Ministerie van Justitie en Veiligheid

> Retouradres Postbus 20301 2500 EH Den Haag

Aan de Voorzitter van de Tweede Kamer
der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/jenv

Ons kenmerk
3388241

Bij beantwoording de datum en ons kenmerk vermelden. Wilt u slechts één zaak in uw brief behandelen.

Datum 28 juni 2021
Onderwerp Integrale aanpak cybercrime

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. Ik heb u hier eerder over geïnformeerd op 29 juni 2020.[1] De aanpak van cybercrime en de versterking van cybersecurity hangen met elkaar samen. Over de voortgang van de Nederlandse Cybersecurity Agenda (NCSA) wordt u heden apart geïnformeerd.

Het leven van burgers speelt zich inmiddels voor een groot deel online af, en dit deel is tijdens de coronacrisis verder gegroeid. We zijn in ons dagelijks leven steeds afhankelijker van de online wereld. Dit vergroot de mogelijkheden voor criminelen om slachtoffers te maken en de impact die online criminaliteit kan hebben. De afgelopen jaren is inzet gepleegd op vier sporen, te weten preventie, ondersteuning van slachtoffers, wetenschappelijk onderzoek en opsporing, vervolging en verstoring. In deze brief worden de ontwikkeling van cybercrime en enkele in het oog springende maatregelen uiteengezet. Een overzicht van maatregelen is opgenomen in de bijlage. Ondanks de inspanningen blijft het tegengaan van cybercrime een forse uitdaging die een blijvende inspanning vraagt.

Algemeen beeld – ontwikkeling cybercrime
Cybercrime[2] neemt in de politieregistraties al meerdere jaren gestaag toe. Tijdens de coronacrisis heeft deze toename zich voortgezet. Criminelen hebben ingespeeld op de situatie en de online criminele activiteiten zijn toegenomen. Zo steeg het aantal registraties van computervredebreuk van rond de 2.000 in de jaren 2014-2016 naar 4.865 in 2019 en 11.120 in 2020.[3] De werkelijke dreiging en omvang van cybercrime wijkt waarschijnlijk af van de politieregistraties, omdat de aangiftebereidheid nog steeds zeer laag is. In het kader van de Veiligheidsmonitor gaf in 2019 5,5% van de respondenten aan slachtoffer te zijn geworden van hacken.[4] Als meerdere vormen van online criminaliteit worden bezien, en naast cybercrime andere online delicten zoals aan- en verkoopfraude

[1] Kamerstukken 2019/20, 26 643, nr. 696
[2] De term cybercrime betreft in deze brief criminaliteit waarbij ICT-systemen zowel doel als middel zijn (ook wel cybercrime in enge zin genoemd). Voorbeelden daarvan zijn ransomware en het 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. Overigens zijn er diverse criminele werkwijzen die elementen van cybercrime in enge zin en gedigitaliseerde criminaliteit combineren.
[3] data.politie.nl
[4] opendata.cbs.nl

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Datum
28 juni 2021

Ons kenmerk
3388241

worden meegenomen, dan geeft 13% van de respondenten aan slachtoffer te zijn geworden.[5] Het verzamelen van aanvullende gegevens over slachtofferschap en schade is nodig om een meer compleet beeld te krijgen. Daarom wordt momenteel gewerkt aan een uitbreiding van de Veiligheidsmonitor en een aparte monitor voor vormen van online criminaliteit.

Cybercriminelen worden steeds geraffineerder in het gebruik van sociale en technische kwetsbaarheden. *Social engineering* en de inzet van *malware* zoals ransomware vormen onverminderd een aanzienlijke dreiging. Gezien de nog vaak onvoldoende beveiligingsmaatregelen en onoplettendheid bij eindgebruikers hoeft een aanval echter niet altijd geraffineerd te zijn om succes te hebben.[6] Het voortbestaan van *cybercrime-as-a-service* blijft er voor zorgen dat ook minder vaardige criminelen cyberaanvallen kunnen uitvoeren. Eén van de conclusies in het Cyber Security Beeld Nederland (CSBN) 2021 is dat cybercriminaliteit de nationale veiligheid kan raken indien dit leidt tot omvangrijke schade aan digitale processen. In een aantal gevallen genieten cybercriminelen bescherming van de staat van waaruit zij opereren of is er sprake van samenwerking.[7]

Gerichte ransomware-aanvallen op grote bedrijven en instellingen vormen een toenemende dreiging voor de economische en maatschappelijk veiligheid.[8] Ondanks het gebrek aan kwantitatieve gegevens is het beeld van de politie dat zowel het MKB als grote organisaties in toenemende mate doelwit zijn van ransomware. Recente cybercriminele incidenten zoals bij de Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO) en de gemeente 't Hof van Twente tonen de grote impact die deze criminaliteitsvorm ook in Nederland kan hebben.[9] De politie heeft gesignaleerd dat een deel van het ontvangen losgeld direct wordt geïnvesteerd in nieuwe aanvallen. Ransomware wordt bovendien steeds vaker gecombineerd met het publiceren of doorverkopen van tijdens de aanval weggesluisde informatie. Door het gebruik van cryptovaluta zorgen criminelen dat hun identiteit bij het ontvangen van losgeld afgeschermd blijft in het geval van cybercriminele afpersing zoals ransomware.[10] Ook DDoS-aanvallen worden gecombineerd met pogingen tot afpersing. In de Jaarverantwoording Politie en in het CSBN wordt uitgebreid op de dreiging van onder meer ransomware ingegaan.

