Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2018–2019

28 684 Naar een veiliger samenleving

Nr. 564 **BRIEF VAN DE MINISTER VAN JUSTITIE EN VEILIGHEID**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 12 juni 2019

Op 20 april 2018 bent u geïnformeerd over de integrale aanpak van cybercrime (Kamerstuk 28 684, nr. 522). 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 aanpak. Ik beperk mij in deze brief tot de belangrijkste observaties. Voor meer gedetailleerde informatie per maatregel verwijs ik naar de bijlage. De aanpak van cybercrime en de versterking van cybersecurity worden in samenhang met elkaar vormgegeven. Over de voortgang van de brede Nederlandse cybersecurity agenda (NCSA) wordt u heden apart geïnformeerd (Kamerstuk 26 643, nr. 614).

Cybercrime blijft vaak voorkomen en neemt volgens diverse rapportages toe. De dreiging blijft onverminderd hoog en er is geen reden om aan te nemen dat dit in de nabije toekomst verandert. De inzet om burgers en organisaties te beschermen, daders op te sporen en te vervolgen, criminele werkwijzen te verstoren en slachtoffers te ondersteunen blijft nodig. Het afgelopen jaar is voortvarend invulling gegeven aan zowel bestaande als nieuwe initiatieven. Er wordt meer gedaan aan preventie en daders worden aangepakt. De regering heeft extra kunnen investeren in de aanpak. Naast de investeringen uit het Regeerakkoord (bijlage bij Kamerstuk 34 700, nr. 34) is eind 2018 bij Najaarsnota (Kamerstuk 35 095, nr. 1) een incidentele investering van € 30 miljoen mogelijk gebleken ten behoeve van cybersecurity en (ondermijnende) cybercrime. Een deel van dit bedrag is aangewend voor de integrale aanpak van cybercrime. Het betreft onder meer investeringen in de opsporingsmogelijkheden van de politie, kennisontwikkeling binnen het Openbaar Ministerie, publieksvoorlichting en ondersteuning van het lokaal bestuur.

Algemeen beeld cybercrime

De mogelijkheden om met diverse apparaten continu online te zijn en te communiceren brengt zowel kansen met zich mee als bedreigingen. Cybercrime is zeer schaalbaar. Er is inmiddels sprake van een omvangrijke

kst-28684-564
ISSN 0921 - 7371
's-Gravenhage 2019

mondiale, grotendeels ondergrondse cybercriminele online-economie, waarbij voor elke stap in het criminele proces diensten worden verhandeld. Ook Nederlandse ICT-infrastructuur wordt hiervoor veelvuldig aangeboden en er zijn hostingpartijen die vanuit Nederland criminaliteit faciliteren.[1] Door de laagdrempelige en gebruiksvriendelijke mogelijkheden is cybercrime uitvoerbaar voor een toenemende diversiteit aan daders, bijvoorbeeld zij die minder technisch onderlegd zijn. De politie constateert dat sommige dadergroepen in het zware criminele milieu hun activiteiten verruimen en naast traditionele misdrijven ook digitale delicten plegen. Enerzijds is er sprake van nieuwe typen daders, anderzijds wordt met technologie het scala aan tools en mogelijkheden voor «klassiekere» typen daders uitgebreid.

Het gebruik van *ransomware* groeit nog steeds en het wederrechtelijk overnemen van gegevens, vaak ten behoeve van andere strafbare feiten zoals fraude, is een prominente dreiging. Het gebruik van *social engineering* groeit ook, waarbij *phishing* via mails de meest gebruikte methode blijft.[2] *Phishing* blijft daarmee een veel gebruikte werkwijze, met zowel bij individuen als organisaties veel potentiële slachtoffers.[3] Het aantal aanvallen met behulp van *phishing* lijkt EU-breed stevig toe te nemen.[4] Cryptovaluta worden vaak misbruikt voor het witwassen van crimineel geld. Bij bonafide gebruikers van cryptovaluta wordt getracht deze te ontvreemden.[5] Het aantal geregistreerde gevallen van computervredebreuk neemt toe.[6] Van dit laatste is echter onduidelijk of dit wordt veroorzaakt door een reële toename van dit fenomeen of een toename van de meldings- of aangiftebereidheid.

