rathenau Instituut.

European Commission (2015). *Proposal for a Directive of the European Parliament and of the Council on Certain Aspects Concerning Contracts for the Supply of Digital Content*. Brussels: European Commission.

European Commission (2016). ‘Communication: Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry’. https://ec.europa.eu/digital-single-market/en/news/communication-strenghtening-europes-cyber-resilience-system-and-fostering-competitive-and

European Parliament (2016). ‘Cybersecurity: MEPs Back Rules to Help Vital Services Resist Online Threats’. http://www.europarl.europa.eu/news/en/news-room/20160701IPR34481/cybersecurity-meps-back-rules-to-help-vital-services-resist-online-threats

FTC (2015). ‘FTC Report on Internet of Things Urges Companies to Adopt Best Practices to Address Consumer Privacy and Security Risks’. https://www.ftc.gov/news-events/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices

FTC (2016). ‘ASUS Settles FTC Charges That Insecure Home Routers and “Cloud” Services Put Consumers’ Privacy At Risk’. https://www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges-insecure-home-routers-cloud-services-put

GfK (2015). *Cybersecurity 2015: Awareness, gedrag & digitaal verantwoord ondernemen*. Hilversum: GfK.

Gov.uk (2014). ‘Guidance: Procurement Policy Note 09/14: Cyber Essentials Scheme Certification’. https://www.gov.uk/government/publications/procurement-policy-note-0914-cyber-essentials-scheme-certification

Greenberg, A. (2015). ‘Hackers Remotely Kill a Jeep on the Highway—With Me in It’. https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

Hendrikman, M. (2016). ‘Ddos-aanval op dns-provider Dyn werd uitgevoerd met Mirai-botnet’. https://tweakers.net/nieuws/117059/ddos-aanval-op-dns-provider-dyn-werd-uitgevoerd-met-mirai-botnet.html

Hendriks, A., D. Brandt, K. Turk, V. Kocsis, D. in ’t Veld, T. Smits (2016). *Economische kansen Nederlandse cybersecurity-sector: Een verkenning*. Zoetermeer en Amsterdam: Verdonck, Klooster & Associates B.V. en SEO Economisch Onderzoek.

Hilton, S. (2016). ‘Dyn Analysis Summary of Friday October 21 Attack’. http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/

Hulsebosch, B. & A. van Velzen (2015). ‘Inventarisatie en classificatie van standaarden voor cybersecurity’. https://www.wodc.nl/binaries/2552-volledige-tekst_tcm28-73951.pdf

Inspectie Veiligheid en Justitie (2015). *Gebruik van beveiligingsadviezen van het Nationaal Cyber Security Centrum. Thematisch inspectieonderzoek*. Den Haag: Inspectie Veiligheid en Justitie.

ISE (2016). ‘Three-level IT baseline security system ISKE’. https://www.ria.ee/en/iske-introduction.html

ITU (2015). ‘Global Cybersecurity Index & Cyberwellness Profiles’. http://www.itu.int/pub/D-STR-SECU-2015

Kamerstukken I 2013-2014, CVIII, C. Technische aspecten van (bedrijfs)spionage, juridische normering en privacy. Verslag van een expertmeeting, vastgesteld 5 juni 2014.

Kamerstukken II 2015-2016, 34 372, nr. 2. Wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit (computercriminaliteit III).

Kamerstukken II 2016-2017a, 34 588, nr. 2. Regels met betrekking tot de inlichtingen- en veiligheidsdiensten alsmede wijziging van enkele wetten (Wet op de inlichtingen- en veiligheidsdiensten 20..).

Kamerstukken II 2016-2017b, 34 372, nr. 23. Motie van het lid Recourt, 13 december 2016.

Kamerstukken II 2016-2017c, 34 372, nr. 14. Motie van het lid Recourt en Tellegen, 13 december 2016.

Kamerstukken II 2016-2017d, 34 588, nr. 58. Motie van het lid Schouten, 8 februari 2017.

Kamerstukken II 2016-2017e, 34 588, nr. 56. Motie van het lid Recourt, 8 februari 2017.

Kamerstukken II 2016-2017f, 34 588, nr. 66. Motie van het lid Recourt, 8 februari 2017.

Keijzer, R. (2016). ‘Insulinepomp uit VS kan gehackt worden’. http://agconnect.nl/artikel/insulinepomp-uit-vs-kan-gehackt-worden

KPMG (2013). *Vijf denkfouten over cybersecurity: Een bestuurdersperspectief op cybersecurity*. Amstelveen: KPMG.

Landler, M. & J. Markoff, ‘Digital Fears Emerge After Data Siege in Estonia’. In: *The New York Times* 29 mei 2007.

Lonkhuyzen, L. van, ‘Meeste melding van datalekken uit zorgsector’. In: *NRC Handelsblad* 28 december 2016.

Lonkhuyzen, L. van, ‘Datalekken bij gemeenten; ‘het is een beetje een zooitje’’. In: *NRC Handelsblad* 27 januari 2017.

Ministerie Binnenlandse Zaken en Koninkrijksrelaties (2012). ‘Baseline Informatiebeveiliging Rijksdienst: Tactisch Normenkader (TNK)’. http://www.earonline.nl/images/ear/6/6f/BIR_TNK_1_0_definitief.pdf

Ministerie van Economische Zaken (2016). *Digitale Agenda: Vernieuwen, vertrouwen, versnellen*. Den Haag: Ministerie van Economische Zaken.

MIVD (2016). *MIVD Jaarverslag 2015*. Den Haag: Militaire Inlichtingen- en Veiligheidsdienst.

Nakashima, E., ‘Powerful NSA hacking tools have been revealed online’. In: *The Washington Post* 16 augustus 2016. https://www.washingtonpost.com/world/national-security/powerful-nsa-hacking-tools-have-been-revealed-online/2016/08/16/bce4f974-63c7-11e6-96c0-37533479f3f5_story.html?utm_term=.a7b20034bd7e

NCSC (2014). *Cybersecuritybeeld Nederland CSBN-4*. Den Haag: Nationaal Cyber Security Centrum.

NCSC (2015). *Cybersecuritybeeld Nederland CSBN 2015*. Den Haag: Nationaal Cyber Security Centrum.

NCSC (2016). *Cybersecuritybeeld Nederland CSBN 2016*. Den Haag: Nationaal Cyber Security Centrum.

Nederlandse Vereniging van Banken (2016). ‘Factsheet veiligheid en fraude’. https://www.nvb.nl/media/document/000254_od15799-nvb-factsheet-veiligheid-en-fraude-06-06.pdf

NIST (2014). ‘Framework for Improving Critical Infrastructure Cybersecurity’. https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

NOS (2015). ‘Nieuwe wet veiligheidsdiensten: hard nodig of gevaarlijk?’. http://nos.nl/nieuwsuur/artikel/2070103-nieuwe-wet-veiligheidsdiensten-hard-nodig-of-gevaarlijk.html

Overvest, B. & B. Straathof (2015). *What Drives Cybercrime? Empirical Evidence from DDoS Attacks*. Den Haag: Centraal Planbureau.

Prins, R., ‘AIVD moet helpen digitale ophaalbrug snel te openen’. In: *Het Financieele Dagblad* 10 mei 2016.

PwC & VU (2014). *Cybercriminaliteit tegen Nederlandse organisaties: een digitale dreiging*. Amsterdam: PwC & Vrije Universiteit Amsterdam.

PwC (2014). *Verkenning naar gescheiden ICT-netwerken en -diensten in Nederland*. Amsterdam: PwC.

PwC (2016). *Moving Forward with Cybersecurity and Privacy: How Organizations are Adopting Innovative Safeguards to Manage Threats and Achieve Competitive Advantages in a Digital Era*. New York, NY: PwC.

Rathenau Instituut (2014). ‘Notitie cyberintelligence en publiek belang: Expertmeeting Eerste Kamer 6 mei 2014’. https://www.rathenau.nl/nl/publicatie/notitie-cyberintelligence-en-publiek-belang

RVS (2016). ‘Samenvatting advies voorstel nieuwe Wet op de inlichtingen- en veiligheidsdiensten’. https://www.raadvanstate.nl/adviezen/samenvattingen/tekst-samenvatting.html?id=421

Security.nl (2016). ‘Beveiligingsbedrijf verdenkt scriptkiddies van aanval op Dyn’. https://www.security.nl/posting/490384/Beveiligingsbedrijf+verdenkt+scriptkiddies+van+aanval+op+Dyn

Scott, J. & D. Spaniel (2016). ‘Rise of the Machines: The Dyn Attack Was Just a Practice Run’. http://icitech.org/wp-content/uploads/2016/12/ICIT-Brief-Rise-of-the-Machines.pdf

Traynor, I. (2007). ‘Russia Accused of Unleashing Cyberwar to Disable Estonia’. https://www.theguardian.com/world/2007/may/17/topstories3.russia

Trend Micro (2016). ‘Frequently Asked Questions: BlackEnergy’. https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/faq-blackenergy

US Department of Homeland Security (2016). ‘Strategic Principles for Securing the Internet of Things (IoT)’. https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf

Verhagen, H. (2016). *De economische en maatschappelijke noodzaak van meer cybersecurity: Nederland digitaal droge voeten*. Den Haag: PostNL.

Voster, W. & J. de Bruijn (2016). *Cyber security supply chain risicoanalyse 2015*. Den Haag & Utrecht: Royal Dutch Shell & Power of 4.

Zetter, K. (2014). ‘Hacker Lexicon: What Is an Air Gap?’ https://www.wired.com/2014/12/hacker-lexicon-air-gap/

Bijlage 1: Deelnemers interviews

Ioannis Agrafioti, Oxford University

Philipp Amann, Europol

Axel Arnbak, De Brauw Blackstone Westbroek N.V.