Advies betalen losgeld
Het advies vanuit het Kabinet, het OM en de politie blijft om geen losgeld te betalen bij een ransomware-aanval. Het betalen van losgeld biedt geen garantie op ontsleuteling van gegevens en houdt het criminele verdienmodel in stand. Om ransomware te voorkomen is het onder meer belangrijk om de digitale weerbaarheid op orde te hebben. Het instellen van twee-factorauthenticatie kan hierbij al aanzienlijk helpen.

Preventie

Het verhogen van de cyberweerbaarheid van burgers, bedrijven en instellingen blijft een punt van aandacht. Mensen gedragen zich online minder veilig dan ze denken en schatten de kans dat ze schade ondervinden van online risico's laag in.

[5] Veiligheidsmonitor 2019. Het genoemde percentage betreft vier onderzochte delicten, te weten hacken, identiteitsfraude, aan- en verkoopfraude en cyberpesten.
[6] Jaarverantwoording politie 2020; Europol Internet Organised Crime Threat Assessment (IOCTA) 2020
[7] Cyber Security Beeld Nederland (CSBN) 2021.
[8] IOCTA 2020, ENISA Threat Landscape 2020
[9] Kamerstukken II, 2020/21, 31 288 nr. 910
[10] IOCTA 2020

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Datum
28 juni 2021

Ons kenmerk
3388241

Bij veel succesvolle cyberaanvallen zijn onvoldoende basismaatregelen voor digitale weerbaarheid getroffen. De afgelopen jaren zijn diverse activiteiten uitgevoerd om de bewustwording van risico's en de bekendheid met basismaatregelen te ondersteunen. Deze activiteiten zijn gericht op het algemene publiek en op de specifieke doelgroepen jongeren, senioren, laaggeletterden en het MKB. Voor het algemene publiek zijn twee landelijke campagnes uitgevoerd, te weten 'Eerst checken, dan klikken' door het Ministerie van JenV in 2019 en 'Doe je updates' door het Ministerie van EZK van november 2019 tot januari 2021.[11] In het kader van het convenant voor de preventie van cybercrime wordt met private partners samengewerkt aan onder meer het aanpakken van *social engineering* en *spoofing,* evenals aan de verbreding van het gebruik van twee-factorauthenticatie. Op de website www.veiliginternetten.nl kunnen burgers terecht voor voorlichting en vragen over veilig online gedrag. Ten behoeve van de verspreiding van informatie over actuele cybercrimefenomenen en preventieve tips is, mede naar aanleiding van de suggestie van het Kamerlid Van Dam (CDA) tijdens het Algemeen Overleg cybersecurity op 9 december 2020, in samenwerking met de politie en de Fraudehelpdesk een pilot gestart met een periodiek 'cyberweerbericht'. In dat bericht worden actuele dreigingen en preventieve maatregelen periodiek gepubliceerd, onder meer op www.veiliginternetten.nl.

Voor het voorkómen en tegengaan van daderschap van cybercrime onder jongeren ontwikkelde de politie in navolging van eerdere campagnes het lesprogramma "Framed". Jongeren krijgen via het spelen van een online spel inzicht in verschillende cybercrimedelicten en de gevolgen daarvan. De campagne heeft inmiddels de Digital Interactive Award ontvangen in de categorie Activation. Stichting Halt heeft begin 2021 een nieuwe lesmodule over (online) fraude en cybercrime voor jongeren gelanceerd, gericht op het voorkómen van slachtoffer- en daderschap. Deze activiteiten maken deel uit van de brede aanpak van jeugdcriminaliteit. Op 23 juni jl. heeft de Minister voor Rechtsbescherming u nader over de voortgang van deze aanpak geïnformeerd.[12]

Cyber Offender Prevention Squad (COPS)
In 2020 is bij de politie een tijdelijk projectteam gestart dat zich richt op daderpreventie. Het projectteam COPS beoogt het afschrikken van (potentiële) daders, het stimuleren van positieve keuzes en het verzwakken en verstoren van daders die bewust kiezen voor cybercrime. In 2020 zijn een daderpreventiestrategie en een interventietoolkit ontwikkeld en getest. Ook is een samenwerking met de *gaming*-industrie gestart.

In april 2020 is de campagnemaand 'Senioren en Veiligheid' georganiseerd om senioren meer weerbaar te maken. Hiervoor is onder meer voorlichtingsmateriaal over online fraude en cybercrime verspreid en zijn vrijwilligers van ouderenbonden voorgelicht om hierover de juiste informatie te geven aan senioren. Voor laaggeletterden heeft het Ministerie van BZK in samenwerking met JenV het programma 'Klik en Tik: Veilig Online' gelanceerd op www.oefenen.nl.

De door de ministeries van JenV en BZK samen het Digital Trust Center (DTC) geïnitieerde City Deal Lokale Weerbaarheid Cybercrime is in oktober 2020 ondertekend. Deze City Deal omvat momenteel 18 projecten van gemeenten, regionale samenwerkingsverbanden Veiligheid en Platforms Veilig Ondernemen,

[11] Kamerstukken 2019/20, 26 643, nr. 696
[12] 2021Z11586

gericht op het versterken van de weerbaarheid van jongeren, laaggeletterden, senioren en het MKB. Een voorbeeld is het project van de gemeente Breda, waar een groot aantal digitale wijkambassadeurs zijn opgeleid. Het netwerk van ambassadeurs helpt bij de uitvoering van de preventieve aanpak op het gebied van digitale criminaliteit. De opleidingsmodule die voor de digitale ambassadeurs is ontwikkeld kan ook in andere gemeenten worden ingezet.