Preventie

Begin 2019 heeft de politie een campagne uitgevoerd om jongeren bewust te maken van de strafbaarheid van cybercriminaliteit en de gevolgen daarvan, onder meer door inzet van sociale media, waaronder vlogs en gamefora. De campagne leidde tot discussies onder jongeren en kreeg veel aandacht en waardering. Eind mei is een grote publiekscampagne van het Ministerie van Justitie en Veiligheid (JenV) tegen *phishing* gestart, in nauwe samenwerking met het Ministerie van Economische Zaken en Klimaat (EZK), de politie en een groot aantal bedrijven en brancheorganisaties uit onder meer de internet-, ICT- en telecomsector en het bankwezen. In oktober van dit jaar geeft het Ministerie van EZK, in samenwerking met het Ministerie van JenV, een vervolg aan deze publiekscampagne, waarbij de focus op digitale veilige hard- en software zal liggen.

In 2018 is onder verantwoordelijkheid van het Ministerie van EZK het Digital Trust Center (DTC) opgericht. Dit heeft onder andere geresulteerd in de lancering van de website www.digitaltrustcenter.nl. Op de website wordt informatie en advies gegeven voor ondernemers uit het niet als vitaal aangemerkte deel van het bedrijfsleven, bijvoorbeeld over vijf basisprincipes voor veilig digitaal ondernemen.[7] In het derde kwartaal van 2019 wordt een interactief platform gestart waar het DTC, mede op basis

---

[1] ENISA Threat Landscape Report 2018, januari 2019, p. 34; https://nos.nl/artikel/2286613-justitie-en-branche-willen-af-van-foute-hostingbedrijven.html
[2] Internet Organised Crime Threat Assesment (iOCTA) 2018, Europol
[3] iOCTA 2018
[4] ENISA Threat Landscape Report 2018, januari 2019, p. 24
[5] iOCTA 2018
[6] CBS, 8 februari 2019, https://opendata.cbs.nl/statline/#/CBS/nl/dataset/83648NED/table?ts=1557411041196
[7] Het als vitaal aangemerkte deel van het bedrijfsleven krijgt informatie en advies van het Nationaal Cyber Security Centrum (NCSC).

van samenwerking met het Nationaal Cyber Security Centrum (NCSC) dreigingsinformatie en kennisproducten toegankelijk maakt en waar ondernemers kennis en informatie kunnen delen. In 2018 zijn met subsidies van het DTC zes nieuwe samenwerkingsverbanden gestart voor verhoging van de cyberweerbaarheid in het bedrijfsleven in Noord-Nederland, Limburg, de haven van Amsterdam, de maakindustrie in Oost-Nederland, bij groentezaadveredelingsbedrijven en in de Defensie gerelateerde industrie. De samenwerkingsverbanden leveren generieke tools op voor het versterken van de landelijke cyberweerbaarheid in het MKB. In mei 2019 is de inschrijfronde voor het subsidietraject van 2019 gesloten. De aanvragen worden momenteel beoordeeld, zodat er straks vijf of zes nieuwe samenwerkingsverbanden door het DTC ondersteund kunnen worden.
In samenwerking met gemeenten en regionale Platforms Veilig Ondernemen zijn projecten en pilots gestart, gericht op het versterken van de cyberveiligheid binnen gemeenten en het MKB door de bewustwording en weerbaarheid te vergroten. Gemeenten en regionale platforms hebben zodoende een aanvullende rol op de landelijke preventieactiviteiten.