Kraesten Arnold, Ministerie van Defensie

Jaya Baloo, KPN

Arie van Bellen, ECP

Bibi van den Berg, Universiteit Leiden

Herbert Bos, Vrije Universiteit

Aad van Boven, SecureMe2

Lotte de Bruijn, Nederland ICT

Marjolijn Durinck, ECP

Jos de Groot, Ministerie van Economische Zaken

Wim Hafkamp, Rabobank

Raymond van den Hoek, Bol.com

Erik Huizer, Surfnet

Demosthenes Ikonomou, ENISA

Gerrie de Jonge, PostNL

Elena Kvochko, Barclays

Steven Luitjens, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Dave Maasland, ESET

Nicole Mallens, VNO-NCW/MKB-Nederland

Ron de Mos, Nederland ICT

Jason Nurse, Oxford University

Wouter Oosterbaan, NCTV

Bastiaan Overvest, CPB

Erik Poll, Radboud Universiteit

Ronald Prins, Fox-IT

Melanie Rieback, Radically Open Security

Marijn Schuurbiers, Nationale Politie

Ton Siedsma, Bits of Freedom

Robert Spronk, AIVD

Eelco Vriezekolk, Agentschap Telecom

Maurice Wessling, Consumentenbond

Jos Weyers, TenneT

Patricia Zorko, NCTV

Grote multinational

Bijlage 2: Deelnemers workshops

Kraesten Arnold, Ministerie van Defensie

Herbert Bos, Vrije Universiteit

Aad van Boven, SecureMe2

Jeremy Butcher, Fox-IT

René Corbijn, Nederland ICT

Michel van Eeten, TU Delft

Nico van Eijk, Instituut voor Informatierecht

Jos de Groot, Ministerie van Economische Zaken

Raymond van den Hoek, Bol.com

Floor Jas, Surfnet

Eric Kaasenbrood, Rabobank

Linda Kool, Rathenau Instituut

Matthijs Kouw, Rathenau Instituut

Gino Laan, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Jos Leenheer, NCSC

Dave Maasland, ESET

Nicole Mallens, VNO-NCW/MKB-Nederland

Geert Munnichs, Rathenau Instituut

Erik Poll, Radboud Universiteit

Els Prins, VNO-NCW/MKB-Nederland

Melanie Rieback, Radically Open Security

Hessel Schut, Nationale Politie

Ton Siedsma, Bits of Freedom

Jelte Timmer, Rathenau Instituut

Maurice Wessling, Consumentenbond

AIVD

Bijlage 3: Trendanalyse

Jasper Veldman, Tommy van der Vorst, Leonie Hermanussen & Reg Brennenraedts

In dit hoofdstuk wordt een poging gedaan trends in cybersecurity te ontwaren. We doen dit op basis van kwantitatieve data over de factoren die bijdragen aan het ontstaan van manifestaties van cyberaanvallen: belangen, dreigingen en weerbaarheid.

1. Doelstelling

Het doel van deze trendanalyse is het geven van een onderbouwde inschatting van de ontwikkelingen in cyberdreigingen en cyberweerbaarheid van de Nederlandse samenleving en economie. Het Nationaal Cyber Security Centrum (NCSC) heeft sinds 2010 jaarlijks het Cybersecuritybeeld Nederland (CSBN) uitgebracht. Het CSBN biedt zowel kwalitatief als kwantitatief inzicht in de belangen, dreigingen en weerbaarheid op het gebied van cybersecurity in Nederland. De kwantitatieve inzichten die het CSBN geeft zijn echter vaak niet direct te gebruiken voor een trendanalyse. De gegeven cijfers gaan bijvoorbeeld over het aantal afgehandelde incidenten door het NCSC. De cijfers geven een goed beeld van het voorkomen en de impact van cyberaanvallen, maar zeggen weinig over de (omgevings)factoren die daaraan ten grondslag liggen.

De cijfers van het NCSC kunnen verleiden tot het ontwaren van trends. Het is echter de vraag of het überhaupt mogelijk is om ‘harde’ voorspellingen te geven over trends in cybersecurity. Dit heeft te maken met de dynamiek tussen aanvallers en verdedigers. Een cyberaanvaller maakt gebruik van technische en menselijke kwetsbaarheden in systemen en organisaties om daarmee een bepaald doel te bewerkstelligen. Wanneer een kwetsbaarheid bekend is, kan deze in de meeste gevallen worden opgelost, en moet de aanvaller op zoek naar een andere kwetsbaarheid. Cybersecuritytrends zijn het nettoresultaat van deze rat race, waarin enerzijds aanvallers continu moeten innoveren en anderzijds (potentiële) doelwitten beschermingsmaatregelen moeten treffen. Deze dynamiek maakt dat een trendanalyse geen uitspraken kan doen over cyberaanvallen die nog niet zijn ‘ontdekt’. Als dat wel (volledig of deels) mogelijk zou zijn, zou de bescherming immers ook (in principe) kunnen worden gerealiseerd, wat de dreigingstrend juist weer teniet zou doen. Met andere woorden: de dreigingen die we kunnen voorspellen zijn de dreigingen waartegen we ons het gemakkelijkst kunnen beschermen.

Wat wél mogelijk is, is het analyseren van trends ten aanzien van cyberaanvallen die we al kennen. Zo kunnen we uitspraken doen over het aantal criminelen dat toegang heeft tot de middelen die nodig zijn voor een bepaalde aanval en over het aantal doelwitten dat beschermingsmaatregelen heeft genomen tegen een bepaald type aanval. Daarnaast verwachten we patronen te kunnen onderscheiden in de levensloop van een cyberaanval.

Deze gegevens zijn echter ook geen garantie voor het met zekerheid vaststellen van trends. Ten eerste kunnen gegevens over de aanvallende en verdedigende zijde vertekend zijn of zelfs niet beschikbaar zijn. De oorsprong van de cijfers verdient daarom aandacht: waar komen deze cijfers vandaan en zijn er misschien belangen en waarden die in de cijfers doorklinken? Ten tweede is het mogelijk dat cijfers na verloop van tijd moeilijk met elkaar vergeleken kunnen worden. Ter illustratie: waar financiële fraude in het cyberdomein in eerste instantie op het niveau van de individuele consument speelde, zijn nu juist de financiële instellingen zelf het doelwit geworden van cyberaanvallen. Gegevens over financiële fraude in het cyberdomein hebben betrekking op verschillende doelwitten en methoden. Daarmee verkrijgen deze gegevens een andere betekenis na verloop van tijd. Die betekenis kan worden platgeslagen wanneer zuiver in termen van schade van financiële cyberfraude wordt geredeneerd. In dit onderzoek kijken we naar trends in de driehoek dreigingen, weerbaarheid en belangen, en de manifestaties die daaruit voortvloeien. De focus ligt daarbij op de onderliggende factoren die bepaalde trends verklaren. Vergeleken met het CSBN nemen we daarmee een iets grotere afstand van specifieke aanvallen. Het doel van de trendanalyse is niet om een dekkend beeld te geven van *alle* cybersecuritytrends.

Ook het geven van een voorspelling ten aanzien van nu nog niet bekende cyberaanvallen is nadrukkelijk geen doelstelling. Onze studie richt zich op vijf cyberaanvallen die vandaag de dag relevant zijn: digitale spionage, DDoS, cyberfraude, ransomware en malware. Deze cyberaanvallen zijn geselecteerd op basis van input van ENISA, CPB en de verschillende experts in de interviews en workshops. In paragraaf 2 gaan we dieper in op de keuze voor deze cyberaanvallen.

In de volgende paragraaf bespreken we het analytisch kader dat is gehanteerd in het onderzoek. In de daaropvolgende paragrafen geven we de trends weer van de belangrijkste cyberaanvallen. Elk van de cyberaanvallen bespreken wij aan de hand van de manifestaties, dreigingen en weerbaarheid. Aan het eind van het hoofdstuk geven we een overzicht van de belangrijkste conclusies van het onderzoek.

2. Analytisch kader

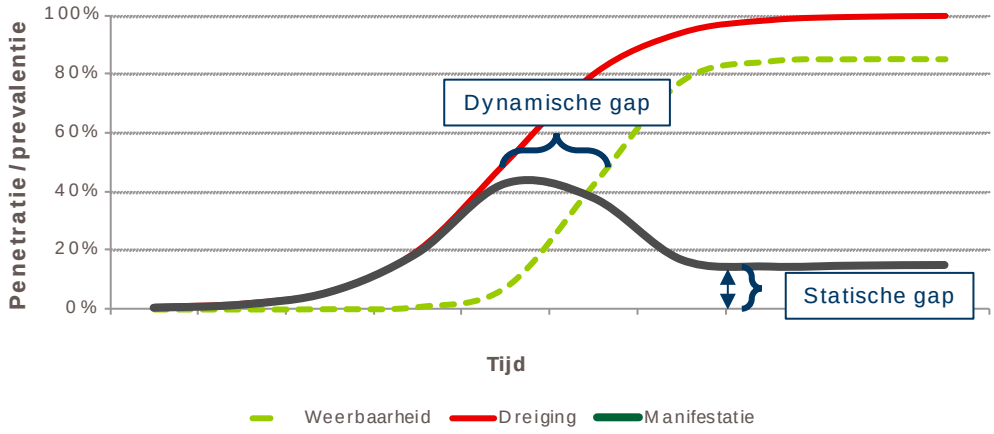
Voor cyberdreigingen geldt dat zowel aan de aanvallers- als de doelwitkant sprake is van innovatie. Aanvallers ontdekken en adopteren continu nieuwe aanvalsmethoden en middelen. Aan de doelwitkant geldt dat (in reactie op nieuwe aanvalstypen) beschermingsmethoden worden geïntroduceerd en geadopteerd. De introductie hiervan zal altijd achterlopen op de introductie van een aanvalstype, maar de adoptie kan mogelijk wel sneller verlopen.

We stellen vast dat de wetten voor *adoptie* van innovatie hier gelden: bij introductie van een nieuw type aanval heeft slechts een kleine groep aanvallers beschikking over de aanval, waarna de rest

deze langzaam zal adopteren. Dat proces verloopt volgens een S-curve, een wiskundige functie die door Rogers wordt toegepast voor het beschrijven van de adoptie van innovaties[1]. Een voorbeeld is ransomware: in eerste instantie zijn cryptolockers alleen beschikbaar voor criminelen die deze zelf ontwikkelen. Later verschijnen complete *toolkits* op de markt, waarmee het samenstellen van een cryptolocker zeer laagdrempelig wordt. Vervolgens worden cryptolockers zelfs als dienst verkrijgbaar. Net als in een 'normale' markt is aan beide zijden dus uiteindelijk sprake van *commoditization.*

Bij de weerbaarheid verloopt de adoptie ook via een dergelijke curve. In eerste instantie is slechts een klein deel van de doelwitten beschermd tegen de aanvallers. Zij hebben bijvoorbeeld kennis over de aanval en weten welke beschermingsmaatregelen zij moeten treffen. Na verloop van tijd krijgen steeds meer (potentiële) doelwitten kennis van de aanval en nemen ook zij de juiste maatregelen. Tot het moment dat (bijna) iedereen de beschermingsmaatregelen heeft geadopteerd.

Het verschil tussen adoptie van een aanvalstype door aanvallers en adoptie van bescherming daartegen door (potentiële) doelwitten leidt tot een *gap*, welke bepalend is voor het aantal combinaties aanvaller/doelwit/methode dat kan worden verwacht. Zodra de meeste doelwitten beschermd zijn, zullen de aanvallers overstappen naar een andere methode. Figuur 1 toont de gap tussen de adoptiecurves aan aanvaller- en doelwitzijde.