In het Actieprogramma Veilig Ondernemen 2019–2022 heeft het Nationaal Platform Criminaliteitsbeheersing cybersecurity in het MKB als prioriteit opgenomen. De pilots in de City Deal Lokale Weerbaarheid Cybercrime gericht op het MKB passen binnen de doelstelling van het Actieprogramma. In het kader van het Actieprogramma is een onderzoek naar cyber-ketenafhankelijkheden in waardeketens van bedrijven gepubliceerd. Vervolgonderzoek richt zich op concreet handelingsperspectief voor het MKB binnen de ketens. Daarnaast is een gedragsexperiment gestart om inzicht te krijgen in gedragsbeïnvloeding en gedragsinterventies.

Het DTC heeft de afgelopen twee jaar meerdere projecten gestart en producten ontwikkeld gericht op bedrijven. Zo kunnen ondernemers de weerbaarheid van hun onderneming testen met de Basisscan Cyberweerbaarheid, is er een *Digital Trust Community* waarin aangesloten bedrijven actuele en relevante informatie kunnen uitwisselen en is de Wegwijzer voor cybersecurity-initiatieven ontwikkeld. Deze wegwijzer helpt ondernemers snel hun weg te vinden in de vele cybersecurity-initiatieven die Nederland rijk is.

Opsporing, vervolging en verstoring

Het internet mag geen vrijplaats voor criminelen zijn. Adequate opsporing en vervolging zijn hiervoor noodzakelijk. Eerder heb ik uw Kamer geïnformeerd over de uitdagingen bij de rechtshandhaving in het digitale domein.[13] De schaalbaarheid van cybercrime creëert een grote hoeveelheid (potentiële) slachtoffers. Daarnaast is het internet inherent grenzeloos en biedt het veel technische mogelijkheden voor anonimisering. Om deze uitdagingen het hoofd te kunnen bieden is de afgelopen jaren geïnvesteerd in de versterking van de opsporing in het digitale domein in het algemeen en de bestrijding van cybercrime in het bijzonder. Een deel van de middelen uit het Regeerakkoord en een deel van de eenmalige investering bij de Najaarsnota in 2018 zijn hieraan besteed, met name bij de politie, het OM en het NFI.

De politie werkt inmiddels met een landelijk dekkende aanpak, bestaande uit onder meer het *Team High Tech Crime* (THTC) en tien cybercrimeteams in de regionale eenheden. De onderzoeken zijn conform de Veiligheidsagenda verdeeld in reguliere onderzoeken uitgevoerd op regionaal niveau, fenomeenonderzoeken, die gericht zijn op de brede bestrijding van eenheidoverstijgende cybercriminele fenomenen en dadergroepen, en onderzoeken van het THTC, waar het gaat om onderzoeken met een *high tech*-component. De regionale cybercrimeteams zijn daarbij steeds complexere zaken gaan uitvoeren. Ze assisteren bovendien reguliere opsporingsteams bij de bestrijding van gedigitaliseerde criminaliteit die zowel door cybercriminelen als door niet-cybercriminelen wordt gepleegd, zoals helpdeskfraude, vriend-in-noodfraude en betaalverzoekfraude. De capaciteit bij het OM blijft nog achter bij die van de politie.

[13] Kamerstukken 2019/20, 28 684, nr. 621.

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Datum
28 juni 2021

Ons kenmerk
3388241

De resultaten in het kader van de Veiligheidsagenda tonen de afgelopen jaren een stijgende lijn. Het aantal uitgevoerde reguliere onderzoeken bij politie vertoont een forse stijging, van 299 in 2018 naar 468 onderzoeken in 2020. Ook het aantal fenomeenonderzoeken stijgt. Ondanks dat de ambitie van 41 in 2020 met 39 net niet is behaald, is dit wel een stevige toename ten opzichte van de 21 fenomeenonderzoeken in 2019. Eén fenomeenonderzoek omvat vaak vele, soms duizenden slachtoffers, en soms betreft het vele miljoenen aan financiële schade. De ambitie van 20 *high tech crime*-onderzoeken is met 12 opsporingsonderzoeken niet behaald en gedaald ten opzichte van voorgaande jaren. De oorzaak daarvan ligt vooral in de toenemende technische en juridische complexiteit van de fenomenen en de onderzoeken, wat een grotere inzet van capaciteit en hoogwaardige kennis vergt. Deze onderzoeken betreffen de meest hoogtechnologische of nieuwe criminele werkwijzen en opsporingsmethoden. Ze nemen vaak meerdere jaren in beslag en bestrijken veelal verschillende subdoelstellingen. Ook wordt er binnen de onderzoeken aan technische en juridische innovaties gewerkt, die vervolgens aan de hele opsporing ten goede komen.

De politie zet in op datagedreven bestrijding van cybercrime, waarbij sprake is van intensieve samenwerking: nationaal en internationaal, publiek en privaat. Vaak is er sprake van brede samenwerkingsverbanden waarbij het THTC en het Landelijk Parket van het OM samenwerken in (internationale) coalities van overheidsdiensten en private bedrijven. Het THTC was tot april 2021 voorzitter van de *Joint Cybercrime Action Taskforce* van Europol en de politie neemt deel aan het *EMPACT-platform.*[14] De Landelijk Officier van Justitie voor Cybercrime bij het Landelijk Parket is lid van het *European Judicial Cybercrime Network* (EJCN). Ook investeren de politie en het OM in samenwerking met private partijen. De projecten NoMoreDDoS, NoMoreRansom, NoMorePhishing en het afgeronde project ter bestrijding van de *Tech Support Scam* zijn voorbeelden hiervan. Het *NoMoreRansom*-portal had in juni 2020 sinds de lancering vier jaar eerder ervoor gezorgd dat zo'n $ 632 miljoen aan geëist losgeld niet in de zakken van criminelen terecht is gekomen. Voor de bestrijding van ransomware heeft de politie een speciale taskforce opgericht met als doel in internationaal verband en met publieke en private partijen ransomware te bestrijden. Daarnaast nemen de politie en het Ministerie van EZK deel aan het in 2020 opgerichte Anti-Abuse Netwerk (AAN), een publiek-privaat samenwerkingsverband voor het tegengaan van het onwetend faciliteren van criminaliteit door hostingproviders. Een voorbeeld van een regionaal samenwerkingsverband is de Taskforce Digitale Veiligheid van de regio Amsterdam, waar het OM aan deelneemt, dat zich richt op het verhogen van de weerbaarheid tegen digitale indringers en criminelen. In 2020 zijn tien politiemensen geworven voor versterking van de publiek-private samenwerking van de regionale cybercrimeteams.