Opsporing, vervolging, sanctionering, verstoring

De ambities uit de landelijke beleidsdoelstellingen voor 2018 zijn niet helemaal gehaald. Er zijn 299 reguliere en 43 complexe opsporingsonderzoeken gerealiseerd, waar de ambitie 310 respectievelijk 50 onderzoeken betrof. Wel was er in de afgelopen jaren steeds sprake van een stijgende lijn in het aantal opsporingsonderzoeken.[8] Ook laten voorlopige cijfers een verhoogd aantal ophelderingen en registraties van verdachten van computervredebreuk zien.[9] Het afgelopen jaar is naast de opsporingsonderzoeken aandacht uitgegaan naar alternatieve en aanvullende interventies. Ook was er veel capaciteit gemoeid met internationale spoedverzoeken ten behoeve van de opsporing in andere landen. Inmiddels zijn nadere afspraken gemaakt over de nieuwe landelijke beleidsdoelstellingen voor de periode 2019–2022 in de nieuwe Veiligheidsagenda. Voor de looptijd van de Veiligheidsagenda is de verwachting dat de ambitie verder kan groeien. De ambitie richt zich ten opzichte van de ambitie van de Veiligheidsagenda 2015–2018 meer op de aanpak van cybercriminele fenomenen en dadergroepen.

De investeringen in de politie en de strafrechtketen uit het Regeerakkoord hebben een versterking van de capaciteit mogelijk gemaakt. Zoals eerder gemeld aan de Kamer betreft het 46 fte bij de landelijke eenheid en 60 fte met specifieke digitale expertise ten behoeve van de regionale eenheden bij de politie.[10] Daarnaast zijn middelen vrijgemaakt uit het Regeerakkoord en uit de incidentele middelen bij Najaarsnota 2018 voor het versterken van de ICT-ondersteuning van de opsporing in het digitale domein.

Uitgelicht: wet Computercriminaliteit III in werking

Op 1 maart 2019 is de wet Computercriminaliteit III in werking getreden. De wet heeft enkele aanvullende strafbaarstellingen en bevoegdheden geïntroduceerd, waaronder de bevoegdheid tot het heimelijk en op afstand binnendringen in een geautomatiseerd werk. Inmiddels worden de eerste ervaringen opgedaan met de inzet van deze bevoegdheid, zoals onlangs bij het offline halen van één van de grootste *online mixers* voor

[8] Kamerstuk 35 200 VI, nr. 1, p. 25
[9] CBS, 8 februari 2019, https://opendata.cbs.nl/statline/#/CBS/nl/dataset/83648NED/table?ts=1557411041196
[10] Kamerstuk 29 628 nr. 784, 15 juni 2018 en Aanhangsel Handelingen II 2017/18, nr. 3220

cryptovaluta.[11] Dergelijke mixers worden veel gebruikt om criminele geldstromen te verhullen. Ook is het wederrechtelijk overnemen en «helen» van gegevens strafbaar gesteld en is de strafbaarheid van *grooming* en van verleiding van minderjarigen tot ontucht verruimd, zodat inzet van de zogenaamde «lokpuber» mogelijk is geworden. De wet biedt daarmee extra mogelijkheden voor de aanpak van cybercrime en gedigitaliseerde criminaliteit, zodat het internet geen vrijhaven wordt voor criminelen.

Uitgelicht: Integrale aanpak online seksueel (kinder)misbruik

Naast een stevige aanpak van cybercrime gaat aandacht uit naar andere specifieke fenomenen die via internet slachtoffers maken. Zo heeft uw Kamer op 21 mei jl. het wetsvoorstel herwaardering strafbaarstelling actuele delictsvormen,[12] met daarin de zelfstandige strafbaarstelling van misbruik van seksueel beeldmateriaal (waaronder wraakporno), aangenomen. Ook zet ik in op een preventieve aanpak van online seksueel kindermisbruik. Zo wordt een expertmeeting voor professionals van scholen, (jeugd)zorg en de strafrechtketen gehouden om de aanpak van de negatieve effecten van sexting te verbeteren. Daarnaast wordt de aanpak van downloaders van kinderporno geïntensiveerd en is de publiek-private samenwerking versterkt om kinderpornografische content sneller van internet te laten verwijderen. Verder zet ik in op een bestuursrechtelijke aanpak, om bedrijven die kinderporno niet accuraat verwijderen met een bestuursrechtelijk handhavingsinstrumentarium hiertoe te dwingen. In de nieuwe Veiligheidsagenda zijn er voor de aanpak van kinderporno nieuwe afspraken gemaakt, als onderdeel van de cyberparagraaf. U ontvangt nog voor het zomerreces een voortgangsbrief over de aanpak van online seksueel kindermisbruik, waarin ik nader inga op bovengenoemde acties.

