Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2019–2020

26 643 Informatie- en communicatietechnologie (ICT)

33 552 Slachtofferbeleid

Nr. 696 **BRIEF VAN DE MINISTER VAN JUSTITIE EN VEILIGHEID**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 29 juni 2020

De dreiging van cybercrime is onverminderd groot, terwijl de afhankelijkheid van het internet is toegenomen. Het aanpakken van criminelen die misbruik maken van het internet vraagt daadkrachtig optreden. Met deze brief informeer ik u, mede namens de Minister voor Rechtsbescherming en de Staatssecretaris van Economische Zaken en Klimaat, over de voortgang van de integrale aanpak van cybercrime. Hierover heb ik u eerder op 12 juni 2019 geïnformeerd (Kamerstuk 28 684, nr. 564). In de brief zet ik de belangrijkste acties van het afgelopen jaar uiteen. De bijlage bevat meer gedetailleerde informatie per maatregel. De aanpak van cybercrime en de versterking van cybersecurity vertonen samenhang. Over de voortgang van de Nederlandse Cybersecurity Agenda[1] (NCSA) wordt u apart geïnformeerd.

Cybercrime is voortdurend in ontwikkeling. Een adequate bescherming van de samenleving tegen cybercrime vereist de doorlopende verwerking van nieuwe inzichten en ontwikkelingen. In het afgelopen jaar zijn meerdere wetenschappelijke onderzoeken naar cybercrime gepubliceerd.[2] In expertsessies is gekeken hoe de onderzoeksresultaten verwerkt kunnen worden in de aanpak. De wetenschappelijke inzichten ondersteunen de opzet en de maatregelen van de huidige aanpak. Op enkele punten worden de maatregelen verfijnd en aangepast. In deze brief worden de uitkomsten per spoor uiteengezet.

Algemeen beeld – cybercrime blijft een dreiging

De dreiging van cybercrime voor burgers en organisaties is zeer reëel. De afgelopen jaren toonden een toename van cybercrime. Ook in de

[1] Kamerstuk 26 643, nr. 536.
[2] Kamerstukken 28 684 en 33 552, nrs. 589, 593 en 595.

kst-26643-696
ISSN 0921 - 7371
's-Gravenhage 2020

coronacrisis bleef cybercrime verontrustend verder stijgen.[3] Door de coronacrisis neemt de afhankelijkheid van digitale dienstverlening bovendien toe, door het thuiswerken, het volgen van online onderwijs en de toename van online bestellingen bij webwinkels. Criminelen maken misbruik van deze afhankelijkheid. Daarbij toont de coronacrisis eens te meer dat criminelen snel inspelen op ontwikkelingen in de samenleving.[4] Het lijkt erop dat online criminaliteit in de coronacrisis definitief is doorgebroken als business model. Zo ziet de politie een forse toename van fraude via communicatieapps.

Door de goede Nederlandse ICT-infrastructuur en het gunstige vestigingsklimaat blijft Nederland een aantrekkelijk land voor cybercriminelen. Illegale activiteiten voltrekken zich op Nederlandse servers of worden (on)bewust gefaciliteerd door in Nederland gevestigde hosters. Het gebruik van geavanceerde digitale middelen blijft bovendien niet beperkt tot vormen van cybercrime. Ook bij andere criminaliteitsvormen ziet de politie een toename van het gebruik van deze middelen om misdrijven te plegen of af te schermen, geholpen door professionele dienstverleners.

Ransomware-aanvallen blijven een grote dreiging. De laatste jaren hebben met name zware, georganiseerde en technisch vaardige cybercriminelen *ransomware* als lucratief verdienmodel ontdekt.[5] Deze criminelen zijn in staat processen van grote bedrijven en instellingen te verstoren en hierbij (bedrijfs)informatie te vergaren. Naast de vergrendeling van systemen vindt bij *ransomware* in toenemende mate ook afpersing plaats door dreiging van de publicatie van informatie.[6] *Ransomware* leidt dan ook tot aanzienlijke financiële en economische schade.[7] *Phishing* blijft een veelvuldig gebruikte methode als initiëring van online criminaliteit. Hierbinnen ontstaan nieuwe werkwijzen, zoals *phishing* via sms *(smishing)* of andere communicatieapps.[8] Het aantal slachtoffers van computervredebreuk blijft stijgen ten opzichte van voorgaande jaren.[9] Ook *DDoS*-aanvallen zijn een blijvend risico.[10] De uitvoering van deze aanvallen blijft laagdrempelig vanwege de criminele dienstverlening. De hoeveelheid *DDoS*-aanvallen in Nederland is licht gedaald, maar lijken in omvang en duur toe te nemen.[11]

Ransomware-aanvallen

De *ransomware*-aanval op de Universiteit Maastricht toont de grote economische en maatschappelijke impact die *ransomware* kan hebben. Nadat de daders via twee *phishing*-mails toegang verkregen, verkenden ze twee maanden lang het netwerk om vervolgens de ransomware in te zetten. De universiteit betaalde vervolgens dertig bitcoins, ongeveer 200.000 euro, om weer toegang te krijgen tot het netwerk. Zowel het kabinet als het OM en de politie raden sterk af losgeld te betalen, omdat dit het criminele verdienmodel in stand houdt.[12]

---

[3] De term cybercrime betreft in deze brief criminaliteit waarbij ICT-systemen zowel doel als middel zijn. Voorbeelden daarvan zijn ransomware en inbreken in computersystemen («hacken»). Criminaliteit waarbij ICT-middelen enkel faciliterend zijn, zoals eenvoudige fraudevormen en online drugshandel, wordt aangeduid met de term gedigitaliseerde criminaliteit. De term online criminaliteit omvat beide.