Internationale politieoperatie Ladybird
Begin 2021 haalde de omvangrijke internationale politieoperatie Ladybird het complexe netwerk van servers achter de agressieve *malware* Emotet uit de lucht. Emotet besmette de systemen van ruim 1 miljoen slachtoffers wereldwijd met *malware*, 600.000 mailadressen waren gecompromitteerd en de wereldwijde schade loopt waarschijnlijk in de honderden miljoenen euro's. De criminele werkwijze was sterk georganiseerd, adaptief en technisch zeer complex. De aanpak vergde een omvangrijke samenwerking van vele politiemensen en

[14] *European Multidisciplinary Platform Against Criminal Threats*. Hierbinnen prioriteren politiediensten van EU-lidstaten en Europol cybercrimebestrijding op Europees niveau.

officieren van justitie in acht landen. Twee van de drie hoofdservers bleken in Nederland te staan. Uiteindelijk lukte het om toegang te verkrijgen tot de cybercriminele infrastructuur van Emotet en deze te doorzoeken. Daarbij hebben de politie en het OM mede gebruik gemaakt van de bevoegdheid tot binnendringen in een geautomatiseerd werk. Uiteindelijk is het netwerk overgenomen en is de Emotet-*malware* gedeactiveerd. In samenwerking met het NCSC zijn zoveel mogelijk slachtoffers genotificeerd.

Voor een effectieve opsporing in het digitale domein is zowel nationaal als internationaal regelgeving nodig die is toegesneden op het digitale domein. De Wet computercriminaliteit III is nu ruim twee jaar van kracht. De politie en het OM hebben voortvarend invulling gegeven aan de bevoegdheid tot het heimelijk en op afstand binnendringen in een geautomatiseerd werk. Recent is de bevoegdheid ook in internationaal onderzoek ingezet. De Inspectie Justitie en Veiligheid houdt toezicht op de inzet van de bevoegdheid. Het jaarlijkse toezichtsrapport en de reactie daarop worden voor het zomerreces aan de Kamer gestuurd. Het WODC is inmiddels gestart met de evaluatie. Deze wordt naar verwachting begin 2022 gepubliceerd.

Om de grensoverschrijdende opsporing in het digitale domein te versterken heeft Nederland in de afgelopen jaren actief deelgenomen aan de gesprekken over de E-Evidenceverordening van de EU en over het tweede protocol bij het Cybercrimeverdrag in het kader van de Raad van Europa. De triloog over de E-evidence-verordening is inmiddels gestart. Het concept van het tweede protocol is eind mei goedgekeurd en openbaar gemaakt. Daarmee is een belangrijke mijlpaal bereikt in de gesprekken die in 2017 formeel zijn gestart. Na goedkeuring op politiek niveau en ratificatie zal het protocol snellere en meer efficiënte samenwerking in opsporingsonderzoeken mogelijk maken.

Ondanks de inspanningen en successen in de afgelopen jaren maken de toenemende hoeveelheid cybercrimedelicten en de complexiteit van de opsporing in het digitale domein het lastig voldoende capaciteit en expertise te realiseren. De politie en het OM signaleren bovendien dat zware criminaliteit in het fysieke domein, zoals drugshandel, in toenemende mate wordt ondersteund door gespecialiseerde, criminele digitale dienstverlening. De bestrijding van deze criminaliteitsvormen vraagt steeds vaker een aanpak in het digitale domein, waarbij een beroep wordt gedaan op de gespecialiseerde cybercrimecapaciteit van de politie en het OM. Daarmee worden belangrijke successen geboekt, zoals bij de aanpak van Encrochat en bij de operatie *Trojan Shield*, waarbij het berichtenverkeer van vele criminelen kon worden ingezien. Om een sterkere handhavingsketen te realiseren adviseert de Cyber Security Raad €330 miljoen extra te investeren in het vergroten van inzicht en de aanpak van cybercrime door het OM, de KMar en de politie.[15]

Aandacht voor het slachtoffer
De impact van online criminaliteit op slachtoffers kan groot zijn. Het is van belang slachtofferschap te erkennen en hen hierin te ondersteunen. Slachtofferhulp Nederland heeft in 2020 een grote groep mensen bereikt met de campagne "Van oplichting naar opluchting". Hierin deelden slachtoffers van online criminaliteit hun verhaal. Mede door deze campagne zijn meer mensen lid geworden van online lotgenotengroepen, waarbij slachtoffers over de gevolgen kunnen praten.

[15] Cyber Securty Raad, *Integrale aanpak cyberweerbaarheid*, 6 april 2021

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Datum
28 juni 2021

Ons kenmerk
3388241

Het zorgen voor een adequate behandeling van slachtoffers en tegelijk het effectief houden van de vervolging en het strafproces vormt een forse uitdaging. Vanwege de grote schaalbaarheid van het internet kan een enkel cybercrimedelict immers duizenden slachtoffers maken. In 2020 is er € 1,8 miljoen geïnvesteerd om bij het OM 20 slachtoffercoördinatoren te werven voor het bijstaan van slachtoffers bij impactvolle zaken. Deze coördinatoren zijn niet speciaal voor online criminaliteit aangesteld, maar indien online criminaliteit veel impact heeft, kunnen de coördinatoren hiervoor worden ingezet. De opleidingen van de coördinatoren zijn op 1 januari 2021 gestart. In 2021 wordt het aantal slachtoffercoördinatoren uitgebreid met nog eens 21.