Aandacht voor slachtoffers

Het recente onderzoek van het WODC naar slachtoffers van online criminaliteit gaf een eerste inzicht in de behoeften van slachtoffers en welke gevolgen zij ervaren. Uit het onderzoek blijkt niet dat de gevolgen en behoeften van slachtoffers bij online delicten veel afwijken van traditionele delicten, maar door de kenmerken van het online delict kan de impact voor slachtoffers wel groter zijn. Dit komt met name door de enorme schaal waarop de gevolgen zich online kunnen doen gelden. Momenteel wordt een aantal maatregelen genomen, zoals verbetering van de informatievoorziening aan slachtoffers en het aanpassen van de dienstverlening, en er wordt vervolgonderzoek gedaan. Ik verwijs u hiervoor naar de beleidsreactie van de Minister voor Rechtsbescherming van 7 februari jl.[13]

Wetenschappelijk onderzoek

Ondanks de diverse publicaties over cybercrime is er nog veel ruimte voor kennisontwikkeling. Van enkele onderzoeken worden dit jaar resultaten verwacht. Uit afgeronde onderzoeken blijkt onder meer dat bij het schatten van de aard en omvang van cybercrime gebruikelijke bronnen en methoden onvoldoende zekerheid bieden. Daarom worden innovatieve methoden verkend, zoals gebruik van big data-analyses en textmining van onder meer politieregistraties.

---

[11] https://www.fiod.nl/blog/2019/05/22/fiod-en-om-halen-witwasmachine-voor-cryptovaluta-offline/

[12] Kamerstuk 35 080

[13] Kamerstuk 28 684, nr. 550

Tot slot

Cybercrime blijft zich ontwikkelen. Nieuwe inzichten, bijvoorbeeld uit wetenschappelijk onderzoek, en ontwikkelingen in criminele werkwijzen kunnen aanleiding zijn tot nieuwe maatregelen en samenwerkingsverbanden. Flexibiliteit en samenwerking blijven uitgangspunten bij de aanpak van de diverse en veranderende verschijningsvormen van cybercrime. Ik blijf mij inzetten om cybercrime tegen te gaan.

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

BIJLAGE

OVERZICHT MAATREGELEN

Preventie

Flexibele, snel inzetbare preventiecampagnes

In 2018 is gestart met een beperkte campagne voor het algemeen publiek met gebruik van radio en social media. Het doel was om tips aan te reiken voor een veiliger online gedrag van gebruikers. De campagne wordt in 2019 voortgezet en uitgebreid naar TV. Bij de voorbereiding van deze campagne wordt samengewerkt met private partijen en technisch experts van buiten de overheid. Voor de campagnes in 2019 werken de Ministeries van JenV en EZK nauw samen. Daarbij wordt de doelgroep ook verbreed naar het bedrijfsleven. In de campagnes wordt verwezen naar de websites www.veiliginternetten.nl en www.digitaltrustcenter.nl, waar ook over andere criminele werkwijzen informatie te vinden is. De financiële middelen van beide ministeries worden in onderling overleg ingezet.

Daarnaast heeft begin 2019 vanuit de politie een campagne plaatsgevonden, ondersteund door JenV, om jongeren bewust te maken van de strafbaarheid van cybercriminaliteit en de gevolgen daarvan, onder meer door inzet van sociale media, waaronder vlogs en gamefora. Preventie richt zich dus niet alleen op slachtoffers maar ook op potentiele daders. De eerste fase is uitgevoerd in februari 2019, en de tweede fase is voorzien in het najaar van 2019.