[4] https://www.politie.nl/nieuws/2020/maart/31/cybercriminelen-spelen-in-op-coronavirus.html.

[5] Cybersecuritybeeld Nederland (CSBN) 2020.

[6] https://www.cyberscoop.com/maze-ransomware-mandiant-lessons-learned/.

[7] Internet Organised Crime Threat Assesment (iOCTA) 2019, Europol.

[8] CSBN, 2020.

[9] CBS, 2019. Veiligheidsmonitor.

[10] iOCTA, 2019.

[11] CSBN, 2020.

[12] Kamerstukken 26 643 en 28 684, nr. 678, Kamerstukken 31 288 en 26 643, nr. 832.

Preventie

Uit onderzoek naar slachtofferschap van online criminaliteit lijkt, naast de hoeveelheid internetgebruik, de manier waarop men zich op het internet gedraagt een risicofactor voor slachtofferschap te zijn.[13] Het onderzoek over veilig gedrag online toont bovendien dat respondenten zich minder veilig gedragen dan zij zelf denken. Meer kennis over de digitale wereld leidt daarbij lang niet altijd tot veilig gedrag.[14] Uit de expertsessies bleek dat voor gedragsverandering door betere bewustwording specifiekere en gerichtere communicatie aan verschillende doelgroepen meer effect kan hebben dan enkel algemene communicatie. In 2019 is mede op basis van een convenant met publieke en private partijen de publiekscampagne «Eerst checken, dan klikken» uitgevoerd. Gedurende de

coronacrisis is de campagne door convenantpartners opnieuw verspreid. Het convenant eindigde in mei 2020 en is inmiddels vernieuwd en verlengd voor drie jaar. De wetenschappelijke inzichten zijn verwerkt in het vernieuwde convenant. Hierin is opgenomen dat toekomstige algemene communicatie bij voorkeur aangevuld wordt met communicatie die zich richt op specifieke doelgroepen, vormen van cybercrime en/of preventieve handelingen. In het kader van de Roadmap Digitaal Veilige Hard- en Software is het Ministerie van EZK, in nauwe samenwerking met JenV, in november 2019 de campagne «Doe je updates» gestart. Deze campagne is specifiek gericht op de noodzaak van het regelmatig updaten van slimme apparaten.

Specifiekere communicatie wordt reeds ingezet voor jongeren, ouderen en laaggeletterden. Om deze groepen zo goed mogelijk te bereiken werkt JenV samen met jongeren- en ouderenorganisaties aan bewustwordings-activiteiten. Zo publiceerde www.scholieren.com een video gericht op jongeren met uitleg over hacken en het gebruik van sterke wachtwoorden. In 2019 richtte het jaarlijkse themanummer van het ledenblad van ouderenbond KBO-PCOB zich op cybercrime met daarin adviezen om online activiteiten veiliger uit te voeren. Zoals eerder is toegezegd, wordt later dit jaar een kleine campagne opgezet gericht op de weerbaarheid van ouderen en kwetsbare groepen tegen babbeltrucs.[15] Hierin wordt ook aandacht besteed aan cybercrime.

In 2020 steunt JenV wederom initiatieven en pilots van gemeenten, regionale samenwerkingsverbanden en Platforms Veilig Ondernemen (PVO) die zich richten op het vergroten van de weerbaarheid van jongeren, ouderen, laaggeletterden en ondernemers. Bezien wordt of deze samenwerking in de tweede helft van 2020 kan worden geformaliseerd in een City Deal «Lokale weerbaarheid cybercrime». Voor de invulling en ondertekening van deze City Deal vinden gesprekken plaats met de Ministeries van BZK en EZK, de Vereniging van Nederlandse Gemeenten (VNG) en een tiental gemeenten en regionale samenwerkingsverbanden, zoals PVO's.

Het onderzoek naar daderprofielen toont aan dat voor daders van cybercrime geen eenduidig profiel bestaat. Bij jongere daders bleken enkele kenmerken wel vaker voor te komen. Zij plegen strafbare feiten in eerste instantie vaker uit nieuwsgierigheid, intellectuele uitdaging of

---

[13] Simpta, T., & van Leijssen, E. M. C. (2019). *Slachtofferschap van online criminaliteit*, WODC.
[14] Hoff-de Goede, S., Kleij, R., Weijer S., & Leukfeldt, R. (2019). *Hoe veilig gedragen wij ons online?*. De Haagse Hogeschool – Centre of Expertise Cybersecurity.
[15] Kamerstuk, 28 684, nr. 619.

leergierigheid, en zijn zich niet altijd bewust van de strafbaarheid.[16] De in 2019 door de politie uitgevoerde campagne «je bent maar één klik verwijderd van cybercrime» richtte zich specifiek op het voorkomen van daderschap bij jongeren. In het voorjaar van 2020 is door de politie een snelle, toegespitste start gemaakt met het vervolg van deze campagne aangezien jongeren door de coronacrisis veel online zijn. Het bredere vervolg van de campagne is dit najaar voorzien. Over de aanpak van jeugdcriminaliteit wordt u door de Minister voor Rechtsbescherming nader geïnformeerd.