Wetenschappelijk onderzoek
De afgelopen jaren is in het kader van de integrale aanpak van cybercrime wetenschappelijk onderzoek uitgevoerd naar onder meer daders, slachtoffers en de aard en omvang van cybercrime in Nederland. De uitkomsten onderstreepten in het algemeen de gekozen aanpak en waren daarnaast nuttig voor enige verscherping van de maatregelen. Een adequate aanpak tegen cybercrime vraagt blijvende kennisopbouw. Daarom starten op korte termijn drie nieuwe WODC-onderzoeken en wordt naar verwachting voor de zomer het WODC-onderzoek naar de opsporing, vervolging en verstoring van cybercrime gepubliceerd.

Het is van belang naast kwalitatieve inzichten over voldoende kwantitatieve gegevens te beschikken. Daarom wordt de tweejaarlijkse Veiligheidsmonitor van het CBS uitgebreid ten aanzien van de opgenomen cybercrimedelicten en online criminele fenomenen. De eerste resultaten van de aangepaste Veiligheidsmonitor worden naar verwachting in 2022 gepubliceerd. Om structureel inzicht te krijgen in de trends van diverse vormen van online criminaliteit wordt momenteel gewerkt aan een aanvullende monitor. Deze Monitor Online Criminaliteit zal voortbouwen op de Veiligheidsmonitor en zal in de tussenliggende jaren worden gepubliceerd. De eerste inzichten uit deze monitor worden in 2023 verwacht.

Tot slot
Deze brief toont de voortgang van de integrale aanpak van cybercrime. De investeringen en de inzet van vele partijen hebben geleid tot meer kennis en capaciteit, vele initiatieven die burgers en bedrijven beschermen en ondersteunen, en een versterking van de strafrechtelijke aanpak. Dat is een resultaat om trots op te zijn. Tegelijkertijd is het aantal cybercrimedelicten de afgelopen jaren sterk toegenomen en blijft opsporing in het digitale domein complex. Het probleem dat cybercrime voor de maatschappij vormt, zal naar verwachting blijven toenemen. Dit is een grote opgave, die de komende jaren structurele inspanningen vraagt.

De Minister van Justitie en Veiligheid,

Ferd Grapperhaus

Bijlage – overzicht maatregelen

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Datum
28 juni 2021

Ons kenmerk
3388241

Preventie

Flexibele, snel inzetbare preventiecampagnes
In 2020 is het convenant voor de preventie van cybercrime 'Eerst checken, dan klikken' vernieuwd en verlengd met drie jaar. In dit convenant werken publieke en private partners samen aan de preventie van cybercrime. In het convenant is specifiek aandacht voor *social engineering,* veilig inloggen en *spoofing*. In werkgroepen wordt gekeken welke concrete oplossingen er zijn voor deze onderwerpen. Naast bewustwording voor het algemene publiek wordt aandacht besteed aan de doelgroepen jongeren, senioren, laaggeletterden en het MKB. Om jongeren blijvend bewust te maken van cybercrime en online fraude wordt samengewerkt met het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) en www.scholieren.com. Reeds ontwikkeld preventiemateriaal kan snel worden aangepast aan de actualiteit. Voor ouderen is in april 2021 de campagnemaand 'Senioren en veiligheid' georganiseerd. Via onder meer de ouderenbonden is voorlichtings- en campagnemateriaal over online fraude en cybercrime verspreid. Ook is een 'train-de-trainer'-programma ontwikkeld voor vrijwilligers van ouderenbonden. Hiermee kunnen zij relevante informatie en voorlichting geven aan hun leden. Het Ministerie van BZK heeft in samenwerking met het Ministerie van JenV het voorlichtings- en educatieprogramma 'Klik en Tik: Veilig Online' voor laaggeletterden ontwikkeld. In 2021 kan dit programma gebruikt worden op www.oefenen.nl.

Op 1 oktober 2020 startte Alert Online 2020, voor het eerst onder de vlag van EZK, met een live seminar, geopend door de Staatssecretaris van EZK. In het seminar is onder meer stilgestaan bij de resultaten van het jaarlijkse trendonderzoek dat aan Alert Online is gekoppeld. Gedurende de maand oktober is de "cyberskills test" via sociale media onder de aandacht gebracht. Partners van Alert Online hebben bovendien diverse activiteiten georganiseerd voor medewerkers, klanten en hun directie omgeving, waarbij cybersecurity centraal stond. Voorbeelden daarvan zijn voorlichtingsactiviteiten, trainingen en *escape rooms*. Voor 2021 wordt de aanpak van Alert Online verder doorontwikkeld.

In navolging van eerdere succesvolle daderpreventiecampagnes ontwikkelde de politie in 2020 het lesprogramma "Framed". In een interactieve game spelen jongeren zelf de hoofdrol in een verhaal over cybercrime en moeten zij hierin keuzes maken. Tot op heden is het programma door meer dan 760 scholen aangevraagd en heeft een groot aantal spelers zich geregistreerd. Ook tijdens de sluiting van de scholen vanwege de coronacrisis is "Framed" ingezet, zij het op kleinere schaal. De campagne is inmiddels beloond met een Digital Active Award in de categorie Activation.