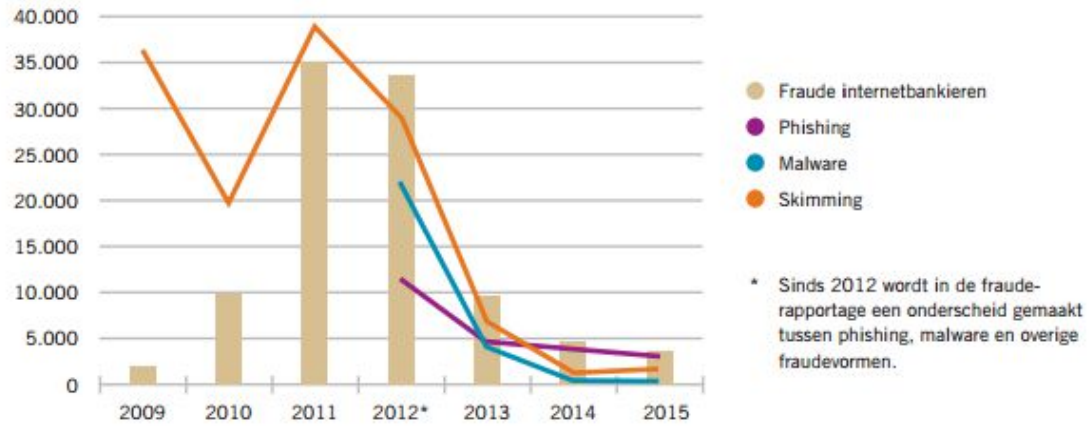
Figuur 1 Voorbeeld ontwikkeling penetratie en prevalentie van een generieke cyberaanval

In eerste instantie is de gap *dynamisch* en gelijk aan het verschil in adoptie aan aanvallers- versus doelwitzijde: er worden aanvallen ingezet waartegen nog geen (goede) bescherming verkrijgbaar of geadopteerd is. Uiteindelijk zal er bij de meeste typen cyberaanvallen, zelfs bij volledige adoptie van een beschermingsmiddel, een gap blijven bestaan. Deze *statische gap* ontstaat door het feit dat op zeer korte termijn variaties van een aanval kunnen worden ontwikkeld die succesvol zijn, ongeacht het weerbaarheidsniveau (bijvoorbeeld: een virus dat nog niet door virusscanners wordt herkend). Het verkleinen van deze *statische gap* kent daarnaast marginale meeropbrengsten, waardoor deze ook zou kunnen worden gezien als een geaccepteerd risiconiveau.

[1] Roger, E.M. (2004). *Diffusion of innovations*.

Een goed voorbeeld van een cyberaanval waarvoor een statische gap geldt, zijn virussen: hoewel virusscanners goed beschikbaar en geadopteerd zijn, kan een nieuw virus schade aanrichten totdat de virusscanners zijn bijgewerkt om ook dit nieuwe virus te herkennen (wat in de regel vrij snel gebeurt). Op de langere termijn kan de statische gap naar (nagenoeg) nul convergeren wanneer een systemische verandering plaatsvindt (bijvoorbeeld: de introductie van App Stores zorgt ervoor dat virussen veel lastiger toegang kunnen krijgen tot systemen). De 'grootte' van de gap staat los van de impact die een cyberaanval met zich mee kan brengen. Als gevolg van technologische ontwikkelingen kan het zo zijn dat aanvallen in impact toenemen (bijvoorbeeld: DDoS-aanvallen worden zwaarder door toename van digitale connectiviteit), terwijl de gap constant blijft.

De consequentie van deze dynamiek in cybersecurity is dat het lastig is om trends te ontwaren. Dit is overigens niet de enige reden waarom het lastig is om trends te ontwaren. Nieuwe dreigingen waarover (nog) onvoldoende informatie beschikbaar is en gebrekkige informatie over het voorkomen van cyberaanvallen maken het aanduiden van trends ingewikkeld. Een cyberaanval kan in korte tijd heel erg sterk groeien, maar als de juiste maatregelen worden genomen ook weer verdwijnen. Een duidelijk voorbeeld is te zien geweest bij de schade door fraude met internetbankieren door phishing en malware. Uit Figuur 2 komt naar voren dat de fraude met internetbankieren tussen 2009 en 2011 hard steeg, maar door de juiste maatregelen ook weer fors afnam in 2013.



Figuur 2 Schade door fraude met internetbankieren (x € 1.000) [2]

In ons onderzoek kijken we daarom vooral naar de historische ontwikkelingen en proberen deze te relateren aan de dynamiek uit Figuur 1. We kijken daarbij vooral hoe de dreiging en weerbaarheid van een cyberaanval zich de afgelopen jaren ontwikkeld hebben en of er sprake is van een dynamische of statische gap.

[2] Nederlandse Vereniging van Banken (2016) *Factsheet Veiligheid en Fraude*.

Cyberaanvallen

Op basis van inschattingen van ENISA[3], CPB en NCSC en gesprekken met cybersecurity-experts hebben we een overzicht gemaakt van relevante cyberaanvallen. Onder meer DDoS-aanvallen, ransomware en digitale spionage werden genoemd door de experts (zie Tabel 1). De aanvallen worden uitgevoerd door diverse actoren. Statelijke actoren en cybercriminelen vormen de belangrijkste actoren en de grootste dreigingen[4]. Ook het Cybersecuritybeeld Nederland kent in 2014, 2015 en 2016 een hoog dreigingsniveau toe aan beroepscriminelen en staten. Daarnaast vormen scriptkiddies een grote dreiging, omdat acties (bedoeld of onbedoeld) flinke maatschappelijke impact kunnen hebben.

Tabel 1 Belangrijkste cyberaanvallen volgens ENISA, CPB en NCSC

Cyberaanval	Toelichting trends
Malware	Malware blijft gestaag groeien.[5] Geen trendbreuk te verwachten.
DDoS	DDoS-aanvallen worden door CPB en NCSC aangestipt als belangrijke cyberaanval. Aanvallen worden effectiever.
Cyberfraude/identiteitsfraude	Specifiekere vormen van phishing en financiële malware.
Ransomware/ rogueware[6]/scareware	Een van de opvallendste vormen van cybercriminaliteit aldus het CPB. Het NCSC omschrijft het als het businessmodel voor cybercrime bij uitstek.
Digitale spionage	Wordt door het NCSC gezien als de belangrijkste cyberdreiging. Ontvangt recentelijk veel media-aandacht, o.a. door vermeende hacks tijdens de presidentsverkiezingen in de VS.

Uit Tabel 1 wordt duidelijk dat verschillende indelingen voor het classificeren van cyberaanvallen kunnen worden gehanteerd. Malware is opgenomen als een aparte aanvalscategorie, terwijl het ook onderdeel is van de andere aanvallen (zoals cyberfraude, waarbij het één van de middelen is).

We kiezen er in deze analyse voor om onderscheid te maken tussen het businessmodel en de aanvalsmethode. Het CBSN hanteert in zijn laatste rapportage drie verschillende businessmodellen: activiteiten gericht op geldelijk gewin, activiteiten gericht op verwerven van informatie en activiteiten gericht op verstoring. Voorbeelden van aanvalsmethoden zijn phishing, malware en ransomware.

Door het aanduiden van businessmodel en aanvalsmethode kan een beter onderscheid worden gemaakt tussen verschillende cyberaanvallen. Cyberfraude is bijvoorbeeld een activiteit die gericht is op geldelijk gewin, waarvoor zowel phishing als malware wordt gebruikt. Hetzelfde geldt voor

---

[3] ENISA (2015). *ENISA Threat Landscape 2015.*
[4] European Union (2015). *Cybersecurity in the European Union and beyond. Exploring the threats and policy response*.
[5] NCSC (2016) CSBN 2016.
[6] Rogueware is software waarvan gebruikers denken dat het helpt om schadelijke software te verwijderen maar juist schadelijke software is.

digitale spionage, waarbij het doel is om informatie te vergaren en zowel phishing als malware worden ingezet om het doel te bereiken.

Voor het onderzoek zullen wij onderstaande cyberaanvallen (als combinatie van aanvalsmethode en businessmodel) onderzoeken.

Tabel 2. Cyberaanvallen naar activiteit en methode

Cyberaanval	Activiteit gericht op	Methode
Cyberfraude	Geldelijk gewin	Malware en phishing
Ransomware	Geldelijk gewin	Ransomware
Digitale spionage	Verwerven van informatie	Malware en phishing
DDoS	Verstoring	DDoS
Verstoring door malware	Verstoring	Malware

Wij hebben voor bovenstaande cyberaanvallen gekozen, omdat deze in onze ogen het belangrijkste zijn. De cyberaanvallen werden veelvuldig genoemd in de literatuurstudie, workshops en de interviews. Eén van de gevaren van deze keuze is dat wij ons het meeste focussen op de cyberaanvallen waar veel over bekend is en die veel aandacht krijgen. Het hoeft niet noodzakelijkerwijs te betekenen dat deze ook de grootste dreiging vormen. Bovendien is de keuze voor deze cyberaanvallen niet allesomvattend. In de volgende paragrafen behandelen we de hierboven genoemde cyberaanvallen.

Het gebruik van statistieken voor trendanalyse

De gekozen indeling heeft als consequentie dat niet alle beschikbare statistieken direct aansluiten op de trendanalyse. De Fraudehelpdesk heeft bijvoorbeeld een overzicht van het aantal gemelde phishing mails. Uit het aantal gemelde phishing mails is echter niet direct af te leiden of het gaat om een activiteit gericht op geldelijk gewin of op het verwerven van informatie.

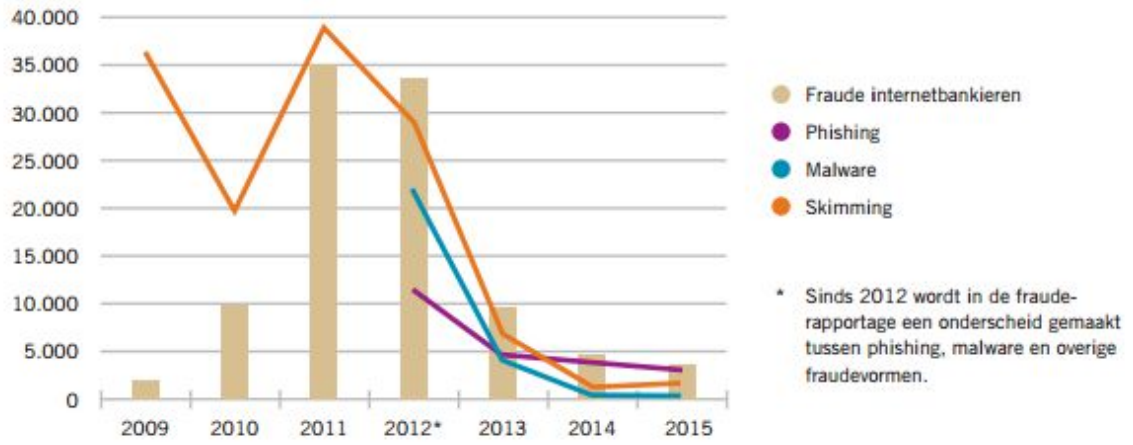
3. Cyberfraude

Cyberfraude concentreert zich met name op online transacties en internetbankieren. Dat is logisch, gezien het relatief grote aandeel van de Nederlanders dat gebruikt maakt van internetbankieren. In 2008 maakte nog maar 57% van de Nederlanders gebruik van internetbankieren, terwijl dat in 2014 was gestegen tot 77% van de Nederlanders.[7]

[7] Via [cbs.nl] en [statline.cbs.nl]