Uit de expertsessies blijkt het belang van technische maatregelen voor de preventie van cybercrime. In het kader van de Roadmap Digitaal Veilige Hard- en Software wordt in EU-verband gepleit voor het stellen van minimum digitale veiligheidseisen aan Internet of Things-apparaten. Daarnaast kunnen technische maatregelen helpen bij het tegengaan van specifieke criminaliteitsvormen, zoals blijkt uit de publiek-private aanpak van helpdeskfraude. In deze samenwerking tussen politie, OM en binnen- en buitenlandse private partijen zijn door een softwarebedrijf zelf technische aanpassingen gedaan aan hun softwareprogramma. Dit bemoeilijkt misbruik van deze software voor het plegen van helpdeskfraude.

Campagne «gamechangers»

Gedurende de coronacrisis is in april 2020 door de politie de campagne «GameChangers» gestart die zich richt op jongeren. Via online uitdagingen en games kunnen jongeren hun digitale vaardigheden testen en ontwikkelen. Zo leren ze cybercrime te herkennen en wordt hen een legaal alternatief geboden wat daderschap kan voorkomen. Met de uitdagingen zijn prijzen te winnen, zoals een politie-ervaring. Wegens succes is de campagne verlengd tot 1 juni en zijn nieuwe uitdagingen toegevoegd.

Opsporing, vervolging, sanctionering, verstoring

Conform de afspraken in de Veiligheidsagenda is in 2019 door de politie en het OM gestart met een eenheidsoverstijgende fenomeenaanpak, naast de reguliere opsporingsonderzoeken. Eenheden richten zich hierbij elk op de bestrijding van een cybercrimefenomeen met een integrale, multidisciplinaire aanpak. In totaal zijn in 2019 21 fenomeenonderzoeken afgerond en eind 2019 bevonden zich 35 onderzoeken in de tactische fase. Dit blijft achter bij de ambitie van 41 onderzoeken. Met 381 reguliere onderzoeken is de landelijke beleidsdoelstelling van 310 ruimschoots gehaald. Het Team High Tech Crime (THTC) heeft negentien van de twintig geambieerde zaken afgerond. Het THTC en het Landelijk Parket constateren daarbij een toename in de (technische) complexiteit van de zaken. In de beantwoording van de Kamervragen over het Jaarverslag 2019 is toegezegd in deze brief voor 2017, 2018 en 2019 het gecorrigeerde aantal veroordelingen voor cybercrime te noemen dat heeft plaatsgevonden nadat hoger beroep is ingesteld.[17] In 2017 zijn 69 meerderjarigen en 9 minderjarigen na hoger beroep veroordeeld. In 2018 ging het om 91 meerderjarigen en 15 minderjarigen, in 2019 betrof het 118 meerderjarigen en 10 minderjarigen.

Het Regeerakkoord heeft bij de politie een uitbreiding van 145 fte mogelijk gemaakt. Na vertraging in de startfase verloopt de werving van politiepersoneel met de juiste expertise inmiddels goed. Naar verwachting is de

[16] Van der Wagen, W., Van't Zand-Kurtovic, E. G., & Fischer, T. F. C. (2020). *Cyberdaders: uniek profiel, unieke aanpak?* WODC.
[17] Kamerstuk 35 470 VI, nr. 1.

werving voor de zomer van 2020 afgerond. Deze medewerkers worden onder andere ingezet bij de cybercrimeteams in de regionale eenheden om de fenomeenaanpak te versterken. De beschikbare capaciteit bij het OM blijft achter bij de politie. De cybercrimeteams werken in een landelijke structuur samen met het THTC en ondersteunen districtsrecherches en basisteams bij de kennisopbouw voor de uitvoering van reguliere onderzoeken naar cybercrime. Dit heeft een positieve invloed op het aantal cybercrimezaken die de regionale eenheden uitvoeren. De cybercrimeteams ontwikkelen in publiek-private samenwerkingen bestrijdingsaanpakken voor fenomenen als *ransomware, phishing, DDoS*-aanvallen, *business email compromise*-fraude en helpdeskfraude.

Binnen de opsporingsonderzoeken die de politie en het OM uitvoeren richten zij zich onder meer op hostingbedrijven die bewust criminaliteit faciliteren, zogenaamde *bullet proof hosters*. Daarnaast wordt in Nederland ook criminaliteit gefaciliteerd door hostingbedrijven die daar zelf (mogelijk) geen weet van hebben. De meeste grote hostingbedrijven gaan dergelijk misbruik van hun systemen actief tegen. Er lijken echter ook bedrijven te zijn die hier weinig werk van maken. In de hostingsector komen bovendien vaak «reseller»-constructies voor, waarbij hostingcapaciteit wordt doorverhuurd. Deze constructies compliceren de opsporing en vervolging van cybercrime. De Ministeries van JenV en EZK werken met de politie en het OM aan maatregelen om het faciliteren van criminaliteit via hostingbedrijven tegen te gaan.

Sinds de inwerkingtreding per 1 maart 2019 van de Wet Computercriminaliteit III wordt de nieuwe bevoegdheid tot het heimelijk en op afstand binnendringen in een geautomatiseerd werk meermaals ingezet. U bent inmiddels geïnformeerd over het aantal inzetten van deze bevoegdheid in 2019.[18] Vanaf 2021 wordt het jaarlijkse aantal inzetten gepubliceerd in het Jaarverslag van JenV. In het Regeerakkoord is afgesproken de wet na twee jaar te evalueren. Omdat de evaluatie naar verwachting erg omvangrijk wordt en er voor de andere onderdelen van de wet naar verwachting na twee jaar beperkt gegevens beschikbaar zijn, heb ik besloten de evaluatie in eerste instantie te beperken tot de bevoegdheid tot binnendringen in een geautomatiseerd werk. Voor de overige onderdelen van de wet wordt aangesloten bij de gebruikelijke evaluatietermijn van vijf jaar na inwerkingtreding.