Ondersteuning veiligheid niet-vitaal bedrijfsleven: Digital Trust Center (DTC)
Het DTC heeft als doel het verhogen van de digitale weerbaarheid van de 1,8 miljoen bedrijven in Nederland die niet behoren tot de vitale sector. Per 2021 is het DTC een vast organisatieonderdeel geworden van het Ministerie van EZK, waarvoor structurele financiering beschikbaar is gesteld. Het DTC biedt laagdrempelig kennis, informatie en advies over onderwerpen gerelateerd aan cyberweerbaarheid. Dit wordt aangeboden via de website, sociale mediakanalen, interactieve tools en toolkits. Zo kan bijvoorbeeld via de Risicoklasseindeling Digitale Veiligheid een bedrijf aan de hand van 11 vragen een inschatting maken hoe groot het risico is op een cyberincident. Het DTC heeft inmiddels 36 samenwerkingsverbanden die zien op cyberweerbaarheid, verspreid over diverse

regio's, sectoren en ketensamenwerkingen. Deze verbanden delen kennis en algemene informatie over cyberweerbaarheid vanuit het DTC met hun achterban, en concrete dreigingsinformatie via een vaste mailing. De doelstelling is dat er voor eind 2021 40 samenwerkingsverbanden zijn.

Het ministerie van EZK werkt verder aan het laten voldoen van het DTC aan de voorwaarden voor een organisatie die objectief kenbaar tot taak heeft andere organisaties of het publiek te informeren (OKTT) in de zin van de Wet beveiliging netwerk- en informatiesystemen (Wbni). Om de juridische basis voor het verwerken van persoonsgegevens te versterken is gestart met het opstellen van een wetsvoorstel. Daarnaast is eind 2020 gestart met de inrichting van een informatiedienst voor het delen van concrete risico-informatie met individuele bedrijven. Het voornemen is om in de zomer binnen de huidige juridische mogelijkheden met de informatiedienst te starten. Hierover heeft de Staatssecretaris van EZK de Kamer recent geïnformeerd.[16]

Ondersteuning gemeenten en MKB-ondernemingen
Voor de bestuurlijke aanpak van cyberveiligheid in gemeenten is een wegenkaart ontwikkeld. Deze wegenkaart onderscheidt vier rollen voor gemeenten, waaronder de preventieve aanpak van cybercrime. Ten behoeve van deze preventieve aanpak is in oktober 2020 de City Deal Lokale Weerbaarheid Cybercrime ondertekend. Binnen de City Deals worden 18 pilots uitgevoerd, gericht op MKB, gemeenten en wijken, en de groepen jongeren, senioren en laaggeletterden. De eerste fase van de City Deal heeft vier doelstellingen, namelijk het bundelen van innovatiekracht bij lokale koplopers, het koppelen van landelijke initiatieven op het thema cybercrime, het ontwikkelen van nieuwe kennis en het bestuurlijk agenderen van het thema 'lokale aanpak cybercrime'. De voortgang wordt jaarlijks geëvalueerd. De Stuurgroep, onder leiding van burgemeester Buma van Leeuwarden, bewaakt de voortgang van de City Deal. Momenteel wordt gesproken over een tweede fase van de City Deal.

Digitaal veilige hard- en software
De afgelopen jaren is in het kader van de Roadmap Digitaal Veilige Hard- en Software (DVHS) veel vooruitgang geboekt. Hierover heeft de Staatssecretaris van EZK de Kamer op 14 december 2020 geïnformeerd.[17] De inzet bij de *Radio Equipment Directive* is dat de wettelijke minimumeisen die gesteld kunnen worden aan de veiligheid van *Internet of Things*-apparaten dit jaar gereed zijn. Hierna zal een overgangstermijn starten en standaardisatie plaatsvinden. Na afloop van deze overgangstermijn kunnen producten die niet voldoen aan de cybersecurityeisen door het Agentschap Telecom van de markt worden gehaald en geweerd. Het Ministerie van EZK ondersteunt het Nederlandse voorzitterschap van een Europese CEN/CENELEC werkgroep voor *Internet of Things*-veiligheid met een subsidie voor het Nederlandse normalisatie-instituut (NEN).

De Europese *Cyber Security Act* (CSA) creëert een Europees stelsel voor de certificering van ICT-producten, -diensten en –processen. De eerste Europese certificeringsschema's zijn in ontwikkeling, waaronder voor clouddiensten. Nederland draagt hier met de Online Trust Coalitie vanuit publieke en private expertise aan bij. Nederland implementeert de CSA via het wetsvoorstel Uitvoeringswet cyberbeveiligingsverordening voor het inrichten van het certificeringstelsel in Nederland en wijst het Agentschap Telecom aan als de

[16] Kamerstukken II, 2020/21, 2021Z09619
[17] Kamerstukken II, 2020/21, 26 643, nr. 735

nationale autoriteit en toezichthouder. Het wetsvoorstel is inmiddels aangeboden aan de Kamer.[18]

In opdracht van de ministeries van EZK en JenV heeft het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) in samenwerking met diverse private partijen de eerder genoemde Risicoklasseindeling Digitale Veiligheid ontwikkeld, vindbaar op de website van het DTC.[19] Hiermee kunnen ondernemers hun risicoprofiel met bijbehorende te nemen maatregelen bepalen. Daarnaast is het door het CCV ontwikkelde Certificatieschema Pentesten in april 2021 gepubliceerd.[20] Aanbieders van pentesten kunnen zich op basis hiervan laten certificeren. Dit verschaft duidelijkheid voor de afnemer over de kwaliteit van deze dienst. Naar verwachting zal rond de zomer het eerste certificaat voor pentesten worden uitgereikt.