Manifestaties

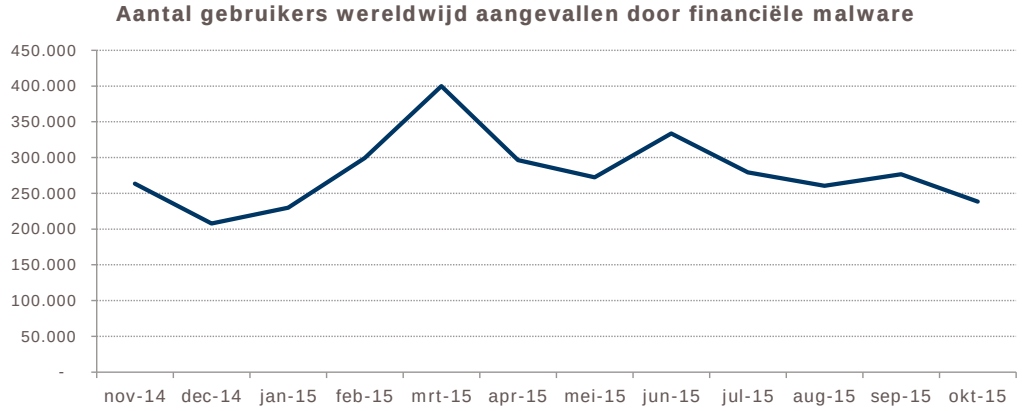
De schade door fraude met internetbankieren is in Nederland de afgelopen jaren fors afgenomen, zo blijkt uit informatie van de Nederlandse Vereniging van Banken.[8] In 2011 bedroeg de schade door fraude met internetbankieren nog 35 miljoen euro. In de eerste helft van 2016 was de schade bij internetbankieren nog maar 148.000 euro. In Figuur 3 is ook goed de manifestatiecurve te zien die geschetst is in Figuur 1. Tussen 2009 en 2011 neemt de fraude door internetbankieren fors toe en na 2012 neemt de schade ook weer fors af.



Figuur 3 Schade door fraude met internetbankieren (x € 1.000)[9]

Dreigingen

Uit Figuur 4 komt naar voren dat de afgelopen twee jaar het aantal gebruikers dat wereldwijd is aangevallen door financiële malware redelijk constant gebleven. Dit correspondeert ook met de gegevens uit Figuur 3, waar in de periode 2014-2015 de schade door cyberfraude nagenoeg gelijk is gebleven. Het blijft echter lastig om bovenstaande cijfers, die over de gehele wereld gaan, te vertalen naar de Nederlandse situatie.



Figuur 4 Aantal gebruikers wereldwijd aangevallen door financiële malware[10]

[8] NVB (2016) *Nauwelijks fraude bij internetbankieren*. [nvb.nl]
[9] Nederlandse Vereniging van Banken (2016) *Factsheet Veiligheid en Fraude*.
[10] Kaspersky (2016) *Security Bulletin 2015.*

Wat in Nederland ook meespeelt, is dat criminelen andere manieren vinden voor cyberfraude. In 2015 stak zogenaamde ‘pas-opstuurfraude’ de kop op, waarbij klanten van banken door een crimineel worden geïnformeerd over een nieuwe betaalpas middels een *phishing mail.* Hierin werden zij gevraagd de oude betaalpas op te sturen (in het kader van recycling). Op deze manier krijgen criminelen de betaalpas van klanten in handen. Vaak hebben ze de pincode al eerder afgekeken, of vragen ze om die op te sturen.[11] Het gaat hierbij om een variant op cyberfraude en kan gezien worden als resultante van de statische gap. Dat houdt in dat criminelen, ondanks de maatregelen die banken hebben genomen, er toch nog in slagen om schade aan te richten. Voor banken is het ook nagenoeg onmogelijk om zich hier helemaal tegen te wapenen, omdat zij altijd (licht) achter lopen op de criminelen. De maatregelen zijn echter wel genoeg om de schade binnen te perken te houden.

Weerbaarheid

Zoals hierboven aangegeven zijn de banken er de afgelopen jaren in geslaagd om fraude met internetbankieren terug te dringen. Met andere woorden: banken zijn erin geslaagd om weerbaarheid te vergroten. Zo weten banken de pogingen tot fraude steeds beter te detecteren en laten de klanten zich steeds minder misleiden. Bij het laatste aspect speelt vooral mee dat banken een grote voorlichtingscampagne zijn gestart in de media, onder meer via de website Veiligbankieren.nl. Ook hebben banken meer aandacht voor andere factoren die nodig zijn om succesvol te kunnen frauderen. Zo hebben de banken hun pijlen gericht op het bemoeilijken van het daadwerkelijk ‘uit de bank’ krijgen van het buitgemaakte geld via geldezels.

Een andere oorzaak voor de afname van fraude bij internetbankieren is het feit dat steeds meer Nederlanders gebruik maken van *mobiel* bankieren. Het ontwikkelen van mobiele malware is duurder voor criminelen, vanwege de grote diversiteit in apparatuur en software (bij Android) en de strenge controle op software en beveiliging in het besturingssysteem (bij iOS/Apple). Ook is het lastiger om generieke malware te ontwikkelen. Internetbankieren op de desktop bestaat bij alle banken uit een webapplicatie waarbij dezelfde technieken worden toegepast, maar de apps van de verschillende banken maken gebruik van verschillende technieken en zijn bijvoorbeeld in verschillende programmeertalen geschreven.[12]

In Nederland is het aantal gebruikers van apps voor mobiel bankieren de afgelopen jaren fors toegenomen. In 2012 lag het aantal gebruikers van de ING-app rond de miljoen personen, terwijl in 2016 er 2,8 miljoen mensen gebruik van maakten. [13,14]

De rol van digitale vaardigheden bij weerbaarheid

Zoals uit Figuur 3 naar voren kwam, is phishing één van de methodes voor het uitvoeren

[11] Veiligbankieren (2016) *Pas opstuurfraude*. [veiligbankieren.nl]
[12] Security.nl (2015) *ING: mobiel bankieren apps niet interessant voor crimineel*. [security.nl]
[13] NOS (2013) *Veel meer gebruikers banken-app*. [nos.nl]
[14] Security.nl (2016) *ING Mobiel Bankieren-app heeft 2,8 miljoen gebruikers*. [security.nl]

van cyberfraude. Voor het meten van de weerbaarheid tegen phishing kijken wij naar de digitale vaardigheden van de Nederlandse internetgebruikers. Hoe groter deze digitale vaardigheden, hoe groter de kans dat internetgebruikers een phishing mail herkennen of weten dat bijgevoegde bestanden niet geopend moeten worden. Dit geldt overigens niet alleen specifiek voor cyberfraude, maar ook voor digitale spionage en ransomware.

Het CBS heeft beperkte informatie over de digitale wijsheid van Nederlanders. Sinds 2015 houdt het CBS wel een enquête onder Nederlanders om de kennis/vaardigheden op het gebied van computers in kaart te brengen. De hierna genoemde percentages hebben betrekking op personen die in de drie maanden voorafgaand aan het onderzoek internet gebruikt hebben. Om die reden tellen ze niet op tot 100%: niet iedereen heeft in die drie maanden internet gebruikt. Uit de enquête komt naar voren dat in 2016 41,1% van de Nederlanders over meer dan basis computerkennis/vaardigheden beschikt. Dat is 1,6 procentpunt meer dan in 2015. Ook het aandeel van de Nederlanders met alleen basiskennis/vaardigheden is toegenomen: van 28,8% naar 30,9%. Het aandeel mensen dat geen (0,3%) of geringe (17,3%) kennis/vaardigheden van computers heeft, blijft nog altijd substantieel.

Het is niet eenvoudig om bovenstaande uitkomsten direct te vertalen naar weerbaarheid. Iemand met meer dan basis computerkennis/vaardigheden kan nog altijd slachtoffer worden van cybercriminaliteit. De verwachting is dat de meeste slachtoffers in de groep met geringe kennis/vaardigheden worden gemaakt. Het is dan ook noodzakelijk om de digitale wijsheid in die groep te vergroten. Door de digitalisering van de samenleving zijn ook de minder ICT-vaardige burgers gedwongen om steeds vaker gebruik te maken van internet(bankieren).

Conclusie

Bij cyberfraude is de dynamische en statische gap van cyberaanvallen goed waar te nemen. In de periode 2009-2011 is de schade door cyberfraude fors toegenomen. Op dat moment hebben de banken veel moeite gedaan om de weerbaarheid te vergroten door middel van voorlichtingscampagnes. Bovendien heeft de ontwikkeling van mobiele apps ook geholpen om de fraude terug te dringen. Vanaf 2013 heeft dat ook zijn vruchten afgeworpen en is de schade door cyberfraude fors afgenomen. De schade en manifestaties van cyberfraude die nu nog te zien zijn komen doordat (1) de maatregelen niet altijd tot 100% bescherming leiden en (2) op korte termijn variaties (zoals pas-opstuurfraude) op cyberfraude ontstaan waar in eerste instantie nog geen bescherming tegen is. Dit komt overeen met de statische gap zoals geformuleerd in paragraaf 1.2.

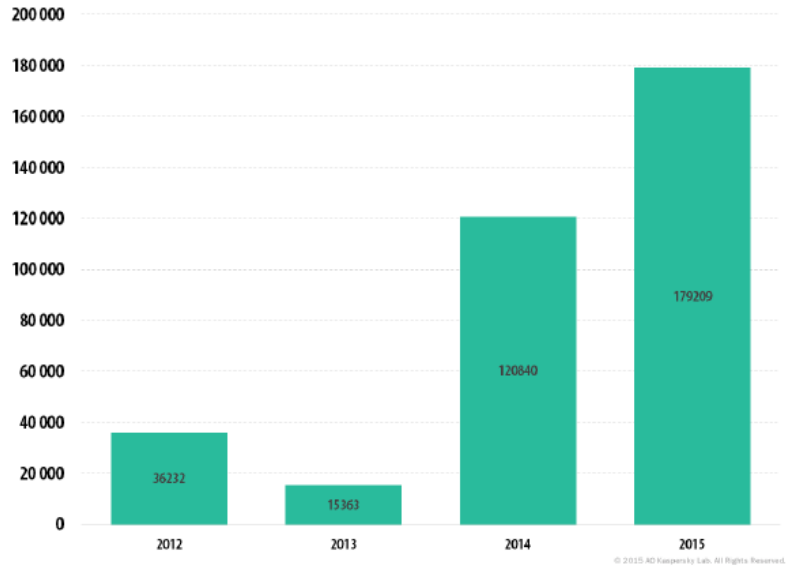
4. Ransomware

Ransomware is een populaire methode onder criminelen, omdat er veel geld mee te verdienen valt. Het CPB heeft voor de Risicorapportage Cyberveiligheid Economie geïnventariseerd wat de (geschatte) omzet van criminelen is bij ransomware. Dit blijkt te variëren tussen de € 70.000 en € 1.500.000. De kosten zijn echter beperkt. [15] Trustwave heeft specifiek gekeken naar de verhouding tussen de kosten en (verwachte) opbrengsten. Uit hun berekeningen komt naar voren dat criminelen met een simpele ransomware campagne een *return on investment* kunnen behalen van 1.425%.[16]

Nederland is specifiek een interessant doelwit voor criminelen, omdat Nederlanders bereid zijn om veel geld te betalen voor het terughalen van hun bestanden. Uit informatie van de Nederlandse politie komt naar voren dat voor een bepaald type ransomware Nederlandse en Belgische slachtoffers gemiddeld € 300,- per persoon betaalden.[17]

Manifestaties

Uit data van verschillende antivirusaanbieders blijkt dat de manifestaties van ransomware de afgelopen jaren flink zijn toegenomen. Specifiek betreft het hier de *encryptors:* ransomware die bestanden op de computer (en eventueel verbonden apparaten) van een slachtoffer codeert, en pas na betaling van losgeld weer decodeert. In 2015 zijn bijna 180.000 gebruikers aangevallen door encryptors (zie Figuur 5). Het lijkt alsof de top van ransomware nog niet bereikt is en het aantal manifestaties de komende jaren zal toenemen.