Ondersteuning veiligheid MKB-ondernemingen: Digital Trust Center

Het doel van het DTC is om het niet als vitaal aangemerkte deel van ondernemend Nederland in staat te stellen zich weerbaarder te maken tegen cyberaanvallen.[14] Hiermee wordt invulling gegeven aan de motie-Hijink[15]. Op 8 juni 2018 is de website digitaltrustcenter.nl gestart, waarop de vijf basisprincipes voor veilig digitaal ondernemen centraal staan. In het derde kwartaal van 2019 wordt een interactief platform gestart waar het DTC mede op basis van samenwerking met het NCSC dreigingsinformatie en kennisproducten toegankelijk maakt en waar ondernemers kennis en informatie kunnen delen. In 2018 zijn zes nieuwe samenwerkingsverbanden gestart met subsidie van het DTC. Deze samenwerkingsverbanden zullen samen met het DTC de cyberweerbaarheid verhogen van het bedrijfsleven in Noord-Nederland, Limburg, de haven van Amsterdam, de maakindustrie in Oost-Nederland, bij groentezaadveredelingsbedrijven en in de Defensie gerelateerde industrie. Op 19 september 2018 heeft de Staatssecretaris van Economische Zaken en Klimaat de kamer schriftelijk geïnformeerd over de resultaten van de subsidieregeling van 2018. Gezien de succesvolle resultaten in 2018, is besloten de subsidieregeling opnieuw open te stellen en de looptijd te verlengen met twee jaar tot 1 april 2021. Ook voor de nieuwe uitvraag is wederom € 1 miljoen ter beschikking gesteld. Hiermee wordt een groeiend netwerk voor digitaal veilig ondernemen gefaciliteerd. Tevens kunnen ondernemers voor informatie en advies terecht op de website van het DTC (www.digitaltrustcenter.nl).

Ondersteuning gemeenten en MKB-ondernemingen

In 2018 is de samenwerking met de G4, G40, VNG en het CCV tot stand gekomen, die zich richt op cyberveiligheid van de gemeentelijke organisatie, lokale cybercrises en de aanpak van cybercrime en cyber in de

[14] Voor de vitale sectoren vervult het NCSC deze functie.
[15] Kamerstuk 26 643, nr. 473

openbare orde. De komende periode wordt gewerkt aan de verbreding van de initiatieven naar de andere gemeenten. Begin 2020 worden de resultaten van de gemeentelijke projecten gepresenteerd tijdens een conferentie van het CCV. Het Ministerie van JenV ondersteunt projecten en pilot-initiatieven van gemeenten en Platforms Veilig Ondernemen die naar verwachting ook in andere regio's en gemeenten, toegesneden op de lokale situatie, toepasbaar zijn.

Digitale veiligheid in het MKB kan alleen in samenwerking met, en voor een belangrijk deel ook door, het bedrijfsleven worden vormgegeven. Het komende jaar worden een aantal onderzoeken en acties uitgewerkt en uitgevoerd om de cyberveiligheid van het MKB verder te vergroten. Deze maatregelen zullen worden beschreven in het actieprogramma «Veilig Ondernemen» 2019–2022.

Digitaal veilige hard- en software

Het Ministerie van EZK heeft samen met het Ministerie van JenV en private partijen de Roadmap Digitaal Veilige Hard- en Software opgesteld en deze in 2018 aan de Kamer gestuurd. Het betreft een mix van maatregelen om de digitale veiligheid te bevorderen. Momenteel wordt er in EU-verband gekeken naar de mogelijkheden die de *Radio Equipment Directive* biedt op het gebied van minimum digitale veiligheidseisen aan *Internet of Things*-apparaten. De Europese Commissie zal in 2019 een impact assessment uitvoeren. De Nederlandse inzet is dat de Europese Commissie overgaat tot het stellen van eisen, zodat op termijn voor alle met internet verbonden apparaten minimale digitale veiligheidseisen gelden. Daarnaast heeft de EU de Cyber Security Act aangenomen die een stelsel creëert voor cybersecurity certificering van ICT-producten, -diensten en -processen. Nederland zet in op de voortvarende ontwikkeling van cybersecurity certificeringschema's. U zal door de Staatssecretaris van Economische Zaken en Klimaat worden geïnformeerd over de voortgang van de roadmap.