Opsporing, vervolging, sanctionering en verstoring

Versterking aanpak bij politie en strafrechtketen

Met de gelden uit het Regeerakkoord is onder meer een uitbreiding van de cybercrimeteams in de regionale eenheden van de politie gerealiseerd. Bij het OM blijft de capaciteit voor de aanpak van cybercrime hierbij achter. De politie heeft een landelijk dekkende aanpak voor cybercrime. Hierin bestrijdt het THTC de complexe en georganiseerde vormen van cybercriminaliteit en die met een internationale component. De eenheidsoverstijgende fenomeenonderzoeken worden uitgevoerd door de tien regionale cybercrimeteams. De districtsrecherches en basisteams werken, met ondersteuning van de cybercrimeteams, aan veelvoorkomende cybercriminaliteit. De cybercrimeteams nemen steeds complexere onderzoeken voor hun rekening, die eerder alleen het THTC zou kunnen uitvoeren. Het OM en de politie zijn daarnaast deelnemer aan de Cyber Intel/Info Cel (CIIC) die in 2020 van start is gegaan en waar gezamenlijk informatie over dreigingen of incidenten geanalyseerd kunnen worden.

Bewustwording hostingproviders

Nederlandse hostingdiensten worden misbruikt voor het plegen van cybercrime en andere vormen van online criminaliteit, via malafide hostingbedrijven (*bullet proof hosters*), maar ook via hostingbedrijven die zich daar niet van bewust zijn. De hostingsector werkt zelf aan het beperken van misbruik van de eigen systemen voor criminele doeleinden. In 2020 is het publiek-private Anti-Abuse Netwerk (AAN) opgericht. Dit samenwerkingsverband richt zich op het tegengaan van *abuse*, onder meer door het verbeteren van het delen van informatie over misbruik en kwetsbaarheden. Het strafrechtelijk aanpakken van hostingbedrijven die opzettelijk criminaliteit faciliteren is complex. Onderzocht wordt of wijziging van nationale wet- en regelgeving dit kan verbeteren. Daarnaast wordt met het ministerie van EZK gekeken naar het aanpassen van Europese regelgeving voor hostingproviders in de nieuwe *Digital Services Act*. Het voorstel wordt momenteel in EU-verband besproken. De DSA zou hostingproviders moeten stimuleren misbruik van de dienstverlening tegen te gaan. Nederland heeft gesuggereerd dat het opnemen van een zorgplicht in de DSA, waarmee bedrijven zouden worden verplicht basismaatregelen te nemen om criminaliteit via de eigen systemen te beperken, daarvoor een mogelijkheid is.

[18] Kamerstukken II 2020/21, 35 838 nrs. 1-4

[19] https://www.digitaltrustcenter.nl/risicoklasse

[20] https://hetccv.nl/keurmerken/expert/keurmerk-pentesten

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Datum
28 juni 2021

Ons kenmerk
3388241

Verstoring crimineel verdienmodel
De politie en het OM zetten naast opsporing en vervolging in op alternatieve interventies, waaronder verstoringsactiviteiten. Publiek-private samenwerking is hiervoor van groot belang. Het mede door de politie opgerichte publiek-private platform NoMoreRansom bestaat inmiddels vier jaar. Hierop worden decryptiesleutels kosteloos aangeboden aan slachtoffers van ransomware. Ruim 160 partners zijn aangesloten en het platform heeft naar schatting $ 632 miljoen aan schade voorkomen. In 2020 is het samenwerkingsverband NoMoreDDoS samengegaan met de nationale Anti-DDoS-Coalitie. Dit is een publiek-privaat samenwerkingsverband van overheden, internetproviders en –exchanges, academische instellingen, non-profitorganisaties en banken. De coalitie heeft als doel DDoS-aanvallen vanuit verschillende perspectieven te onderzoeken en te bestrijden. In het kader van het project NoMorePhishing wordt gekeken naar structurele verstoring van *phishing*-aanvallen en het vergroten van het bewustzijn onder potentiële slachtoffers. Het afgelopen jaar heeft TNO in samenwerking met de *Electronic Crimes Taskforce* onderzoek gedaan naar manieren om *phishing*-websites gericht op Nederlandse burgers in kaart te brengen en er tegen op te treden.

Versterking nationale wetgeving
De inventarisatie naar mogelijke wijzigingen van nationale wetgeving die bijdragen aan de aanpak van cybercrime is nog gaande. Er wordt op dit moment een prioritering gemaakt en verschillende voorstellen verder uitgewerkt. Eventuele beslissingen hierover zijn aan een volgend kabinet.

Internationale samenwerking
Voor de bestrijding van cybercrime is internationale samenwerking noodzakelijk. Tot april 2021 was het THTC voorzitter van de *Joint Cybercrime Action Taskforce* (J-CAT) van Europol. Dit operationele samenwerkingsplatform van 16 landen coördineert internationale cybercrimeonderzoeken. Daarnaast heeft de politie bij het EMPACT-platform (*European Multidisciplinary Platform Against Criminal Threats*) daderpreventie, schadelijke hosting en technische harmonisatie bij internationale cybercrimebestrijding geagendeerd. De Landelijk Officier van Justitie voor Cybercrime van het Landelijk Parket is lid van het *European Judicial Cybercrime Network* (EJCN) waar *best practices* worden uitgewisseld en de wijze van samenwerking in opsporingsonderzoeken structureel wordt besproken.

Versterking internationale juridische kaders
Nederland mengt zich actief in de Europese discussie over de E-evidence-verordening. Nederland richt zich nu op de discussies in het Europees Parlement en de triloog. Ook blijft Nederland actief deelnemen aan de gesprekken over een tweede protocol bij het Cybercrimeverdrag van de Raad van Europa. Inmiddels is na jaren van gesprekken een conceptprotocol gereed. Dat is een belangrijke mijlpaal. Het protocol heeft een potentieel groot bereik, omdat inmiddels 65 landen bij het cybercrimeverdrag zijn aangesloten.