Figuur 5 Aantal gebruikers aangevallen door Trojan-Ransom encryptor malware[18]

[15] CPB (2015) *Risicorapportage Cyberveiligheid Economie.* Bron: NCSC (2014, 2015), Fox-IT en berekeningen van het CPB. De nationaliteiten van de slachtoffers zijn onbekend.

[16] Trustwave (2016) *Global Security Report.*

[17] Politie (2016) *Ransomware-slachtoffers bezoeken massaal portal 'No more ransom'*. [politie.nl]

[18] Kaspersky (2016) *Kaspersky Security Bulletin 2016.*

Het aantal manifestaties van ransomware in Nederland is niet exact te bepalen, maar Nederland lijkt in ieder geval een populair doelwit te zijn voor zowel de ransomware variant CTB-Locker en de CoinVault-cryptoware. De Nederlandse politie is er in 2015 in geslaagd om voor 1.400 met CoinVault geblokkeerde computers een code voor de ontgrendeling te achterhalen.[19] Van de 1.400 geblokkeerde computers bleken er 700 in Nederland te staan. De 700 besmettingen duiden wel op een toename ten opzichte van 2014. Trend Micro meldde over dat jaar 20 tot 40 besmettingen per maand door ransomware.[20]

Dreigingen

Eén van de belangrijkste ontwikkelingen aan de dreigingskant voor ransomware is de opkomst van Crime-as-a-Service. In eerste instantie werd ransomware alleen gebruikt door de ontwikkelaars zelf, maar inmiddels stellen zij hun ransomware ook beschikbaar aan derden.[21] De ontwikkelaars zelf ontvangen enkele tientallen dollars voor het verkopen van een licentie voor de ransomware en vaak ook een deel van de winst die wordt gemaakt uit het losgeld. De opkomst van digitale valuta zoals Bitcoin vergemakkelijkt dit proces.

Een tweede dreigingstrend is de opkomst van het piramidemodel voor ransomware. Gebruikers die geïnfecteerd zijn met ransomware krijgen twee opties aangeboden voor het vrijgeven van de data: (1) losgeld betalen of (2) een aantal andere personen besmetten met de ransomware. [22] Op deze manier kan de ransomware zich mogelijk nog sneller verspreiden. De kans bestaat dus dat het aantal dreigingen de komende jaren nog fors zal toenemen.

Weerbaarheid

Om de weerbaarheid tegen ransomware te vergroten is de Nederlandse politie samen met Europol, Intelsecurity en Kaspersky Lab het initiatief *No More Ransom* gestart. Op de website nomoreransom.org kunnen gebruikers onder andere informatie vinden over ransomware en hoe ze zichzelf ertegen kunnen beschermen:

- ☐ Zorg altijd voor de aanwezigheid van een back-up systeem, zodat een ransomware-besmetting uw persoonlijke gegevens niet definitief vernietigt;
- ☐ Gebruik robuuste antivirussoftware om uw systeem te beschermen tegen ransomware;
- ☐ Houd alle software op uw computer up-to-date;
- ☐ Vertrouw letterlijk niemand, aangezien elke account kan zijn aangetast.

Bovenstaande maatregelen hebben betrekking op het voorkomen van besmettingen door ransomware. Daarnaast kunnen slachtoffers op de website ook sleutels vinden die hen kunnen helpen om geblokkeerde apparaten te decoderen en vergrendelde bestanden te ontsleutelen. In augustus 2016 meldde de politie dat de (Engelstalige) website 300.000 keer bezocht was en dat enkele honderden bezoekers hun computers/bestanden hebben kunnen ontgrendelen. Slechts

---

[19] Politie (2015) *Politie zorgt voor doorbraak in recente cryptoware aanval*. [politie.nl]
[20] TrendMicro (2015) *Trend Micro-rapport cybercrime 2014: Online bankieren kwetsbaar en ransomware groter risico*. [blog.trendmicro.nl]
[21] TrendMicro (2016) *Outsourcing crime: How Ransomware-as-a-Service works*. [blog.trendmicro.com]
[22] BleepingComputer (2016) *New Scheme: Spread Popcorn Time Ransomware, get change of free Decryption Key*. [bleepingcomputer.com]

enkele maanden later, in december, wist de politie te melden dat er al bijna 6.000 mensen hun apparaten hebben kunnen ontsleutelen. De forse stijging heeft meerdere oorzaken. Ten eerste zijn er nieuwe decodeersleutels toegevoegd aan de website. Ten tweede is de website nu ook beschikbaar in meerdere talen (naast Engels, ook het Nederlands, Frans, Italiaans, Portugees en Russisch).

Conclusies

Het aantal manifestaties van ransomware is de afgelopen jaren wereldwijd fors toegenomen. Uit de cijfers komt naar voren dat dit ook voor Nederland geldt. Zoals eerder is geconcludeerd is één van de redenen voor de vele aanvallen in Nederland dat er bij de ransomware-campagnes waarschijnlijk een Nederlander betrokken was. Daarnaast is ook ransomware-as-a-service in opkomst, waardoor ook de minder ICT-onderlegde criminelen ransomware kunnen verspreiden.

De afgelopen twee jaar heeft de Nederlandse politie samen met Europol en een aantal makers van antivirussoftware wel het nodige gedaan om de weerbaarheid te vergroten. Ze hebben een website opgezet om voorlichting te geven over de gevaren en stellen (indien beschikbaar) sleutels beschikbaar om de apparaten te ontsleutelen.

Gezien het feit dat het aantal manifestaties tot en met 2015 is toegenomen, lijkt er voorlopig nog sprake te zijn van een dynamische gap. Het effect van de maatregelen van de Nederlandse politie en Europol zijn (nog) niet terug te zien in de cijfers. Wij verwachten echter dat deze maatregelen binnen afzienbare termijn wel effect hebben maar dat het nog wel enige tijd in beslag zal nemen voor het aantal manifestaties zal afnemen. Wanneer het aantal manifestaties zal afnemen is op dit moment niet in te schatten, net als hoe groot de (uiteindelijke) statische gap zal zijn.

5. Digitale spionage

Digitale spionage wordt door de Europese Commissie[23] en het NCSC gezien als één van de belangrijkste cyberaanvallen. De reden hiervoor is dat kennis steeds belangrijker wordt (zowel politiek als economisch gezien) en dat bedrijven en particulieren door de opkomst van smartphones en tablets steeds meer informatie digitaal opslaan. Dit maakt het voor aanvallers aantrekkelijker om digitale in plaats van fysieke spionage uit te voeren. De aanvalsmethoden die voor digitale spionage worden gebruikt, zijn zowel (spear)phishing als malware.

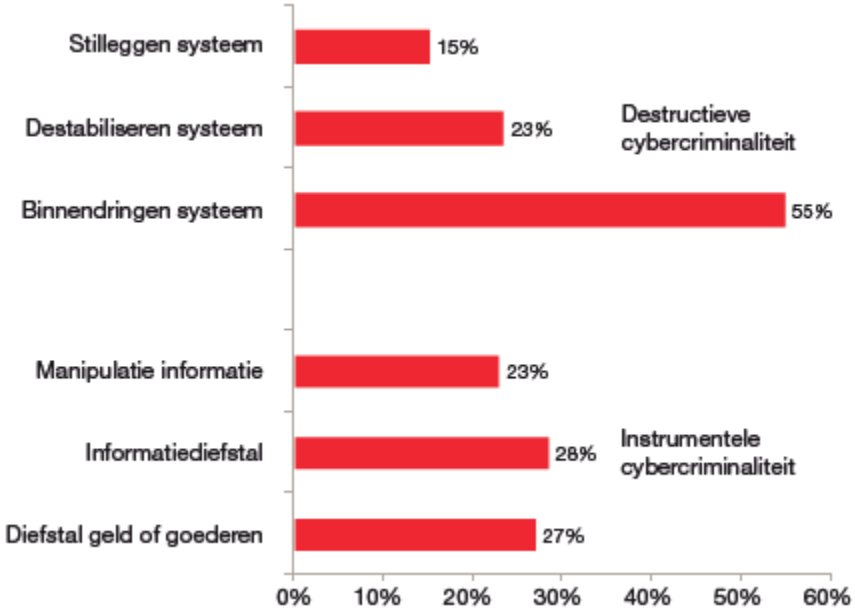
Manifestaties

Het is lastig om goede cijfers te vinden over het aantal manifestaties van digitale spionage. In veel gevallen wordt digitale spionage niet ontdekt of wordt er geen melding van gemaakt. Bedrijven zijn hierbij bang voor imagoschade of boetes wanneer zij niet tijdig het geconstateerde datalek hebben

[23] European Union (2015). Cybersecurity in the European Union and beyond. Exploring the threats and policy response

gemeld bij de toezichthouder. De boetes vanuit de Wet Meldplicht Datalekken kennen een maximum van 500.000 euro en in bijzondere gevallen kan deze boete nog hoger uitvallen.

In het onderzoek van PwC en de Vrije Universiteit Amsterdam (2015) is aan 195 bedrijven die aangaven slachtoffer te zijn geweest van cybercriminaliteit gevraagd wat het achterliggende doel van de criminele activiteiten is geweest. Uit Figuur 6 komt naar voren dat bij meer dan de helft van de bedrijven het de bedoeling was om het systeem binnen te dringen.



Figuur 6 Frequenties van destructieve en instrumentele cybercriminaliteit[24]

Dreigingen

Inlichtingendiensten constateren dat statelijke actoren steeds vaker digitale middelen inzetten. In het CSBN wordt digitale spionage aangemerkt als een significante bedreiging voor de nationale veiligheid.[25] Het gaat dan vooral om activiteiten met een laag volume, maar een hoge opbrengst per doelwit. Concrete getallen over het aantal incidenten of het aantal bespiedde bedrijven worden hierin echter niet genoemd.