Opsporing, vervolging, sanctionering en verstoring

Versterking aanpak van de politie en in de strafrechtketen

Tijdens de vorige regeerperiode is de politie gestart met de opbouw van cybercrimeteams in de regionale eenheden van de politie. Het Regeerakkoord heeft een forse investering in de politie mogelijk gemaakt. Deze komt deels ten goede aan de opsporing van cybercrime en gedigitaliseerde criminaliteit. In de Veiligheidsagenda zijn voor 2019 inmiddels afspraken gemaakt over het aantal onderzoeken en het type onderzoeken dat prioriteit krijgt. Naar aanleiding van het verloop in 2019 worden nadere afspraken voor 2020 en verder gemaakt.

Bewustwording hostingproviders

De private sector is in overleg met het Ministerie van EZK gestart met het project Abuse 2.0. Dit project is gericht op het verbinden van marktpartijen om diverse vormen van cybercrime sneller te onderkennen en met elkaar te delen, zodat private partijen zelf maatregelen kunnen nemen. De aangesloten bedrijven lopen zo minder kans cybercrime te faciliteren. In 2018 is tijdens de ONE-conference www.abuseplatform.nl gestart. In 2019 wordt gestreefd naar aansluiting van zo veel mogelijk nieuwe partijen op het platform.

Verstoring crimineel verdienmodel

Om criminaliteit niet te laten lonen, ook in die gevallen waarin er geen reëel zicht is op een veroordeling, wordt er ook stevig ingezet op het verstoren van criminele verdienmodellen. Daarvoor worden opkomende criminele werkwijzen geanalyseerd, vaak in publiek-privaat verband, en wordt bezien welke slimme interventies kunnen worden ingezet om het criminelen zo lastig mogelijk te maken. De politie en het Openbaar Ministerie pasten in 2018 de Greenfields-werkwijze toe op criminele werkwijzen en passen de aanpak daarop aan. Een voorbeeld van een nieuwe projectmatige aanpak is de zogenaamde *tech support scam*, die op initiatief van het Landelijk Parket en het arrondissementsparket Rotterdam, in samenwerking met de politie en de private sector wordt aangepakt. Inmiddels zijn door de private sector enkele technische maatregelen doorgevoerd en zijn arrestaties in India gedaan. Het aantal meldingen en aangiften van deze vorm van criminaliteit is gedaald. Andere voorbeelden zijn het project NoMoreRansom.org om *ransomware* tegen te gaan en NoMoreDDoS voor het tegengaan van DDoS-aanvallen.

Versterking nationale wetgeving

Op 1 maart 2019 is de wet Computercriminaliteit III (Kamerstuk 34 372) in werking getreden. De wet heeft enkele aanvullende strafbaarstellingen en bevoegdheden geïntroduceerd, waaronder de bevoegdheid tot binnendringen in geautomatiseerd werk. De politie en het Openbaar Ministerie beschikken hiervoor over gespecialiseerde medewerkers. De extra mogelijkheden die de wet biedt, versterken ook de aanpak van cybercrime, zodat het internet geen vrijhaven wordt voor criminelen.

Internationale samenwerking

De politie en het Openbaar Ministerie werken aan het versterken van de rechtshulpprocessen voor digitaal bewijs. Het 24/7 contactpunt is inmiddels apart georganiseerd, zodat de werkzaamheden van het contactpunt minder interfereren met de landelijke opsporingsonderzoeken. De Europese Commissie werkt daarnaast aan het digitaliseren van rechtshulpprocedures en het vergemakkelijken van het grensoverschrijdend vergaren van elektronisch bewijs. In het Europees netwerk van cyberofficieren worden *best practices* en kennis over de specifieke bevoegdheden uitgewisseld om de samenwerking bij het vergaren van elektronisch bewijs effectief en zorgvuldig te kunnen vormgeven.