Aanpak jonge (potentiële) daders en beperking recidive
Sinds eind 2017 werken het OM, de politie, Halt, de Raad voor de Kinderbescherming, Reclassering Nederland en het bedrijfsleven samen in de pilot Hack_Right aan een interventie voor jongeren tussen de 12 en 30 jaar die voor het eerst een cyberdelict plegen. In totaal hebben 39 jongeren het programma doorlopen, zijn bezig of zijn aangemeld. Inmiddels zijn er 22 (cybersecurity) bedrijven aangesloten. Het streven is het programma eind 2021 in te dienen bij

de Erkenningscommissie Justitiële Interventies. Hiertoe is een handreiking voor de uitvoering ontwikkeld en zijn de eerste stappen gezet in de procesevaluatie.

Daarnaast is het bestaande risicotaxatie-instrumentarium (LIJ) aangevuld, zodat het ook gebruikt kan worden voor jongeren die zich schuldig hebben gemaakt aan cybercrime of gedigitaliseerde criminaliteit. Daarbij is de bestaande aanpak Tools4U aangevuld voor online daders.

Het project 'aanpak cybercrime' van de reclassering is in 2020 beëindigd. De reclassering ontwikkelde in dit kader een training 'Gedigitaliseerde criminaliteit'. Deze training is inmiddels door honderden reclasseringswerkers gevolgd en wordt momenteel als gevolg van Covid-19 online aangeboden. De Landelijke Kenniskring Cybercrime met daarin gespecialiseerde reclasseringswerkers uit iedere regio blijft actief. Ingezet wordt op het verder ontwikkelen van kennis en het uitwisselen van ervaringen in cyberzaken. Voor deze reclasseringswerkers en specialisten zijn methodische handvatten beschreven.

Verbetering aangifteproces
Voortgang is geboekt op het verbeteren van het aangifteproces. Zo is de digitale aangiftemogelijkheid voor hulpvraagfraude gerealiseerd en tevens beschikbaar gemaakt voor intake- en servicemedewerkers om de aangifte op het bureau goed op te kunnen nemen. Voor intake- en servicemedewerkers is bovendien een cursus ontwikkeld voor het vergroten van hun digitale basiskennis. Ook wordt de kennis over cybercrime bij *casescreeners* versterkt. De cybercrimeteams bieden ondersteuning bij complexe aangiftes en op diverse plekken worden politievrijwilligers ingezet ter ondersteuning van de intake- en servicemedewerkers.

Aandacht voor slachtoffers
Ondersteuning slachtoffers
Slachtofferhulp Nederland heeft in 2020 de campagne "Van oplichting naar opluchting" uitgevoerd. De campagne deelde verhalen van slachtoffers van *phishing* en andere vormen van online criminaliteit. Met de campagne zijn veel mensen bereikt en er zijn meer mensen lid geworden van online lotgenotengroepen. Hierin kunnen slachtoffers hun ervaringen met elkaar delen.

Slachtoffercoördinatoren
Het OM is in 2020 begonnen met de inzet van slachtoffercoördinatoren voor impactvolle zaken, waaronder impactvolle online delicten. Deze coördinatoren helpen en begeleiden slachtoffers hun wensen tijdens het strafproces beter kenbaar te maken, en informeren hen persoonlijk over hun rechten en hun zaak. Het aantal slachtoffercoördinatoren is in 2020 uitgebreid met 20 fte. In 2021 is een verdere uitbreiding met nog eens 21 fte voorzien.

Voeging slachtoffers strafproces
Vanwege de schaalmogelijkheden van het internet maken cybercriminelen vaak veel slachtoffers tegelijk. Het is een uitdaging om de strafrechtketen zodanig in te richten dat enerzijds deze slachtoffers de aandacht krijgen die ze verdienen en anderzijds het strafproces niet dermate vertraagt dat de berechting van de verdachten naar de achtergrond verdwijnt. Gekeken wordt of bij grote aantallen slachtoffers de voeging van hen in het strafproces kan worden verbeterd.

Slachtoffernotificatie en schadebeperking

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Datum
28 juni 2021

Ons kenmerk
3388241

Bij cybercrime kunnen er veel slachtoffers zijn van één delict. Vaak weten slachtoffers dit zelf niet, wat het risico op het voortduren van een strafbaar feit vergroot. In een van de vele notificatieacties hebben de politie en het OM bijvoorbeeld circa 50.000 slachtoffers genotificeerd. Het effectief delen van operationele gegevens is echter juridisch complex. In het kader van de aanpassing van de Wet politiegegevens wordt onder meer gekeken of aanpassingen noodzakelijk zijn om het notificeren van grote hoeveelheden slachtoffers te vergemakkelijken. Dat zou ook de notificatie bij cybercrimedelicten helpen. In de evaluatie van de Wet beveiliging netwerk- en informatiesystemen wordt de mogelijke rol van het NCSC bij het notificeren van slachtoffers bezien, binnen en buiten haar doelgroep.

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Datum
28 juni 2021

Ons kenmerk
3388241

Wetenschappelijk onderzoek
Het afgelopen jaar is het onderzoek naar de aard en omvang van cyber- en gedigitaliseerde criminaliteit gepubliceerd. Naar verwachting wordt het onderzoek naar opsporing, vervolging en verstoring van cybercrime in de zomer gepubliceerd. In de WODC-programmering voor 2021 zijn drie nieuwe onderzoeken opgenomen. Deze zien op de in- en doorstroom van cyberdaders, de impact van encryptie op de opsporing en gedragsverandering ter voorkoming van slachtofferschap van cybercrime en online criminaliteit. Om het kwantitatieve inzicht in cybercrime te vergroten is de tweejaarlijkse Veiligheidsmonitor aangepast en wordt gewerkt aan een nieuwe monitor gericht op online criminaliteit.