De dreiging van digitale spionage valt uiteen in economisch gemotiveerde spionage en politieke/diplomatiek gemotiveerde spionage. Economische spionage is gericht op het achterhalen van bedrijfsinformatie en zal altijd aanwezig zijn (en is ook altijd aanwezig geweest). In de jaren zeventig was er in Nederland een rel rondom gestolen informatie van het bedrijf Urenco. Destijds ging het nog om fysieke diefstal van bedrijfsinformatie. Ten aanzien van politiek/diplomatiek gemotiveerde spionage zien we dat deze steeds vaker gepaard gaat met sabotage en pogingen tot beïnvloeding van de publieke opinie. Zo wordt er gesuggereerd dat cybercriminaliteit een aanzienlijke rol bij de meest recente Amerikaanse presidentsverkiezingen heeft gespeeld. De

[24] PwC en VU (2015). *Cybercrminaliteit tegen Nederlandse organisaties – een digitale dreiging.*
[25] CSBN (2016). Cybersecuritybeeld Nederland 2016

vermeende rol van Rusland in het uitvoeren van cyberaanvallen tijdens de verkiezingscampagne en beschuldigingen over en weer zetten de internationale verhoudingen op scherp.

De digitalisering van de samenleving heeft ervoor gezorgd dat aanvallers ook van afstand kunnen inbreken bij een partij. Het gaat hier (nog steeds) vaak om partijen die genoeg middelen (zowel geld als manschappen) tot hun beschikking hebben om aanvallen uit te voeren. Het kan dan bijvoorbeeld gaan om *zero-day* kwetsbaarheden - kwetsbaarheden waartegen nog geen bescherming beschikbaar is. Een andere optie is de gerichte en geavanceerde *social engineering* aanval.[26] Deze aanvallen zijn zo opgezet dat slachtoffers onbewust malware verspreiden aan de spionagedoelwitten. Dit doen ze door malware te koppelen aan content die een grote kans heeft om binnen een bepaalde doelgroep te worden verspreid. Voorbeelden hiervan zijn een grappig filmpje over gebeurtenissen op kantoor, waarvan de kans groot is dat deze onder collega's van kantoren wordt verspreid, of een e-mail die afkomstig lijkt te zijn van een bekende of instantie waarmee een slachtoffer onlangs nog heeft gecommuniceerd. Een belangrijke techniek hierbij is *spearphishing*, waarbij zo veel mogelijk (persoonlijke) informatie over het slachtoffer wordt verzameld, die vervolgens wordt aangesproken per e-mail op een zodanige manier dat de afzender als een te vertrouwen partij overkomt. Dit vergroot de kans dat een slachtoffer een geïnfecteerd bericht opent. Vaak wordt hierbij gebruik gemaakt van informatie die het slachtoffer zelf vrijwillig openbaar maakt, bijvoorbeeld via sociale media. Spearphishing berichten zijn een belangrijke methode om een systeem binnen te komen, waarna het systeem van het slachtoffer gecompromitteerd is en andere aanvalsmethoden kunnen worden ingezet.

Weerbaarheid

Voor de beveiliging tegen digitale spionage worden steeds geavanceerdere authenticatieystemen ingezet. In veel gevallen wordt er gebruik gemaakt van tweestapsauthenticatie. Doordat daarbij twee verschillende 'bewijzen' van identiteit nodig zijn, en het voor een aanvaller moeilijker is om beide te verkrijgen, wordt een aanval moeilijker. De tweede factor bestaat veelal uit een controle per sms, biometrische informatie (zoals vingerafdrukken) of de koppeling van een e-identiteitsbewijs aan een wachtwoord.

Voor een deel van de aanvallen is het echter ook nagenoeg onmogelijk om beveiligingsmaatregelen te nemen. Als gebruik wordt gemaakt van *zero-day* kwetsbaarheden biedt geen enkele anti-virusscanner bescherming. De bescherming zit dan vooral in het alert blijven op verdachte mails, niet zomaar een bijlage openen of een gevonden usb-stick in de computer stoppen. Zo heeft de oplettendheid van een medewerker van de Onderzoeksraad voor de Veiligheid (OCC) ervoor gezorgd dat hackers geen toegang kregen tot de servers van de OVV.[27] Hij kreeg een nep-email van een 'collega' dat hij zich opnieuw moest aanmelden, maar hij vertrouwde het niet en heeft het dan ook niet gedaan.

---

[26] CSBN (2016). *Cybersecuritybeeld Nederland 2016*

[27] Trouw (2017) *Russen deden hackpoging OVV rond publicatie rapport MH17.* [trouw.nl]

De AIVD vervult in dit verband een rol van grote betekenis omdat men daar beschikt over de kennis om met behulp van bijvoorbeeld netwerkdetectie spionage op bedrijfsnetwerken op te sporen. Bij een groot deel van de bedrijven ontbreekt het aan kennis, financiën, middelen en tijd om geavanceerde (spionage)aanvallen op te merken.[28]

Conclusie

Spionage zal altijd aanwezig zijn in de samenleving. Digitale spionage-aanvallen worden uitgevoerd door partijen die over meer dan voldoende middelen (zowel geld als manschappen) beschikken. Dit maakt het erg lastig om de weerbaarheid tegen spionage te vergroten, omdat de ingezette middelen vaak zeer geavanceerd zijn. Het gevolg hiervan is dat bij digitale spionage sprake lijkt te zijn van een grote (statische) gap tussen dreigingen en weerbaarheid.

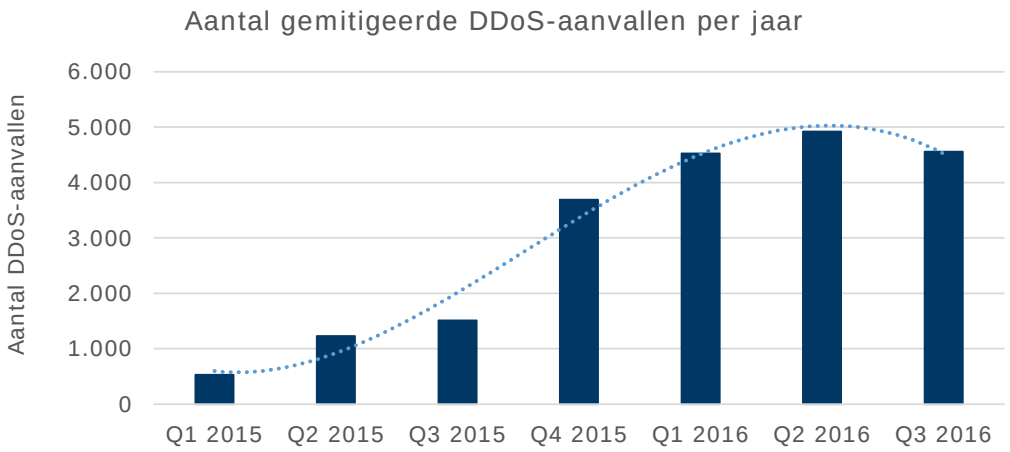
6. DDoS

De DDoS-aanval is één van de meest bekende verstorende aanvallen. Met behulp van een DDoS-aanval kan een website voor lange tijd worden platgelegd. Eén van de belangrijkste redenen dat DDoS-aanvallen steeds populairder worden, is het feit dat de kosten van het laten uitvoeren van een DDoS-aanval niet bijzonder hoog zijn. Scott & Spaniel (2016) rapporteren typische gemiddelde kosten tussen de $25 en $150 voor een 24 uur durende aanval tegen één doelwit.[29]

Manifestaties

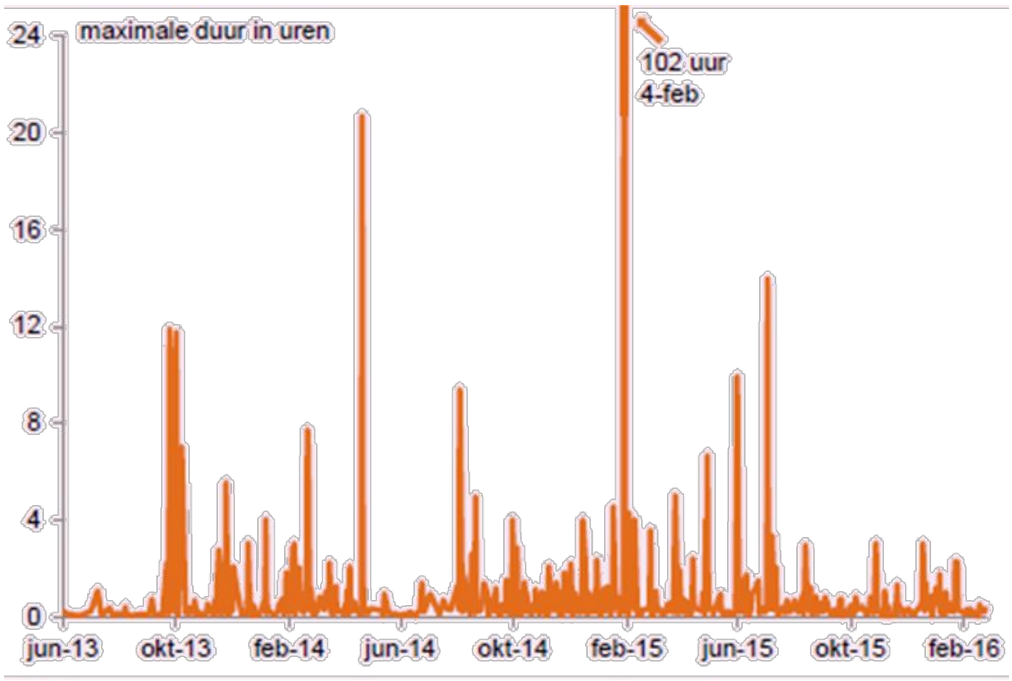
Uit Figuur 7 komt naar voren dat het aantal door Akamai gemitigeerde DDoS-aanvallen sterk toe nam in 2015. Voor het afgelopen kwartaal zien we echter een lichte afname. Het kan betekenen dat de gap van DDoS ook aan het afnemen is. Het gaat hierbij echter niet om het aantal daadwerkelijke aanvallen, maar om het aantal gemitigeerde aanvallen. Bovendien is het belangrijk om te onthouden dat het gaat om data van een aanbieder van diensten om DDoS-aanvallen tegen te houden. De aanbieder wil laten zien dat hij veel DDoS-aanvallen tegenhoudt, zodat zijn klanten meer diensten afnemen. Het is echter één van de weinige bronnen met informatie over het aantal (gemitigeerde) DDoS-aanvallen.