Versterking internationale juridische kaders

In 2018 heeft Nederland actief bijgedragen 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 tegen het voorstel te stemmen gezien de onvoldoende rechtsstatelijke waarborgen. De JBZ-raad heeft het voorstel wel aangenomen. Nederland richt zich nu op de discussies in het Europees parlement en de triloog. Inmiddels is ook een akkoord bereikt over de bijbehorende richtlijn over het aanwijzen door private dienstverleners van een juridisch vertegenwoordiger in de EU. In het kader van de Raad van Europa blijft Nederland actief deelnemen aan de gesprekken over een tweede protocol bij het Cybercrimeverdrag.

Aanpak jonge (potentiële) daders en beperking recidive

Samen met onder meer de politie, het Openbaar Ministerie, Halt en de Raad voor de Kinderbescherming worden het risicotaxatie- en diagnose-instrumentarium (LIJ) en het interventiepalet aangevuld voor jeugdige cyberdaders. Daarnaast wordt in het kader voor strafvervolging jeugd en adolescenten de bestaande richtlijn aangevuld met richtlijnen en strafmaten voor jeugdige cyberdelinquenten. In de pilot Hack_Right beproeven het Openbaar Ministerie 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.

De reclassering is eind 2018 gestart met een project in het kader van de aanpak van cybercrime. Het project richt zich onder meer op het ontwikkelen van nieuwe of aanvullende werkwijzen en interventies voor daders die zich schuldig hebben gemaakt aan cybercrime, daarbij wordt aangesloten bij wetenschappelijk onderzoek.

Verbetering aangifteproces

De aangiftebereidheid van cybercrime is lager dan bij traditionele criminaliteit. De politie is voornemens voor bepaalde vormen van cybercrime digitale aangifte mogelijk te maken, zodat de drempel voor slachtoffers om aangifte te doen omlaag gaat. De aandacht gaat als eerste uit naar ransomware en helpdeskfraude.

Aandacht voor slachtoffers

In 2018 heeft het WODC onderzoek gedaan naar behoeften, gevolgen en verantwoordelijkheden na slachtofferschap van cybercrime en gedigitaliseerde criminaliteit. Het rapport is in februari 2019 aan de Kamer aangeboden. Momenteel worden een aantal maatregelen genomen en vervolgonderzoek gedaan. De Minister voor Rechtsbescherming heeft de Kamer hierover op 7 februari 2019 geïnformeerd.[16]

Slachtoffernotificatie en schadebeperking

Het informeren van slachtoffers (slachtoffernotificatie) is zowel voor slachtoffers zelf van belang als ter voorkoming van nieuwe slachtoffers. Door het snel informeren van slachtoffers kan de schade worden beperkt. Het delen van operationele gegevens is juridisch niet altijd mogelijk. Momenteel worden de mogelijkheden en barrières voor het delen van informatie met slachtoffers onderzocht.

Wetenschappelijk onderzoek

- Het hierboven genoemde onderzoek naar slachtofferzorg is inmiddels gepubliceerd.
- Het onderzoek naar aard en omvang van cyber- en gedigitaliseerde criminaliteit bestaat uit twee delen, waarvan het eerste deel naar verwachting in 2019 gereed is en het tweede deel in 2020.
- Het secundaire onderzoek naar slachtofferschap van cyber- en gedigitaliseerde criminaliteit is naar verwachting gereed in 2019.
- De onderzoeken naar het verstoren van cyber- en gedigitaliseerde criminaliteit en het onderzoek naar de strafrechtelijke aanpak van cyber- en gedigitaliseerde criminaliteit zijn samengevoegd. Het onderzoek is inmiddels gestart en is naar verwachting in 2021 gereed.

[16] Kamerstuk 28 684, nr. 550

– In 2018 is onderzoek gestart naar cyberbewustzijn en risicoperceptie. Dit onderzoek is naar verwachting eind 2019 gereed.
– Een onderzoek naar daderprofielen en interventies is gestart in 2018 en is naar verwachting eind 2019 gereed.
– Twee onderzoeken ten aanzien van de rol van gemeenten en burgemeesters zijn naar verwachting eind 2019 gereed.