Tot slot blijkt uit het onderzoek naar daders van cybercrime dat bij het voorkomen van recidive klassieke interventies bruikbaar zijn, indien ze worden aangepast aan de digitale context. De pilot Hack_Right, waarbij Halt samen met het OM, de politie, de Raad voor de Kinderbescherming, Reclassering Nederland en het bedrijfsleven werkt aan een aanvullende interventie voor jonge daders is verlengd tot 31 december 2021.

Opsporingsonderzoeken bullet proof hosters

In 2019 is in samenwerking met de Nederlandse politie in Duitsland een *bullet proof hoster* ontmanteld, gevestigd in een oude NAVO-bunker. Vanuit deze «cyberbunker» hostten de zeven verdachten een omvangrijke, wereldwijde online drugsmarktplaats. Vier van de verdachten waren Nederlanders. Ook is in 2019 de *bullet proof hoster* KV Solutions opgerold, waarbij een versie van het Mirai-botnet uit de lucht is gehaald. Via dit grote botnet werden DDoS-aanvallen uitgevoerd.

[18] Kamerstuk 35 470 VI, nr. 1.

Aandacht voor het slachtoffer

Recent onderzoek naar slachtofferschap van online criminaliteit toont dat de impact van online delicten groot kan zijn. Daarnaast hebben slachtoffers soms te maken met onbegrip uit hun omgeving. Er is behoefte aan erkenning van het slachtofferschap, ook vanuit overheidsinstanties. Inmiddels zijn enkele nieuwe maatregelen genomen om slachtoffers beter te ondersteunen. Begin 2020 is Slachtofferhulp Nederland (SHN) een campagne gestart gericht op slachtoffers van online criminaliteit. Via het programma «Mens als maat» ontwikkelt SHN instrumenten voor de omgeving van slachtoffers om deze beter te ondersteunen. Het OM is in 2020 begonnen met de inzet van slachtoffercoördinatoren bij impactvolle zaken, waaronder online delicten.

Campagne Slachtofferhulp Nederland

In mei 2020 is de campagne «Van oplichting naar opluchting» van Slachtofferhulp Nederland van start gegaan. Deze campagne deelt de verhalen van slachtoffers van *phishing* en andere vormen van online criminaliteit. Slachtoffers worden gestimuleerd te praten over het delict, waarbij zij online steun kunnen vinden bij lotgenoten. Het doel is om schaamte weg te nemen en de impact van slachtofferschap te verkleinen.

Wetenschappelijk onderzoek

De inzichten uit de gepubliceerde onderzoeken zijn waardevol gebleken voor de aanpak. Momenteel lopen nog twee onderzoeken bij het WODC. De resultaten daarvan worden in 2020 en 2021 verwacht. Daarnaast voeren andere kennisinstellingen onderzoek uit naar cybercrime en gerelateerde onderwerpen. Het blijft van belang wetenschappelijke inzichten te verwerken in de aanpak en nieuw onderzoek dat bijdraagt aan de aanpak waar mogelijk te stimuleren. Om tegemoet te komen aan de gewijzigde motie van het lid Van Toorenburg[19] om te bezien of een nationaal rapporteur voor internetcriminaliteit gewenst is, zal onderzoek worden uitgevoerd naar lacunes in het overheidsbeleid inzake online content vanuit een burgerperspectief.

Tot slot

De samenleving digitaliseert, waarbij de online en offline levens van burgers zich in toenemende mate vermengen. Ook criminelen vinden steeds beter hun weg op het internet. Een veilige online samenleving vraagt een toekomstbestendige aanpak van cybercrime. De overheid en private partijen hebben hierin een gezamenlijke verantwoordelijkheid. Samenwerking blijft daarom een belangrijk uitgangspunt. Het afgelopen jaar leverden vele partijen onophoudelijke inspanningen en boekten successen. Tegelijkertijd blijft de dreiging van cybercrime groot en ontwikkelen criminaliteitsvormen zich in rap tempo. De bestrijding van cybercrime blijft hierdoor onverminderd van belang.

De Minister van Justitie en Veiligheid,
F.B.J. Grapperhaus

[19] Kamerstuk 34 602, nr. 4.

