Bijlage – overzicht maatregelen

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.[1]

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.[2] 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

[1] Kamerstukken II, 2020/21, 2021Z09619
[2] Kamerstukken II, 2020/21, 26 643, nr. 735

certificeringstelsel in Nederland en wijst het Agentschap Telecom aan als de nationale autoriteit en toezichthouder. Het wetsvoorstel is inmiddels aangeboden aan de Kamer.[3]

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.[4] Hiermee kunnen ondernemers hun risicoprofiel met bijbehorende te nemen maatregelen bepalen. Daarnaast is het door het CCV ontwikkelde Certificatieschema Pentesten in april 2021 gepubliceerd.[5] 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.

---

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

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

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

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

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.

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.