[28] Algemene Inlichtingen- en Veiligheidsdienst (2017) *Economische cyberspionage.* [aivd.nl]
[29] Scott & Spaniel (2016). *Rise of the Machines: The Dyn Attack Was Just a Practice Run. Institute for Critical Infrastructure Technology.*



Figuur 7. Aantal DDoS-aanvallen gemitigeerd door Akamai[30]

De impact van DDoS-aanvallen wordt daarnaast niet louter bepaald door het aantal aanvallen, maar vooral door de intensiteit en de duur van de aanval. Uit cijfers van het CPB blijkt dat de intensiteit en duur van de aanvallen sterk fluctueert (zie Figuur 8).[31] Het kan dus zo zijn dat het aantal aanvallen wel afneemt (en de gap ook), maar dat de duur en intensiteit toeneemt. Een lange en grote aanval heeft een grotere impact op de maatschappij dan vijf korte en kleine aanvallen. Zoals ook blijkt uit real-time weergave van DDoS aanvallen op platformen als Digital Attack map en Norsecorp fluctueren de doelwitten en herkomst van DDoS-aanvallen sterk.



Figuur 8 DDoS-aanvallen op Nederlandse doelen zijn meestal van korte duur[32]

[30] Akamai (2016) *State of the internet security. Q1, Q2, Q3, Q4; Akamai (2015) State of the internet security. Q2, Q3, Q4*
[31] CPB (2016) *Risicorapportage cyberveiligheid Economie.*
[32] Uit CPB (2016). *Risicorapportage cyberveiligheid Economie*. Bron: Digital Attack Map. Op basis van 2% van de DDoS-aanvallen uit de attack map.

Dreigingen

De belangrijkste dreigingstrend ten aanzien van DDoS aanvallen is het ontstaan van steeds grotere en efficiënte botnetten. Een van de voorbeelden hiervan is Malware Mirai: hiermee worden automatisch Internet of Things-devices (zoals aan internet gekoppelde camera's) gevonden, besmet en toegevoegd aan een botnet. Dergelijke devices hebben inmiddels zoveel rekenkracht aan boord dat ze, vanuit malware-perspectief, volwaardige alternatieven zijn geworden voor desktops. Mirai biedt een krachtig ontwikkelplatform dat naar wens kan worden aangepast en geoptimaliseerd. Inmiddels zijn reeds miljoenen IoT devices onderdeel van Mirai botnetten. Een belangrijke ontwikkeling die hieraan ten grond slag ligt is dat steeds meer devices worden aangesloten op het internet.

Vanaf september 2016 veroorzaakte het Mirai-botnet (mede) verscheidende grote aanvallen, waaronder op krebsonsecurity.com (de website van de Amerikaanse beveiligingsonderzoeker Brian Krebs), de Franse internetprovider IVH, de DNS-infrastructuur van Dyn (waardoor websites als Twitter, Amazon, Tumblr, Reddit, Spotify en Netflix slecht bereikbaar waren), de campagnewebsites van Donald Trump en Hillary Clinton, e-mail publicatieservers van WikiLeaks en websites van vijf Russische banken.[33] Zoals blijkt uit deze voorbeelden wordt Mirai binnen enkele maanden in verschillende landen door verschillende actoren ingezet. Hierbij richt Mirai zich op diverse sectoren, zoals de financiële sector, de telecomsector en de publieke sector. Interessant hierbij is dat aanvallen niet alleen plaatsvinden op websites, maar ook op fysieke infrastructuren, zoals de telecominfrastructuur of verwarmingssystemen van huizen (via 'slimme' thermostaten). Kaspersky spreekt de verwachting uit dat IoT-apparaten worden gebruikt voor het faciliteren van Advanced Persistent Threats (APT). Deze dreiging zal zich vooral richten op high value doelwitten die connectiviteit inzetten in fabricage en industriële processen.[34]

Bij DDoS speelt daarnaast ook de *commoditization* van de aanval een rol. Net als bij ransomware is DDoS nu ook beschikbaar *as a service*. Dat betekent dat iedereen nu met een simpele muisklik een DDoS-aanval kan uitvoeren op een website of server.

Weerbaarheid

DDoS-aanvallen afweren is kostbaar, maar het wordt steeds effectiever.[35] De Nationale Beheersorganisatie Internet Providers heeft ook de NaWas (Nationale anti-DDoS wasstraat) opgericht. De NaWas biedt on demand beveiliging tegen DDoS-aanvallen. Het is bedoeld voor middelgrote en kleinere internetproviders voor wie het te kostbaar is om zelf de anti-DDoS apparatuur in te kopen. Zij kunnen op deze manier voor een gunstig tarief hun weerbaarheid tegen DDoS-aanvallen vergroten.

Om de weerbaarheid te vergroten tegen de Mirai-malware is een innovatie naar buiten gebracht. Hackers hebben verschillende kwetsbaarheden in de Mirai malware gevonden die gebruikt kunnen

---

[33] Scott & Spaniel (2016). *Rise of the Machines: The Dyn Attack Was Just a Practice Run. Institute for Critical Infrastructure Technology.*
[34] Kaspersky (2015). *Kaspersky security bulletin 2014.*
[35] CSBN (2016). Cybersecuritybeeld Nederland 2016

worden om de malware op besmette IoT-apparaten te deactiveren en nieuwe, lastig te kraken wachtwoorden en gebruikersnamen te geven, waardoor besmetting met nieuwe malware wordt bemoeilijkt. Op deze manier kunnen de IoT-apparaten niet meer worden toegevoegd aan het botnet. Echter, de vraag is of devices niet *by default* beveiligd zouden moeten zijn tegen malware als Mirai. Dit roept discussie op over wie verantwoordelijk dan wel aansprakelijk is voor de beveiliging van devices (zie Box 1).

Box 1. Beveiliging van devices.

De Federal Trade Commission (FTC, de Amerikaanse marktautoriteit) is een reeks aanklachten gestart tegen hardware producenten ASUS, TRENDnet en recentelijk D-Link. De aanklacht tegen D-Link was op grond van consumentenmisleiding: de fabrikant adverteerde met veilige apparatuur, maar in werkelijkheid werden de meest basale veiligheidsmaatregelen niet genomen. De 'geavanceerde' netwerkbeveiliging bestond onder meer uit een standaard wachtwoord en gebruikersnaam. De FTC stelt dat D-Link hiermee de privacy van Amerikaanse consumenten in het geding brengt.
Een andere zaak waarbij privacy een grote rol speelt betreft de *My Friend Cayla* pop van fabrikant Genesis Toys. Deze pop zou informatie opslaan voor marketingdoeleinden. De pop is inmiddels uit de handel gehaald, maar het is niet het enige *connected* speelgoed waarbij beveiligings- dan wel privacy issues ontstaan.

Naast aanklagen van misleidende of malafide praktijken zou ook bestaande aansprakelijkheidswetgeving kunnen worden gemoderniseerd, waardoor fabrikanten verplicht worden om een bepaald minimum beveiligingsniveau te waarborgen (*security by design*). Het is echter de vraag of daarmee het probleem is opgelost, omdat veel gebruikers software en hardware online bestellen bij fabrikanten die wellicht niet gebonden zijn aan deze wetgeving en daardoor goedkopere onbeveiligde producten kunnen aanbieden. En wie is er in het geval van *open source software* aansprakelijk? Het bewustzijn van consumenten van het belang van beveiliging en de bereidheid om bijvoorbeeld extra te betalen voor een veilig product lijkt een belangrijk uitgangspunt te zijn voor het slagen van welke aanpak dan ook.

Naast het verkleinen van kwetsbaarheden is baat bij het nemen van maatregelen tegen cybercriminelen. Zo voert Europol operaties uit tegen *DDoS-for-hire* services. Tussen 5 en 9 december dit jaar arresteerde Europol 34 gebruikers uit 13 landen voor het gebruiken van tools voor DDoS aanvallen. In deze internationale operatie werkte Europol samen met rechtshandhavingsautoriteiten uit Australië, België, Frankrijk, Hongarije, Letland, Nederland, Noorwegen, Portugal, Roemenië, Spanje, Zweden, het Verenigd Konikrijk en de Verenigde Staten.[36]

[36] Europol (12 december 2016). Joint international operation targets young users of DDOS cyber-attack tools. [europa.eu]

Conclusie

Uit cijfers van één van de aanbieders van bescherming tegen DDoS-aanvallen blijkt dat het aantal gemitigeerde DDoS-aanvallen licht is afgenomen eind 2016. Het aantal DDoS-aanvallen geeft echter weinig inzicht in de dreiging die ervan uit gaat. Het gaat vooral om de duur en de grootte. Bovendien is het lastig om de cijfers van deze aanbieder te interpreteren. Hij wil laten zien dat hij veel DDoS-aanvallen tegenhoudt, zodat zijn klanten meer diensten afnemen.

Voor wat betreft dreigingen is een aantal trends waar te nemen, waaronder de opkomst van (slecht beveiligde) IoT-apparaten, waardoor de botnetten eenvoudig kunnen groeien, en DDoS-as-a-service. Tegelijkertijd worden ook maatregelen genomen om de weerbaarheid tegen DDoS-aanvallen te vergroten, onder meer door het oprichten van een nationale anti-DDoS wasstraat. Afgaande op de beschikbare informatie schatten wij in dat de manifestaties van DDoS-aanvallen op korte termijn nog meer zullen toenemen. De maatregelen die genomen worden lijken effectief te zijn. Het is niet te zeggen wanneer de manifestaties van DDoS-aanvallen zullen afnemen en hoe groot de (uiteindelijke) statische gap zal zijn.

7. Verstoring door malware

Tot slot kijken we naar de verstoringen die veroorzaakt worden door malware – volgens het CBS nog steeds een groot probleem voor Nederlandse huishoudens.

Manifestaties

In de halfjaarlijkse Security Intelligence-rapportages brengt Microsoft in kaart hoe vaak antivirussoftware bepaalde typen malware tegenkomt.[37] Uit de rapportages over de afgelopen periode 2014-2015 zijn de volgende waarnemingen te halen:

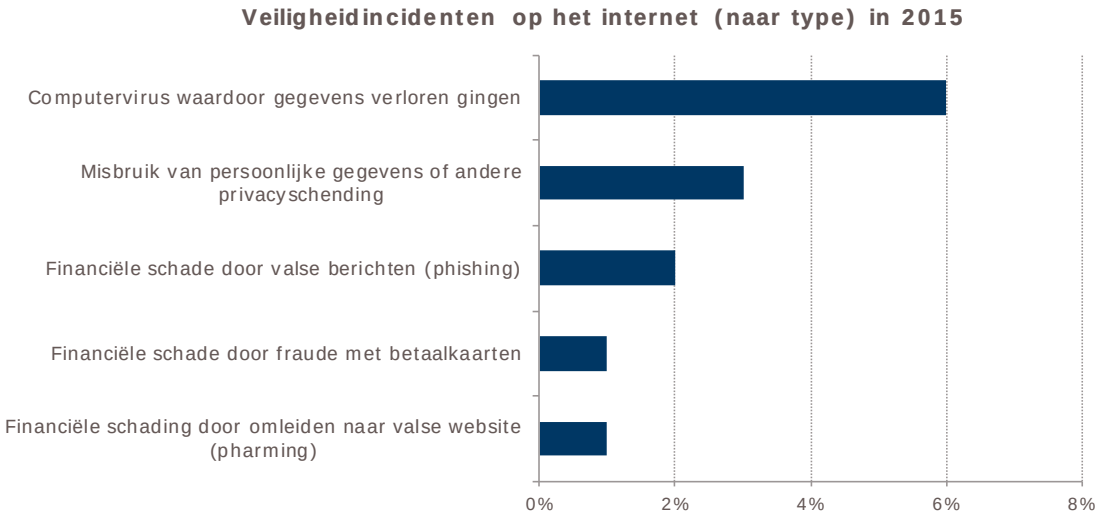
- ☐ Virussen worden waargenomen op 1% tot 1,5% van de rapporterende computers. Dit percentage is relatief stabiel gebleven over de afgelopen anderhalf jaar.
- ☐ Trojaanse paarden worden op 4% tot 8% van de computers waargenomen. Eind 2015 zat het percentage gerapporteerde Trojaanse paarden op 7%.
- ☐ Wormen vormen na Trojaanse paarden de grootste groep malware. Eind 2015 kwamen wormen op bijna 4% van de computers voor. Dit is wel een daling ten opzichte van begin 2014, toen het percentage nog op bijna 6% zat.