Bijlage – overzicht maatregelen

Preventie

Flexibele, snel inzetbare preventiecampagnes

In 2019 is de brede publiekscampagne «Eerst checken, dan klikken» uitgevoerd. Het doel van de campagne was om mensen bewust te maken van de gevaren van *phishing* en aan te sporen tot veiliger online gedrag. Ook is aandacht gevraagd voor fraude via communicatieapps. Bij de uitvoering van de campagne is samengewerkt met private partijen en technisch experts van buiten de overheid. De campagne is via TV, online artikelen en displays, sociale mediakanalen en kanalen van de convenantpartners verspreid. Hierbij zijn ook specifieke uitingen gedaan richting jongeren en ouderen. Het effectonderzoek toont een bovengemiddelde waardering voor de campagne en de afzonderlijke uitingen daarvan ten opzichte van andere Rijksoverheidcampagnes. De uitingen slaan aan bij de doelgroep en geven veel nieuwe informatie. Uit het effectonderzoek blijkt echter dat het controleren van links en bijlagen, en kennis daarover achterblijft. Het blijkt dat na een combinatie van media-uitingen mensen aangeven vaker links en/of plotselinge betaalverzoeken te controleren. Het effect van de campagne op gedragsverandering lijkt echter nog beperkt. De uitingen gericht op ouderen zijn goed ontvangen. Het aantal lezers van de berichtgeving met tips en uitleg over internetcriminaliteit is hoger dan verwacht. Gedurende de coronacrisis brachten convenantpartners en andere betrokkenen nogmaals het gevaar van *phishing* onder de aandacht, met name via sociale media. Het convenant «Eerst checken, dan klikken» is in mei 2020 met drie jaar verlengd. Deze voortzetting richt zich op de preventie van cybercrime met aandacht voor specifieke thema's. De convenantpartners kunnen zo communicatie specifieker uitdragen naar hun doelgroep of branche.

Eind 2019 en begin 2020 is door het Ministerie van EZK, in nauwe samenwerking met het Ministerie van JenV, de campagne «Doe je updates» uitgevoerd. Het doel was om consumenten voor te lichten over de noodzaak van het regelmatig updaten van slimme apparaten. Deze updates beveiligen de meeste slimme apparaten. Consumenten zijn hier echter beperkt van op de hoogte. Het overbrengen van deze kennis is daarom van belang voor de digitale weerbaarheid van burgers. De campagne is via online kanalen, radiocommercials en muziekdiensten verspreid. In de campagnes van de Ministeries van JenV en EZK wordt verwezen naar www.veiliginternetten.nl en voor het bedrijfsleven naar www.digitaltrustcenter.nl. Mede door deze campagnes, de cybersecurity-maand in oktober en Alert Online is breder ingezet op preventie van cybercrime en cyberveiligheid. Gezamenlijk hebben deze initiatieven veel mensen bereikt. Dit is deels terug te zien in de verdubbelde bezoekersaantallen van www.veiliginternetten.nl in de maanden juni en oktober 2019, en februari 2020. In de toekomst blijven de Ministeries van JenV en EZK samenwerken bij preventieactiviteiten gericht op het weerbaarder maken van burgers en organisaties.

In 2019 heeft de politie de campagne «je bent maar één klik verwijderd van cybercrime» uitgevoerd, gericht op daderpreventie bij jongeren. Deze geslaagde campagne is beloond met de Lovie Award en de SpinAward. Gedurende de coronacrisis is een snelle en beperkte start gegeven aan het vervolg van deze campagne. Via de campagne «GameChangers» worden jongeren die vanwege de coronamaatregelen veel online zijn behoed voor het plegen van strafbare feiten. Via meerdere uitdagingen en games wordt jongeren een legitiem alternatief geboden, waarbij zij hun vaardigheden kunnen testen en verbeteren. Bovendien wordt voorlichting

gegeven over de strafbaarheid van cybercrime. De campagne is vanwege succes verlengd tot 1 juni. Hierbij zijn de bestaande uitdagingen verlengd en zijn nieuwe uitdagingen toegevoegd. Het bredere vervolg van de campagne is in het najaar van 2020 voorzien.

Ondersteuning veiligheid niet vitale bedrijfsleven: Digital Trust Center (DTC)

Het doel van het DTC is om het niet vitale deel van ondernemend Nederland in staat te stellen zich weerbaarder te maken tegen cyberaanvallen.[20] Vanwege het belang van veilig digitaal ondernemen wordt het DTC na de programmaperiode van 2018–2020 een vast organisatieonderdeel van het Ministerie van EZK. Hiervoor is structureel financiering beschikbaar. Op deze manier blijft het DTC ondernemend Nederland cyberweerbaar maken. Daarnaast wordt gewerkt om het DTC te laten voldoen aan de wettelijke voorwaarden die worden gesteld aan een OKTT.[21] Een wettelijke basis biedt het DTC meer mogelijkheden om vertrouwelijke informatie over risico's en dreigingen te delen met het niet-vitale bedrijfsleven. Zo kunnen bedrijven hun eigen cyberweerbaarheid verbeteren.

In november 2019 is het digitale platform van het DTC gestart. Via deze digitale ontmoetingsplaats kunnen ondernemers afgeschermd kennis delen over veilig digitaal ondernemen. Daarnaast waren bij het DTC eind 2019 twintig samenwerkingsverbanden van bedrijven aangesloten. Het doel is dit in 2020 uit te breiden naar dertig. Deze samenwerkingsverbanden zijn sectoraal of regionaal georganiseerd. Ook zal het DTC deze zomer informatiepakketten voor brancheorganisaties en gemeenten beschikbaar maken. Op deze manier wordt informatiedeling nog meer gestimuleerd.

Ondersteuning gemeenten en MKB-ondernemingen

In de samenwerking met het Ministerie van BZK en het DTC heeft het Ministerie van JenV in 2020 wederom subsidie verstrekt aan gemeenten, regionale samenwerkingsverbanden veiligheid en Platforms Veilig Ondernemen (PVO). De gesteunde initiatieven zijn gericht op het vergroten van de cyberweerbaarheid van jongeren, ouderen, laaggeletterden en ondernemers. Door deze steun kunnen deze organisaties hun rol bij de preventie van cybercrime beter invullen. Bezien wordt of dit samenwerkingsverband in de tweede helft van 2020 kan worden geformaliseerd in een City Deal. In deze City Deal ontwikkelen interbestuurlijke partners, het bedrijfsleven en kennisinstellingen nieuwe aanpakken om de doelgroepen beter te bereiken en gedragsverandering te bewerkstelligen. Momenteel voert het Ministerie van JenV met het Ministerie van BZK, het DTC, de VNG, gemeenten en regionale samenwerkingsverbanden gesprekken over de invulling van deze City Deal.

Binnen de City Deal wordt tevens de verbinding gelegd met het actieprogramma «Veilig Ondernemen 2019–2022». Dit actieprogramma dient ter versterking van de digitale veiligheid in het MKB. Hierin wordt onder andere experimenteel onderzoek uitgevoerd om het risico van slachtofferschap bij MKB-ondernemingen in de metaalsector te verkleinen. In 2020 is de eerste tussenrapportage opgeleverd en wordt verder onderzoek gedaan naar interventies en de implementatie hiervan. De tussenrap-

[20] Voor de vitale sectoren vervult het NCSC deze functie.

[21] Aanwijzen van het DTC als een organisatie, bedoeld in artikel 3, tweede lid, onderdeel a, Wet beveiliging netwerk- en informatiesystemen, op grond waarvan het NCSC meer informatie over dreigingen en incidenten met het DTC zou kunnen delen.

portage beschrijft de omvang van het probleem, de risicogedragingen en de gedragsdeterminanten van cyber(on)veilig gedrag. Hierna wordt een overzicht met kansen voor gedragsverandering en mogelijke gedragsinterventies gemaakt. Deze kansen worden vervolgens getest in een proeftuin. Publicatie wordt begin 2021 verwacht. Het Ministerie van JenV heeft in aanvulling op het actieprogramma subsidie verstrekt aan pilots die zich richten op cyberweerbaarheid in het MKB. Daarnaast worden er ook dit jaar weer (digitale) bijeenkomsten georganiseerd door PVO's om de bewustwording in het MKB te vergroten.

Digitaal veilige hard- en software

In het kader van de Roadmap Digitaal Veilige Hard- en Software (DVHS) is afgelopen jaar voortgang geboekt bij het verhogen van het cybersecurityniveau van ICT-producten en -diensten en het Internet of Things (IoT). Over de voortgang van de Roadmap DVHS wordt u in het najaar door de Staatssecretaris van Economische Zaken en Klimaat geïnformeerd. De Europese Commissie heeft in 2019 impactstudies uitgevoerd naar het stellen van wettelijke minimumeisen aan de veiligheid van IoT-apparaten via de *Radio Equipment Directive*. Naar verwachting gaat de Commissie dit jaar over tot het formuleren van de noodzakelijke gedelegeerde handelingen. Nederland zet er op in dat de eisen eind 2020 van kracht worden, zodat op termijn minimale veiligheidseisen gelden voor alle apparaten die zijn verbonden met het internet.

In 2019 is de Europese *Cyber Security Act* in werking getreden. Deze verordening vormt een raamwerk voor de certificering van ICT-producten, -diensten en -processen. Inmiddels is begonnen met de ontwikkeling van Europese certificeringschema's voor onder andere clouddiensten. Nederland draagt via het publiek-private *Partnering Trust* bij aan de ontwikkeling van dit schema.

Voor bedrijven en organisaties is toegang tot betrouwbare en kwalitatief hoogwaardige private cybersecuritydienstverlening belangrijk. De Ministeries van JenV en EZK hebben een subsidie verstrekt aan het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) om een risicomodel en kwaliteitsregeling voor leveranciers van cybersecuritydiensten te ontwikkelen. Dit bevordert een basisniveau van betrouwbaarheid en kwaliteit. Oplevering hiervan wordt medio 2020 verwacht, waarna in de tweede helft van dit jaar pilots plaatsvinden en mogelijke verbeteringen worden doorgevoerd. Begin 2021 vindt de definitieve vaststelling en publicatie plaats.

Met bovenstaande passage voldoe ik aan de toezegging van de Minister voor Rechtsbescherming om de Kamer te informeren over de wijze waarop apparaten veiliger kunnen worden gemaakt. Deze toezegging is gedaan tijdens het plenair debat over internetpesters op 18 februari 2020.

Opsporing, vervolging, sanctionering en verstoring

Versterking aanpak van de politie en in de strafrechtketen

De gelden uit het Regeerakkoord hebben onder andere bijgedragen aan de uitbreiding van cybercrimeteams in de regionale eenheden van de politie. Het afgelopen jaar zijn ondanks de lastige situatie op de arbeidsmarkt tachtig fte geworven. Naar verwachting is de werving van in totaal 145 fte in de zomer van 2020 afgerond. De extra capaciteit bij de politie is onder meer ingezet voor de versterking van regionale cybercrimeteams bij de fenomeenaanpak. De capaciteit op cybercrime bij het OM blijft hierbij achter. De fenomeenonderzoeken kunnen zich richten op de

opsporing van criminele samenwerkingsverbanden, maar hebben ook aandacht voor preventie- en verstoringsmogelijkheden. De operationele coördinatie vindt plaats op landelijk niveau. Tussen de basisteams, districtsrecherches, cybercrimeteams en het THTC is de samenwerking versterkt. Ook werkt de politie bij de bestrijding van cybercrime samen met het Nederlands Forensisch Instituut. Voor 2020 zijn inmiddels nieuwe afspraken gemaakt in de Veiligheidsagenda.