De manifestaties van malware op computers lijkt redelijk stabiel over de afgelopen jaren. De variaties kunnen ontstaan zijn door de dynamiek bij malware: zodra zij zijn herkend door de virusscanners komen ze naar voren in de statistieken, waarna aanvallers nieuwe malware gaan ontwikkelen.

Bovenstaande cijfers kunnen ook naast de uitkomsten van de ICT, Kennis en Economie studie van het CBS worden gelegd. Het CBS heeft voor die studie de veiligheidsincidenten op internet in 2015

[37] Microsoft (2015/2016) *Security Intelligence Report Volume 18, 19 & 20.*

in kaart gebracht en geclassificeerd naar type. In onderstaand figuur is het percentage mensen te zien dat in 2015 een veiligheidsincident heeft meegemaakt.



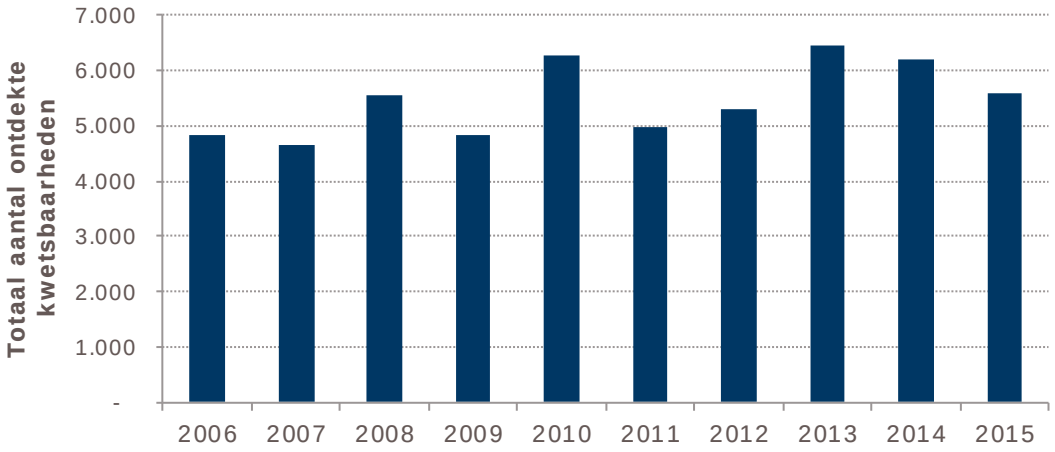
Figuur 9 Veiligheidsincidenten op het internet[38]

Uit bovenstaande figuur komt naar voren dat computervirussen waardoor gegevens verloren gingen onverminderd hoog scoren in veiligheidsincidenten op het internet. Dit komt niet overeen met de uitkomsten van de studie van Microsoft. Een oorzaak hiervan kan de rapportagevorm van het CBS zijn. Mogelijk scharen zij meerdere type malware (of zelfs zaken als ransomware) onder de noemer computervirussen, maar dat wordt niet vermeld in het rapport van het CBS, waardoor de betekenis van deze indicator wat onduidelijk blijft. Daarnaast hoeft het aantal waargenomen virussen op computers niet overeen te komen met een veiligheidsincident.

Dreigingen

De dreiging van de verstoring door malware laat zich goed vangen in het aantal kwetsbaarheden in computersystemen. Een kwetsbaarheid kan namelijk worden gebruikt om een cyberaanval uit te voeren. Symantec heeft in het Internet Security Threat Report het totaal aantal kwetsbaarheiden voor de afgelopen tien jaar op een rij gezet. In onderstaande figuur zijn daarvan de uitkomsten te zien.

[38] CBS (2016) ICT, Kennis en Economie.



Figuur 10 Aantal ontdekte kwetsbaarheden[39]

De afgelopen tien jaar is het aantal ontdekte kwetsbaarheden redelijk stabiel gebleven tussen de 4.500 en 6.500; uitschieters waren de jaren 2010, 2013 en 2014. Naast de ontdekte kwetsbaarheden zijn er natuurlijk ook nog de kwetsbaarheden die nog niet ontdekt zijn.

Weerbaarheid

Voor het analyseren van de weerbaarheid tegen de verstoring door malware kijken wij naar de installatiegraad van antivirussoftware. De bescherming tegen virussen, Trojaanse paarden en wormen kan, naast het niet openen van discutabele bestanden, in de meeste gevallen geregeld worden door het installeren van een goede antivirussoftware. Volgens een studie van de Europese Unie had in 2014 82% van de ondervraagde Nederlanders antivirussoftware geïnstalleerd.[40] Microsoft kwam met een percentage van 80% tot 85% op een vergelijkbaar getal uit.[41]

Een groot deel van de Nederlanders heeft dus antivirussoftware geïnstalleerd. Het is echter niet direct te concluderen dat Nederlanders nu goed beschermd zijn tegen cyberaanvallen als virussen en Trojaanse paarden. Indien de antivirussoftware niet is ingeschakeld of niet regelmatig geüpdatet wordt, heeft deze weinig nut.

Conclusie

Bij verstoring door malware zijn geen duidelijke trends waar te nemen en lijken de dreigingen en weerbaarheid relatief stabiel te zijn. Het aantal ontdekte kwetsbaarheden lag de afgelopen tien jaar tussen de 4.500 en 6.500. Daarnaast is ook het gebruik van antivirussoftware de afgelopen jaren niet substantieel veranderd. Het is zeer waarschijnlijk dat bij verstoring door malware vooral sprake is van een statische gap.

---

[39] Symantec (2016) *Internet Security Threat Report*.
[40] European Commission (2014) *Cyber Security Report.*
[41] Microsoft (2016) *Security Intelligence Report. Regional Threat Assessment.*

8. Conclusie

Voor elk van de cyberaanvallen hebben we in de voorgaande paragrafen een inschatting gegeven van de adoptiedynamiek in de dreigingen en de weerbaarheid. De samenhang tussen de dreigingen en weerbaarheid geeft aan in welke mate sprake is van een *gap.* Op basis van onze trendanalyse zien wij de volgende typen cyberaanvallen:

1. *Cyberaanvallen met kleine, statische gap*. Cyberfraude lijkt onder controle (althans op een voor de banken acceptabel niveau), al zien we hier nog wel nieuwe varianten van ontstaan. Doordat de weerbaarheid inmiddels hoog genoeg is, blijft de schade van deze nieuwe varianten beperkt. Verstoring door malware lijkt voor het grootste gedeelte opgelost te zijn, maar er bestaat nog steeds een niet te onderschatten statische gap. Dat betekent dat deze cyberaanvallen blijvend voor (grote) schade kunnen zorgen.
2. *Cyberaanvallen met grote, statische gap.* Bij digitale spionage lijkt de statische gap door te tijd gezien hoog te blijven. Dit komt omdat het hier gaat om aanvallen met hoge (eenmalige) opbrengst en waar veel geld en middelen voor beschikbaar zijn. Daarmee krijgen aanvallers toegang tot geavanceerde tools en *zero-day exploits*, waartegen nauwelijks bescherming mogelijk is (en blijft).
3. *Cyberaanvallen met dynamische gap*. Bij ransomware en DDoS-aanvallen lijkt nog sprake te zijn van een dynamische gap. Het aantal manifestaties neemt nog toe, mede door de opkomst van *as-a-service* modellen (beide) en IoT (DDoS). Voor beide type aanvallen wordt op dit moment wel veel gedaan om de weerbaarheid te vergroten zoals het *No More Ransom*-initiatief en de nationale anti-DDoS-wasstraat. Wij verwachten dat deze maatregelen binnen afzienbare tijd effect zullen hebben, maar dat het nog wel enige tijd in beslag zal nemen voor het aantal manifestaties zal afnemen. Het is niet met zekerheid te zeggen wanneer het aantal manifestaties zal afnemen en hoe groot de (uiteindelijke) statische gap zal zijn.

Tot slot

Er is een aantal belangrijke kanttekeningen dat bij onze analyse en deze uitkomsten moet worden geplaatst:

1. In de analyse wordt geen rekening gehouden met *nieuwe, onbekende* vormen van cyberaanvallen. Dat is, zoals in het begin van dit hoofdstuk wordt beschreven, een bewuste keuze. De innovatieve dreigingen zijn fundamenteel niet te voorspellen en *juist daarom* zeer gevaarlijk. Zouden we ze wel kunnen voorspellen, dan waren het geen dreigingen geweest.
2. Er zijn andere cyberaanvallen die op dit moment spelen, maar niet in de analyse zijn meegenomen. We hebben gekozen voor een focus op de vijf meest relevante. Dat wil niet zeggen dat andere aanvalstypen geen grote impact hebben op specifieke plekken in de maatschappij.
3. We hebben onze analyse gebaseerd op publiek bekende informatie over cyberaanvallen. Dat klinkt triviaal, maar is een belangrijke kanttekening, aangezien een groot deel van de dreiging en dreigingsactoren zich aan het oog van politie en justitie weet te onttrekken. Het is, anders gezegd, niet mogelijk om in te schatten wat de omvang is van iets dat niet kan worden ‘gezien’.

Wie was Rathenau?

Het Rathenau Instituut is genoemd naar professor dr. G.W. Rathenau (1911-1989). Rathenau was achtereenvolgens hoogleraar experimentele natuurkunde in Amsterdam, directeur van het natuurkundig laboratorium van Philips in Eindhoven en lid van de Wetenschappelijke Raad voor het Regeringsbeleid. Hij kreeg landelijke bekendheid als voorzitter van de commissie die in 1978 de maatschappelijke gevolgen van de opkomst van micro-elektronica moest onderzoeken. Een van de aanbevelingen in het rapport was de wens te komen tot een systematische bestudering van de maatschappelijke betekenis van technologie. De activiteiten van Rathenau hebben ertoe bijgedragen dat in 1986 de Nederlandse Organisatie voor Technologisch Aspectenonderzoek (NOTA) werd opgericht. NOTA is op 2 juni 1994 omgedoopt in Rathenau Instituut.

Rathenau Instituut

Onderzoek & dialoog | Wetenschap, technologie en innovatie