Bewustwording hostingproviders

Diverse rapporten tonen dat de Nederlandse hostingsector veelvuldig wordt gebruikt door criminelen voor het plegen van strafbare feiten. Criminaliteit wordt gefaciliteerd door malafide *(bullet proof hosting)* dan wel onwetende hostingbedrijven die zeer weinig maatregelen nemen *(bad hosting)*. De Ministeries van JenV en EZK, de politie en het OM werken samen aan een aanpak. Daarbij wordt tevens samenwerking met private partijen gezocht, waarbij aandacht is voor de eigen rol en verantwoordelijkheid van de diverse partijen. Deze aanpak is breder dan alleen bewustwording. Het Ministerie van EZK verkent in samenwerking met het Ministerie van JenV de mogelijkheden voor het wijzigen van EU-regelgeving. Verder werken de politie, het OM en een private partij binnen een *Organized Crime Field Lab*, een innovatieve werkvorm, aan maatregelen tegen *bad hosting*.

Verstoring crimineel verdienmodel

De politie heeft bij de aanpak van cybercrime gebruik gemaakt van alternatieve interventies om het maatschappelijk effect te vergroten. In publiek-private samenwerkingen is voor enkele criminaliteitsfenomenen inmiddels een bestrijdingsaanpak ontwikkeld. Dit geeft zicht op meerdere interventiemogelijkheden, van preventie, schadebeperking, slachtoffernotificatie en verstoring tot opsporing.

Het project NoMoreRansom, dat *ransomware*-aanvallen verstoort, bestond in 2019 drie jaar. Inmiddels zijn wereldwijd 150 partners aangesloten en zijn losgeldbetalingen ter waarde van ruim honderd miljoen euro voorkomen. Door de Electronic Crimes Taskforce, bestaande uit de politie, het OM en de bankensector, is het project NoMorePhishing opgezet om *phishing*-aanvallen structureel te verstoren. Bij de bestrijding van DDoS-aanvallen sloot het door de politie opgezette project NoMoreDDoS zich in 2019 aan bij een breder samenwerkingsverband van 25 publieke en private partners. Hierbij wordt een gezamenlijke database ontwikkeld met informatie over de digitale vingerafdruk van DDoS-aanvallen ten behoeve van beschermende maatregelen en de opsporing. Tot slot zijn bij de aanpak van de helpdeskfraude technische maatregelen doorgevoerd, vindt scherper toezicht door de ACM plaats en geven partners preventieadviezen. De schade van helpdeskfraude is gedaald van zes miljoen euro in 2017 naar drie miljoen euro in 2019.

Versterking nationale wetgeving

Gestart is met de inventarisatie van mogelijke wijzigingen van nationale wetgeving die bijdragen aan de aanpak van cybercrime. Bezien wordt in hoeverre de geïnventariseerde wijzigingen nodig zijn en hoe deze zich verhouden tot lopende wetgevingstrajecten, zoals de modernisering van het Wetboek van Strafvordering, de Innovatiewet Strafvordering en de aanbevelingen van de Commissie Koops. Ook wordt de instelling van een Adviescommissie «technologische ontwikkelingen in de (forensische) opsporing» verkend.

Internationale samenwerking

De politie en het OM werken aan het versterken van de rechtshulpprocessen voor digitaal bewijs. Het 24/7 contactpunt is inmiddels georganiseerd binnen de informatieorganisatie, zodat de werkzaamheden van het contactpunt minder interfereren met de landelijke opsporingsonderzoeken.

Internationale samenwerking is voor de politie een belangrijk onderdeel van de bestrijding van cybercrime. Zo was het THTC tot april 2020 voorzitter van de *Joint Cybercrime Action Taskforce* (J-CAT) van Europol. Speerpunten van de J-CAT waren DDoS-bestrijding, de aanpak van dienstverlening voor versleutelen en verhullen van malware en het lokaliseren van verborgen cybercriminele infrastructuren.

Versterking internationale juridische kaders

Sinds 2018 draagt Nederland actief bij aan de Europese discussie over de E-evidence-verordening. Hoewel Nederland groot belang hecht aan de versterking van de regelgeving op dit terrein, was Nederland genoodzaakt in de JBZ-raad geen steun te verlenen aan de algemene oriëntatie. Dit omdat onvoldoende tegemoet was gekomen aan de wensen van Nederland voor een notificatiemechanisme. De JBZ-raad heeft het voorstel wel aangenomen. Nederland richt zich nu op de discussies in het Europees Parlement en de triloog. In 2019 is ook een akkoord bereikt over de bijbehorende richtlijn over het aanwijzen van een juridisch vertegenwoordiger in de EU door private dienstverleners.

In het kader van de Raad van Europa blijft Nederland actief deelnemen aan de gesprekken over een tweede protocol bij het Cybercrimeverdrag. Dit geldt ook voor de gesprekken met de Commissie die onderhandelt met de Verenigde Staten over een EU-VS overeenkomst inzake grensoverschrijdende toegang tot elektronisch bewijsmateriaal voor justitiële samenwerking in strafzaken. U wordt hierover periodiek geïnformeerd in de geannoteerde JBZ-agenda's.

Aanpak jonge (potentiële) daders en beperking recidive

Samen met onder meer de politie, het OM, Halt en de Raad voor de Kinderbescherming worden het risicotaxatie- en diagnose-instrumentarium (LIJ) en het interventiepalet voor jeugdige cyberdaders aangevuld.

In de pilot Hack_Right beproeven het OM en de politie in samenwerking met Halt, de Raad voor de Kinderbescherming, de reclassering en het bedrijfsleven een alternatieve invulling van sancties voor jeugdige *first offenders* van cybercrime. Inmiddels zijn 22 (cybersecurity)bedrijven aangesloten.
Negentien jongeren hebben het programma succesvol doorlopen. Gestart is met de voorbereidingen om Hack_Right te laten toetsen door de Justitiële Erkenningscommissie. Zo werkt men aan een wetenschappelijk onderbouwde handleiding voor begeleiders van alle partners uit de strafrechtketen en het bedrijfsleven.

De reclassering voert een project uit dat zich richt op het bevorderen van kennis over cybercrime en daderprofielen, en het ontwikkelen van nieuwe of aanvullende werkwijzen en interventies voor cyberdaders. Dit project is verlengd tot eind 2020. De reclassering heeft een training «gedigitaliseerde criminaliteit» ontwikkeld. Veel reclasseringswerkers hebben deze inmiddels gevolgd. Daarnaast is een Landelijke Kenniskring Cybercrime

opgericht met daarin reclasseringswerkers uit iedere regio. Hen worden activiteiten aangeboden om de expertise op het gebied van cybercrime te vergroten. Via de Confederation of European Probation (CEP) is met een survey uitgevraagd hoe andere Europese reclasseringsorganisaties omgaan met cybercrime.

Verbetering aangifteproces

De politie heeft initiatieven gestart om het aangifteproces van cybercrime te verbeteren. Cybercrimeteams ondersteunen intake- en servicemedewerkers bij aangiftes van cybercrime en in enkele eenheden worden cybervrijwilligers ingezet bij de intake. Digitale aangifte is mogelijk gemaakt voor helpdeskfraude en fraude via communicatieapps. Dit wordt uitgebreid voor meer delicten. Deze digitale aangiftemodule helpt ook de intake- en servicemedewerkers bij het opnemen van aangiften.

Aandacht voor slachtoffers

Ondersteuning slachtoffer

Slachtofferhulp Nederland (SHN) biedt emotionele, juridische en praktische hulp aan slachtoffers. SHN rekent hiervoor geen kosten. Om slachtoffers nog beter te kunnen helpen worden in het programma «mens als maat» van SHN instrumenten ontwikkeld voor de omgeving van het slachtoffer. Daarbij is er specifiek aandacht voor slachtoffers van online criminaliteit, aangezien deze slachtoffers soms onbegrip uit hun omgeving ervaren. Daarnaast heeft SHN online lotgenotengroepen opgericht voor slachtoffers van online criminaliteit. Ook startte SHN dit jaar de campagne «Van oplichting naar opluchting». De campagne deelt verhalen van *phishing* en andere vormen van online criminaliteit, om zo slachtoffers te stimuleren te praten over het delict. Zij kunnen steun vinden bij lotgenoten in online groepen.

Slachtoffercoördinatoren

Het OM is dit jaar begonnen met de inzet van slachtoffercoördinatoren voor impactvolle zaken. Slachtoffers van impactvolle zaken, waaronder bepaalde online delicten, kunnen hierdoor begeleiding krijgen om hun wensen tijdens het strafproces beter kenbaar te maken. Bovendien worden zij persoonlijk geïnformeerd over hun rechten en hun zaak, waardoor slachtoffers naar verwachting meer erkenning ervaren. Momenteel worden meer slachtoffercoördinatoren geworven.

Voeging slachtoffers strafproces

Vanwege de schaalmogelijkheden van het internet maken cybercriminelen vaak veel slachtoffers tegelijkertijd. Gekeken wordt of bij grote aantallen slachtoffers de voeging van hen in het strafproces kan worden verbeterd.

Slachtoffernotificatie en schadebeperking

Daders van cybercrime kunnen met één delict veel slachtoffers maken. Bovendien is niet iedereen van dit slachtofferschap op de hoogte. Om de schade te beperken en nieuw slachtofferschap te voorkomen is het van belang slachtoffers snel te notificeren. Het op effectieve wijze delen van operationele gegevens blijkt echter juridisch niet altijd mogelijk. Bezien wordt of dit kan worden meegenomen bij de versterking van de nationale wetgeving.

Wetenschappelijk onderzoek

Meerdere onderzoeken naar slachtofferschap en daderschap van cybercrime zijn inmiddels gepubliceerd. De uitkomsten hiervan zijn verwerkt in de aanpak van cybercrime. Het onderzoek naar de aard en omvang van cyber- en gedigitaliseerde criminaliteit wordt naar verwachting na de zomer van 2020 gepubliceerd. De onderzoeken naar het verstoren van cyber- en gedigitaliseerde criminaliteit en het onderzoek naar de strafrechtelijke aanpak van cyber- en gedigitaliseerde criminaliteit zijn samengevoegd. Dit onderzoek is naar verwachting in 2021 gereed. Publicatie van een onderzoek naar de behoeften van burgemeesters in cyberspace is dit jaar voorzien. Buiten het WODC worden door andere kennisinstellingen onderzoeken van belang voor de aanpak van cybercrime uitgevoerd, onder meer bij de Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO).