Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2022–2023

26 643 Informatie- en communicatietechnologie (ICT)

29 911 Bestrijding georganiseerde criminaliteit

Nr. 930

BRIEF VAN DE MINISTER VAN JUSTITIE EN VEILIGHEID

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 4 november 2022

Het leven van burgers en organisaties speelt zich voor een groot deel online af. Dit heeft veel positieve kanten: het internet biedt ons informatie, vermaak, economisch potentieel en meer mogelijkheden voor persoonlijke contacten. We zijn in ons dagelijks leven steeds afhankelijker van de online wereld. De coronacrisis heeft dit versterkt. Dat heeft ook een keerzijde. Criminelen maken gebruik van de voordelen van de online wereld. Het veelvuldig gebruik van de online wereld en de afhankelijkheid ervan vergroten de impact die cybercrime[1] kan hebben. Cybercriminelen kunnen bijvoorbeeld met een ransomware-aanval de gehele bedrijfsvoering van een onderneming platleggen met alle (financiële) schade van dien.[2] Met deze brief informeer ik u, mede namens de Minister van Economische Zaken en Klimaat, over de voortgang van de integrale aanpak van cybercrime en de opsporing in het digitale domein. U bent hier eerder over geïnformeerd op 28 juni 2021.[3] Over de inzet om cybercrime in het midden- en kleinbedrijf tegen te gaan heeft u op 6 juli 2022 een brief ontvangen naar aanleiding van de moties van de leden Ephraïm en Hermans.[4]

Voor de activiteiten die de aanpak van cybercrime in enge zin betreffen, is de voorliggende brief een nadere detaillering van onderdelen van de Nederlandse Cybersecuritystrategie (NLCS), met de focus op criminali-

[1] 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 online fraudevormen, 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.

[2] CSBN 2022 Cybersecuritybeeld Nederland 2022 | Nationaal Coördinator Terrorismebestrijding en Veiligheid (nctv.nl).

[3] Kamerstukken 26 643 en 29 911, nr. 768.

[4] Kamerstukken 26 643 en 32 637, nr. 907.

kst-26643-930
ISSN 0921 - 7371
's-Gravenhage 2022

teitsbestrijding.[5] Daarnaast bevat deze brief maatregelen ter versterking van de opsporing en vervolging in het digitale domein. Deze zijn ook voor vele andere vormen van criminaliteit van belang, zowel voor cybercrime en gedigitaliseerde criminaliteit als voor traditionele, fysieke vormen van criminaliteit. Immers, door het wijdverbreid gebruik van het digitale domein manifesteert bewijs zich steeds vaker in digitale vorm.

Hieronder wordt eerst een beeld van de ontwikkeling van cybercrime geschetst, gevolgd door een beschrijving van de aanpak en concrete prioriteiten daarin. Daarna wordt apart aandacht besteed aan de aanpak van ransomware. Tot slot komt de verbetering van de informatiepositie aan de orde. In de bijlage is een overzicht van maatregelen opgenomen.

Algemeen beeld – ontwikkeling cybercrime

Cybercrime neemt in politieregistraties al meerdere jaren toe, van rond de 2.000 per jaar in de jaren 2014–2017 naar 14.168 in 2021.[6] De toename van het aantal aangiften vertaalt zich in de instroomcijfers van het Openbaar Ministerie (OM). In twee jaar tijd is het aantal verdachten met 47% gestegen.[7] Het slachtofferschap van cybercrime ligt hoog. Het Centraal Bureau voor de Statistiek (CBS) rapporteert dat in 2021 6,9% van de Nederlanders van 15 jaar en ouder slachtoffer is geworden van computervredebreuk («hacken»).[8, 9] Als alle vormen van online criminaliteit worden bezien, geeft in totaal 17% van de Nederlanders aan hiervan slachtoffer te zijn geworden.[10] De toename van online delicten staat in contrast met de ontwikkeling van traditionele criminaliteit: deze neemt al jaren in omvang af.[11] Ter illustratie: waar mijn voorganger enkele jaren geleden meldde dat hacken «inmiddels vaker voorkomt dan fietsendiefstal», zijn nu bijna twee keer zo veel mensen slachtoffer van hacken dan van fietsdiefstal.[12]

De werkwijzen van cybercriminelen blijven zich ontwikkelen en nemen steeds andere vormen aan.[13] Criminelen die voorheen traditionele vormen van criminaliteit plegen, doen dat nu ook online. Zij maken soms gebruik van de actualiteit om misleidende berichten geloofwaardigheid te geven, zoals bleek tijdens de coronacrisis. Daarnaast is er zware, georganiseerde cybercrime, verantwoordelijk voor bijvoorbeeld geavanceerde *ransomware*-aanvallen en datadiefstal bij het midden- en kleinbedrijf (MKB) en grote organisaties.[14] *Ransomware* blijkt met name voor organisaties voor grote problemen te zorgen. Naast dat organisaties zelf direct slachtoffer kunnen worden door een *ransomware*-aanval op hun eigen IT-omgeving kunnen zij ook indirect slachtoffer worden door een *ransomware*-aanval bij organisaties die onderdeel uitmaken van hun toeleveringsketen. Het Cybersecuritybeeld Nederland (CSBN) meldt dat ransomware zelfs de nationale veiligheid kan bedreigen.[15] Uit gegevens

---

[5] De Nederlandse Cybersecuritystrategie (NLCS) geeft de visie van het kabinet op een digitaal veilig Nederland en de doelen en acties die hieraan bijdragen, een overzicht van concrete acties per doelstelling.

[6] data.politie.nl – Geregistreerde misdrijven en aangiften; soort misdrijf, gemeente 2022.

[7] https://www.om.nl/actueel/nieuws/2022/05/03/jaarbericht-om-zorgen-over-misdaad-en-maatschappelijke-klimaat.

[8] Ter vergelijking met politieregistraties: dit zijn 1.000.670 mensen.

[9] CBS – veiligheidsmonitor 5. Online criminaliteit (cbs.nl).

[10] Idem. Dit zijn bijna 2,5 miljoen mensen.

[11] Idem.

[12] Kamerstuk 28 684, nr. 522; CBS – Veiligheidsmonitor.

[13] Europol – Internet Organized Crime Threat Assessment 2021 (iOCTA) Internet Organised Crime Threat Assessment (IOCTA) 2021 | Europol (europa.eu).

[14] CSBN 2020: Cybersecuritybeeld Nederland (CSBN) 2020 | Publicatie | Nationaal Cyber Security Centrum (ncsc.nl), CSBN 2021: Cybersecuritybeeld Nederland 2021 | Publicatie | Nationaal Coördinator Terrorismebestrijding en Veiligheid (nctv.nl).

[15] Idem.

van de politie blijkt dat vooral rechtspersonen slachtoffer worden van *ransomware*. Een bijkomende trend is dat *ransomware* vaker onderdeel is van een combinatie van strafbare feiten, waarbij naast het eisen van de initiële losgeldsom voor het ontsleutelen van gegevens, vertrouwelijke gegevens worden buitgemaakt en een tweede of derde keer losgeld wordt geëist om het publiceren ervan te voorkomen. Ook bedreiging met een DDoS-aanval komt voor.

Criminelen kunnen processen zeer effectief automatiseren en uitbesteden in een inmiddels omvangrijk en professioneel crimineel ecosysteem.[16] Een enkele crimineel kan in één klik duizenden potentiële slachtoffers bereiken. Cybercrime heeft door de grote schaalbaarheid inmiddels qua aantallen slachtoffers, schade en criminele opbrengsten een «industriële omvang» aangenomen.[17] De weerbaarheid is minder schaalbaar. Basismaatregelen zoals het gebruik van multi-factorauthenticatie, het doen van updates en het maken van back-ups worden onvoldoende toegepast.[18] Uit het Alert Online onderzoek (2022) blijkt desalniettemin dat 51% van de Nederlanders op zo veel mogelijk accounts en apparaten multi-factorauthenticatie toepast of bereid is dat te doen.[19] Dit is meer dan de afgelopen jaren het geval was, maar het vergt blijvende aandacht.

De opsporing in de digitale wereld blijft lastig. Technologieën om de privacy van legitieme gebruikers te beschermen worden ook door criminelen gebruikt om hun identiteit en locatie af te schermen. Dader en slachtoffer hoeven elkaar niet fysiek te treffen. Er worden continu nieuwe digitale producten en diensten ontwikkeld, ook specifiek voor criminele doeleinden. Kenmerkend voor het internet is bovendien dat het geen territoriale grenzen kent. Veel daders van vooral georganiseerde cybercrime bevinden zich niet in Nederland, terwijl hier wel slachtoffers worden gemaakt of de Nederlandse digitale infrastructuur voor criminele doeleinden wordt misbruikt. De politie en het OM hebben de afgelopen jaren belangrijke successen geboekt, maar deze zijn niet vanzelfsprekend. Het internet mag geen vrijplaats worden voor criminelen en misdaad mag niet lonen. Ook dat vergt blijvende aandacht.

De aanpak

Om cybercrime adequaat en effectief tegen te gaan richten we ons op twee hoofdsporen. Het eerste spoor richt zich op preventie en slachtofferzorg, waarmee criminaliteit wordt voorkomen en de impact ervan beperkt. Het tweede spoor richt zich op opsporen, vervolgen en verstoren, waarin de strafrechtelijke aanpak voorop staat. Hieronder wordt de invulling per hoofdspoor nader uitgewerkt.

Preventie & slachtofferzorg

De inzet van preventie concentreert zich op drie typen maatregelen: (potentiële) slachtoffers weerbaarder maken (slachtofferpreventie) door hun basisveiligheid te vergroten, de daderpopulatie verkleinen (daderpreventie) door middel van gerichte interventies om daderschap te ontmoe-

[16] CSBN 2022.

[17] CSBN 2022, Nationaal Coördinator Terrorismebestrijding en Veiligheid – Cybersecuritybeeld Nederland 2022 | Publicatie | Nationaal Coördinator Terrorismebestrijding en Veiligheid (nctv.nl).

[18] De set relevante «basismaatregelen» verschilt voor burgers en (vitale) organisaties. Burgers: https://veiliginternetten.nl/5-tips-basisveiligheid/, MKB: De 5 basisprincipes van veilig digitaal ondernemen | Digital Trust Center (Min. van EZK), (vitale) organisaties: https://www.ncsc.nl/onderwerpen/basismaatregelen.

[19] https://www.rijksoverheid.nl/documenten/rapporten/2022/09/30/cybersecurity-onderzoek-alert-online-2022.

digen en recidive te beperken, en systemen en producten waar burgers en bedrijven gebruik van maken veiliger maken (situationele preventie). De zorg voor slachtoffers heeft als doel de impact van criminaliteit en herhaald slachtofferschap te beperken. Het heeft daarmee ook een preventief effect.

Vergroten basisweerbaarheid burgers en MKB

Het vergroten van de digitale basisweerbaarheid is nodig om mensen en organisaties minder vaak slachtoffer te laten worden van cybercrime en om de impact ervan te verkleinen. Het gaat om het informeren van mensen en bedrijven over vormen van cybercrime en het stimuleren van cybersecurity basismaatregelen. Sommige maatregelen vergen geen diepgaande technische kennis, maar veel mensen kunnen enige ondersteuning of een herinnering goed gebruiken. Daarom is publieksvoorlichting op zijn plaats.[20] Het Coalitieakkoord (Bijlage bij Kamerstuk 35 788, nr. 77) heeft hiervoor extra middelen vrijgemaakt op de begroting van het Ministerie van Justitie en Veiligheid, oplopend van € 0,6 miljoen euro in 2023 naar € 2 miljoen structureel vanaf 2027. Eind 2022 is de campagne «doe je updates», gericht op de veiligheid van slimme apparaten, herhaald. In oktober vond de cyber securitymaand plaats, waarin media-aandacht voor multi-factorauthenticatie is gestart. Daarnaast is er aandacht voor het vergroten van de basisweerbaarheid in het Actieprogramma Veilig Ondernemen. In het kader van het project Samen Digitaal Veilig wordt de samenwerking met brancheorganisaties versterkt. De Ministeries van Justitie en Veiligheid, Binnenlandse Zaken en Koninkrijksrelaties, en Economische Zaken en Klimaat werken nauw samen aan het vormgeven van communicatie richting burgers en bedrijven. Een overzicht van maatregelen ter vergroting van de basisweerbaarheid is opgenomen in de bijlage.

City Deal «Lokale weerbaarheid cybercrime»

Gemeenten zijn vanwege hun kennis van de lokale problematiek en netwerken in staat om op lokaal niveau burgers en bedrijven te faciliteren in het nemen van preventieve maatregelen. Met een portfolio van ruim dertig City Deal-projecten is er een ruim aanbod van innovatieve interventies voor gemeenten gecreëerd. De projecten worden geëvalueerd, zodat succesvolle projecten bij meer gemeenten kunnen worden ingezet. In augustus 2022 heb ik met een bijdrage van de Ministeries van Economische Zaken en Klimaat, en Binnenlandse Zaken en Koninkrijksrelaties een meerjarige, structurele subsidie toegekend aan het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) om de City Deal lokale weerbaarheid cybercrime verder te ondersteunen. Daarmee is een bedrag van € 2 miljoen per jaar gemoeid. De focus in de brede inzet ligt op het beschermen van kwetsbare groepen, onder meer zoals genoemd in de Kamerbrieven over de brede preventie van jeugdcriminaliteit en over de preventie van cybercrime in het midden- en kleinbedrijf.[21] Ook wordt de capaciteit voor regionale samenwerking versterkt. Met de tools in een makkelijk keuzemenu van interventies (de «cyber snackbox») en de regionale ondersteuning kunnen kleinere gemeenten met weinig budget en personeel op kortere termijn de eerste stappen zetten voor het versterken van de weerbaarheid tegen cybercrime bij kwetsbare burgers. Dit stimuleert gemeenten om cybercrimepreventie op te nemen in de Integrale Veiligheidsplannen 2023–2026.

[20] Dit is ook opgenomen in het actieplan van de NLCS.
[21] Kamerstuk 28 741 nr. 86; Kamerstuk, 26 643 nr. 907.

Veilige ICT-producten en diensten

Situationele preventie voorkomt dat de gelegenheid voor criminelen om hun schadelijke acties uit te voeren zich voordoet. Voor het tegengaan van cybercrime kan dat gedaan worden door de veiligheid van ICT-producten en diensten te verbeteren. Om de veiligheid van ICT-producten en diensten te verbeteren voor gebruikers (*security-by-design*, voor burgers en bedrijven) wordt onder de tweede pijler van de NLCS ingezet op de implementatie van onder andere Europese wet- en regelgeving en certificering.[22] Daarmee wordt de verantwoordelijkheid voor veiligheid meer bij de producent of aanbieder van ICT-producten en -diensten gelegd, en minder bij individuele burgers en organisaties. Een voorbeeld daarvan is de Nederlandse inzet voor de onlangs door de Europese Commissie gepresenteerde *Cyber Resilience Act.* U bent hierover op 21 oktober jl. met een BNC-fiche geïnformeerd, waarbij Nederland inzet op een zorgplicht voor ICT-producten en -diensten.

Cyber Offender Prevention Squad (COPS)

Omdat een enkele dader in korte tijd vele slachtoffers kan maken, kan daderpreventie effectief zijn in het beperken van cybercrime. Bovendien is het van belang schaars IT-talent te behouden voor een positieve bijdrage aan de samenleving en de strafrechtketen te ontlasten. Met een daderpreventietoolbox wil het daderpreventieteam Cyber Offender Prevention Squad (COPS) van de politie voorkomen dat jongeren een cybercriminele carrière starten of verder ontwikkelen. Dit gebeurt door daders en potentiële daders bij te sturen naar positieve keuzes, en om van daders die bewust kiezen voor cybercrime de positie te verzwakken en hun cybercriminele markten te verstoren.

Slachtoffernotificatie

Bij cybercrime kunnen mensen en organisaties lang slachtoffer zijn, en hun gegevens en hun apparatuur voor een lange periode gecompromitteerd zijn, voordat de negatieve effecten merkbaar worden. Door specifieke en gerichte informatie met slachtoffers en potentiële slachtoffers te delen, kunnen zij de nodige maatregelen nemen om een aanval te voorkomen en/of de schade daarvan te beperken. Bovendien kunnen mensen en organisaties, wiens systemen door criminelen worden misbruikt voor strafbare feiten zoals DDoS-aanvallen, hun systemen opschonen. De afgelopen periode zijn vanuit de politie diverse initiatieven gestart op het gebied van slachtoffernotificatie, waaronder het project «No More Leaks» (zie kader). Om slachtoffers effectiever te kunnen notificeren wordt er een verkenning uitgevoerd naar de wijze waarop dit meer structureel en schaalbaar vormgegeven en uitgevoerd zou kunnen worden. Daarnaast wordt aanpassing van de juridische kaders bezien.

Project No More Leaks

Gestolen inloggegevens zijn onderdeel van de ondergrondse online economie en zijn een bron van vele soorten online criminaliteit. No More Leaks is een project waarmee de politie data kan delen met private partners om misbruik met gestolen inloggegevens te voorkomen. Inloggegevens zijn persoonsgegevens. De inloggegevens worden door de politie uitsluitend «ge*hasht*» gedeeld met deelnemende bedrijven. Met *hashen* wordt bedoeld dat de inloggegevens met behulp van een wiskundige berekening worden

[22] Dit is ook opgenomen in het actieplan van de NLCS.

versleuteld. Dit heeft als doel de persoonsgegevens te beveiligen en te pseudonimiseren. Deelnemende partijen kunnen de lijst met *hashes* van de politie gebruiken als extra beveiligingsmaatregel in hun inlogproces. Als een *hash* overeenkomt, dan krijgt de desbetreffende klant van het bedrijf een wachtwoordwijzigingsverzoek om zo mogelijke schade te voorkomen. Na het wijzigen van het wachtwoord is het account van de klant weer veilig.

No More Leaks heeft als doel om de Nederlandse samenleving digitaal veiliger te maken door bedrijven weerbaarder te maken en daarbij het misbruik van klantaccounts – en de daaruit voortkomende criminaliteit – te doen verminderen. Het project zal nog worden geëvalueerd om te bepalen of en op welke manier deze aanpak wordt gecontinueerd en eventueel uitgebreid.

Opsporen, vervolgen, verstoren

Het internet mag geen vrijplaats zijn voor criminelen en misdaad mag niet lonen. Criminelen moeten worden opgespoord en voor de rechter gebracht. Waar het opsporen en/of vervolgen van cybercriminelen niet haalbaar is of onvoldoende effectief blijkt, is verstoring van criminele processen een alternatieve of aanvullende methode om schade voor burgers en bedrijven te beperken. Deze aanpak richt zich bijvoorbeeld op de criminele verdienmodellen die achter de verschillende vormen van cybercrime schuilgaan. Een voorbeeld van verstoring is de aanpak van «Flubot». Met deze malware konden criminelen meekijken met handelingen op de telefoon van een slachtoffer, bijvoorbeeld het invoeren van wachtwoorden of het doen van bankzaken. De politie en het OM zijn er in geslaagd de verspreiding van de malware te stoppen door in te grijpen in het criminele proces. Bij dit complexe onderzoek waren 11 landen en Europol betrokken. Vanwege de schaalbaarheid van cybercrime is het niet mogelijk en niet effectief om elke melding of aangifte afzonderlijk te behandelen. Daarom is een proactieve en datagedreven aanpak van cybercriminele fenomenen en dadergroepen, waaronder cybercriminele dienstverleners, een uitgangspunt in de strategie van de politie en het OM. Het coalitieakkoord heeft een investering in het OM voor de aanpak van cybercrime mogelijk gemaakt. Het betreft een investering van € 4 miljoen in 2022 oplopend naar € 12 miljoen structureel vanaf 2024. Daarmee wordt in de komende jaren de basis bij het OM op orde gebracht en wordt invulling gegeven aan de motie van de leden Groothuizen en Van Toorenburg.[23] Daarnaast investeert de politie in datagedreven werkwijzen, wat ook de aanpak van cybercrime kan helpen.

Verhoging ambitie opsporingsonderzoeken

In de Veiligheidsagenda 2023 t/m 2026 is cybercrime, net als in de vorige Veiligheidsagenda, een prioritair thema. De ambitie voor de komende vier jaar is om het aantal opsporingsonderzoeken op cybercrime stapsgewijs te laten stijgen. Vooral voor het aantal reguliere onderzoeken is op termijn een stijging in de ambitie bepaald, van 310 naar 450 per jaar. Bovendien is het de ambitie dat een groter deel van deze onderzoeken criminaliteit in georganiseerd verband betreft. In onderstaande tabel is de ambitie voor de komende jaren zichtbaar gemaakt. De alternatieve interventies betreffen acties anders dan vervolging, bijvoorbeeld ter verstoring van criminele werkwijzen. Een andere afspraak die in de Veiligheidsagenda wordt gemaakt is dat de politie het vanaf 2023 voor meer cybercrimefenomenen mogelijk maakt om online melding of aangifte te doen. In een

[23] Kamerstuk 35 570 VI, nr. 60.

aparte brief informeer ik u heden over alle thema's en ambities in de nieuwe Veiligheidsagenda en over de context en de werking ervan.

Ambities Veiligheidsagenda	2023	2024	2025	2026
Cybercrime				
Aantal verdachten cybercrime regulier	310	350	400	450
Waarvan CSV's	10%	10%	20%	20%
Waarvan alternatieve interventies	25%	25%	25%	25%
Aantal fenomeenonderzoeken	41	41	43	45
Waarvan alternatieve interventies	50%	50%	50%	50%
Aantal high tech crime onderzoeken (inclusief alternatieve interventies)	20	20	20	20

Misbruik hostingproviders

Criminelen misbruiken de diensten van hostingproviders voor hun illegale activiteiten. Veel hostingproviders treden hier adequaat tegen op. Om de schaalvoordelen van hostingdiensten minder toegankelijk te maken voor criminelen, is het van belang dat alle hostingproviders hier maatregelen tegen nemen. Daarnaast heeft de politie onlangs diverse hostingproviders op de hoogte gesteld van criminele dienstverleners die mogelijk misbruik maken van hun systemen. Daarbij is verzocht, indien deze partijen bij deze hostingproviders bekend zijn, deze niet meer als klant te accepteren. Voor hostingproviders die willens en wetens criminaliteit faciliteren kan een strafrechtelijke aanpak passend zijn. Onlangs heeft het Gerechtshof in Den Haag bepaald dat dergelijke dienstverleners onder omstandigheden niet zijn uitgesloten van strafrechtelijke aansprakelijkheid, ook niet als zij geen bevel tot ontoegankelijk maken van gegevens hebben ontvangen. Deze uitspraak biedt mogelijkheden voor vervolging van hostingproviders die criminelen actief helpen.[24]

Internationaal verkrijgen van bewijs

Om de grensoverschrijdende samenwerking in het digitale domein te versterken heeft Nederland in de afgelopen jaren actief deelgenomen aan Europese en internationale onderhandelingen voor nieuwe instrumenten die snellere en meer efficiënte samenwerking bij het grensoverschrijdend verkrijgen van elektronisch bewijs beogen. Onderhandelingen binnen de Raad van Europa hebben geresulteerd in een tweede protocol bij het Cybercrimeverdrag (het Verdrag van Boedapest). Nederland heeft het protocol op 12 mei 2022 ondertekend. In de Europese Unie wordt daarnaast gesproken over de E-evidence verordening en de bijbehorende richtlijn, die het vorderen van digitaal bewijs in EU-lidstaten efficiënter maken. De triloog hierover is nog niet voltooid. Begin 2022 zijn onderhandelingen gestart om te komen tot een nieuw verdrag over cybercrime bij de Verenigde Naties. Daarin zijn regelingen voorzien over strafbaarstellingen, strafvorderlijke bevoegdheden en bepalingen die de internationale samenwerking regelen. Volgens de huidige plannen eindigen de onderhandelingen eind 2023.

Aanpak ransomware

Ransomware is een specifiek soort cybercrime. Veel maatregelen voor de algemene aanpak van cybercrime helpen ook tegen ransomware, zoals het bevorderen van beveiligingsmaatregelen. Daarnaast worden enkele specifieke activiteiten ontplooid. Deze worden hieronder kort toegelicht.

[24] ECLI:NL:GHDHA:2022:1550 d.d. 23 augustus 2022.

Informatievoorziening & digitale aangifte

Het Nationaal Cyber Security Centrum (NCSC) en het Digital trust Center (DTC) stellen diverse producten en diensten ter beschikking die organisaties kunnen helpen. Het NCSC waarschuwt organisaties en bedrijven dagelijks voor digitale dreigingen of kwetsbaarheiden die gerelateerd zijn aan malware-aanvallen, zoals *ransomware*. Met de *factsheet Ransomware* bieden het NCSC en het DTC organisaties een overzicht van de verschillende soorten *ransomware* en beschrijft het maatregelen die organisaties kunnen nemen om een ransomware aanval te voorkomen.[25] Het Incidentresponsplan *ransomware* van het NCSC geeft organisaties praktische handvatten om bij een *ransomware*-aanval adequaat te reageren.[26] Het dringende advies blijft om geen losgeld te betalen. Het betalen van losgeld biedt geen garantie dat criminelen de systemen weer toegankelijk maken en houdt bovenal het criminele verdienmodel in stand. Slachtoffers van *ransomware* worden uitdrukkelijk opgeroepen aangifte of melding te doen bij de politie. Het doel van de politie is om digitaal aangifte doen van *ransomware* eind 2022 mogelijk te maken.

Opsporing, vervolging, verstoring – Ransomware Taskforce

Samen met nationale en internationale partners streeft de Ransomware Taskforce van de politie en het OM een brede en proactieve bestrijding van *ransomware* na. Hierbij komen niet alleen opsporing en vervolging aan bod, maar ook verstoring van criminele activiteiten evenals het helpen van (potentiële) slachtoffers. Een voorbeeld daarvan is de succesvolle verstoring van het Emotet-botnet. Daarna zijn eind 2021 tijdens een grote internationale operatie van politie en justitie in acht landen twaalf verdachten opgespoord die vermoedelijk deel uit maken van een wereldwijd netwerk van cybercriminelen. Tijdens een recente actie in oktober 2022 heeft de politie 150 decryptiesleutels van de ransomwaregroep Deadbolt bemachtigd door een truc met de betaling van cryptovaluta. Hierdoor konden veel slachtoffers worden geholpen zonder de criminelen te betalen.

Op de website NoMoreRansom.org bieden de politie en inmiddels meer dan 150 nationale en internationale partners, zoals IT-securitybedrijven en politiediensten, kosteloos de hen bekende ontsleuteltools aan. Hiermee kunnen slachtoffers in bepaalde gevallen zonder losgeld te betalen weer toegang tot hun systemen krijgen. Naar schatting is hiermee in zes jaar tijd internationaal bijna een miljard euro aan schade voorkomen.[27]

Regelgeving cryptovaluta

Ransomware-losgeld wordt vrijwel altijd geëist in cryptovaluta. Deze zijn lastiger traceerbaar dan giraal geld, en gemakkelijker te innen dan contanten. Dat maakt cryptovaluta aantrekkelijk voor criminelen, en lastig voor de opsporing. In EU-verband wordt gewerkt aan verdere aanscherping van anti-witwasregels voor cryptovaluta. Hiervoor verwijs ik naar de beleidsagenda Aanpak Witwassen, die de Minister van Financiën en ik op 23 september jl. aan uw Kamer hebben gestuurd. Ook wordt gewerkt aan een verbod op het verlenen van diensten rondom

---

[25] https://www.ncsc.nl/binaries/ncsc/documenten/factsheets/2020/juni/30/factsheet-ransomware/71059_NCSC_FS+Ransomeware+NL_WEB.pdf.

[26] https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2022/juni/3/incidentresponsplan-ransomware/Incidentenresponsplan+Ransomware.pdf.

[27] https://www.europol.europa.eu/media-press/newsroom/news/unhacked-121-tools-against-ransomware-single-website.

zogenaamde «*privacy coins*», virtuele valuta met ingebouwde anonimiseringsfuncties. Deze regels worden in de loop van 2024 van toepassing.

Internationale samenwerking

De Nederlandse politie werkt intensief samen met buitenlandse politiediensten en organisaties als Europol om cybercriminaliteit, inclusief *ransomware*, te bestrijden. Daarnaast wisselt Nederland internationaal kennis en ervaring over de bestrijding van *ransomware* uit met andere landen via onder meer het *Counter Ransomware Initiative* (CRI). Het CRI is een door de Verenigde Staten geïnitieerd platform waar op strategisch niveau internationale afstemming plaatsvindt ten aanzien van *ransomware*-bestrijding. In EU verband kunnen tevens sancties tegen cybercriminele organisaties worden ingesteld, zoals in 2020 tegen de Noord-Koreaanse organisatie achter de wereldwijde WannaCry-aanval.

Versterken kennis- en informatiepositie

Een belangrijke randvoorwaarde voor preventief en repressief beleid tegen cybercrime is een goede informatiepositie. Dit geldt voor dieper inzicht in slachtofferschap, cijfermatig inzicht in de ontwikkeling van cybercrime in Nederland en inzicht in criminele werkwijzen. Afgelopen jaar is onder meer de Veiligheidsmonitor uitgebreid, waardoor meer inzicht is verkregen in de omvang van diverse typen cybercrime bij natuurlijke personen. Daarnaast wordt gewerkt aan een nieuwe Monitor Online Criminaliteit. De eerste rapportage daarvan wordt in april 2023 verwacht. Daarnaast zet de politie in op het maken van criminaliteitsbeelden, waaronder beelden over cybercrime. Dit is afgesproken in de nieuwe Veiligheidsagenda en zal in de Nationale Intelligence Agenda verder worden uitgewerkt. Deze beelden geven richting aan de keuze van de politie en het OM op welke fenomenen wordt ingezet. Daarnaast kunnen zij helpen bij de beleidsvorming en prioriteitsteling.

Tot slot

Cybercriminaliteit is uitgegroeid tot een veel voorkomende misdaadvorm die aanzienlijke schade berokkent en een risico kan vormen voor de nationale veiligheid. De afgelopen jaren is geïnvesteerd in preventie, de strafrechtelijke aanpak en het versterken van onze kennis over de omvang ervan en de criminele werkwijzen. Gezien het wijdverbreide karakter en de risico's die er mee gepaard gaan is blijvende aandacht nodig.

De Minister van Justitie en Veiligheid,
D. Yeşilgöz-Zegerius

Bijlage: Overzicht maatregelen

Preventie & slachtofferzorg

Campagne «Doe je updates»

Ook dit jaar is geïnvesteerd in de basisweerbaarheid van mensen en organisaties in Nederland. Zo heeft het Ministerie van EZK eind 2021/begin 2022 de vierde ronde van de campagne «doe-je-updates» gedaan, die met name gericht was op het updaten van «slimme» -apparaten.[28] De publiekscampagne «doe je updates» wordt voortgezet. Eind 2022 en begin 2023 is de vijfde ronde voorzien.

Alert Online en campagnes multi-factorauthenticatie

Oktober is traditioneel de Europese cybersecurity maand. In Nederland wordt deze afgetrapt onder de vlag van Alert Online, waarbij met verschillende activiteiten door publieke en private partners van Alert Online aandacht wordt gevraagd voor cybersecurity. In deze maand is bovendien door middel van inzet van *branded content* in diverse media het gebruik van multi-factorauthenticatie gestimuleerd. Daarnaast is het Ministerie van Justitie en Veiligheid voornemens een subsidie aan ECP te verlenen voor het versterken van de campagne ter promotie van het gebruik van multi-factorauthenticatie. Dit kan helpen tegen veel vormen van cybercrime, waaronder het hacken van accounts en ransomware.

Nationaal Platform Criminaliteitsbeheersing – Actieprogramma Veilig Ondernemen

In het kader van het Actieprogramma Veilig Ondernemen 2019–2022 van het Nationaal Platform Criminaliteitsbeheersing (NPC) is de afgelopen vier jaar door overheid en bedrijfsleven intensief samengewerkt om onder andere de cyberweerbaarheid van ondernemers in het midden- en kleinbedrijf te vergroten. Om deze publiek-private aanpak te intensiveren en een vervolg te geven aan de succesvolle aanpak binnen het vorige actieprogramma wordt momenteel gewerkt aan het Actieprogramma Veilig Ondernemen 2023–2026.

City Deal «Lokale weerbaarheid cybercrime»

In het kader van de City Deal is door het CCV de zogeheten de «Cyber Snackbox» ontwikkeld: een makkelijk keuzemenu van interventies. Die is afgelopen zomer naar alle gemeenten gestuurd, zodat ze met eenvoudige interventies een eerste start kunnen maken. De snackbox bevat onder andere een overzicht van relatief gemakkelijke en goedkope toepasbare preventieprojecten (waaronder Hackshield) en een eenvoudige methode om de omvang en schade van cybercrime in een gemeente te schatten, om zo bewustzijn bij de gemeenteraad te creëren.

Cyberweerbericht

In 2021 is gestart met een pilot van het «cyberweerbericht»: een pagina op veiliginternetten.nl waar periodiek de meest actuele vormen van cybercrime waar burgers mee te maken krijgen, worden gedeeld. Het weerbericht wordt samengesteld op basis van een analyse van de politie en de FraudeHelpDesk.

---

[28] Apparaten verbonden aan het internet zoals de slimme thermostaat, slimme deurbel, smart TV etc.

Samen Digitaal Veilig

Het project Samen Digitaal Veilig is onderdeel van nieuwe samenwerkingsafspraken tussen de ondernemersorganisaties (MKB-Nederland en BOVAG) en de Ministeries van Justitie en Veiligheid en Economische Zaken en Klimaat. Het project richt zich op het weerbaar maken van bedrijven. Het platform Samen Digitaal Veilig biedt onder meer een elektronische leeromgeving voor medewerkers, met korte informatieve films en toetsen. Brancheorganisaties spelen in de verspreiding van die informatie een belangrijke rol. Komend jaar wordt onder meer ingezet op gedragsonderzoek en de verspreiding van informatie onder meerdere branches.

Verkenning Anti-Phishing Schild

Naar Belgisch voorbeeld wordt verkend of een «anti-phishing-schild» ook in Nederland kan worden opgezet. Daarmee zou het mogelijk worden criminele links in berichten te melden om deze vervolgens onschadelijk te maken, dan wel van een waarschuwing te voorzien. Dit zou het slachtofferschap van phishing en daaropvolgende delicten kunnen tegengaan.

Cyber Offender Prevention Squad (COPS)

Met een daderpreventietoolbox wil het daderpreventieteam Cyber Offender Prevention Squad (COPS) van de politie voorkomen dat jongeren een cybercriminele carrière starten of verder ontwikkelen. Dit gebeurt door daders en potentiële daders bij te sturen naar positieve keuzes, en om van daders die bewust kiezen voor cybercrime de positie te verzwakken en hun cybercriminele markten te verstoren. De interventies van COPS worden op drie niveaus ingezet. Primaire preventie, zoals de ontwikkeling van educatiemateriaal en bewustzijnscampagnes, richt zich in beginsel op alle jongeren. Secundaire preventie richt zich op jongeren die een grotere kans op daderschap hebben. Jongeren met interesse in cybercrime gerelateerde onderwerpen worden onder meer benaderd met online advertentiecampagnes en bijeenkomsten. De tertiaire interventies voor jongeren die daadwerkelijk cybercrime hebben gepleegd, maar die mogelijk nog bijgestuurd kunnen worden. Dit gebeurt onder meer door stopgesprekken en de alternatieve straf van het programma Hack_Right.

Framed

Opnieuw speelden tienduizenden jongeren van 12 tot 18 jaar de serious game *Framed*, die hen indringend laat ervaren dat cybercriminaliteit strafbaar is en wat de gevolgen kunnen zijn voor slachtoffers. Met de campagne Framed van de politie worden jongeren hier bewust van gemaakt. Een belangrijk middel daarbij is de inzet van een spel op scholen waarmee leerlingen op hun eigen smartphone en vanuit hun eigen leefwereld bewust worden gemaakt van online strafbaar gedrag en welke gevolgen dit gedrag voor hen en voor de slachtoffers heeft. Na gebruik van de game worden de resultaten ook klassikaal nabesproken aan de hand van een landelijk lespakket. De campagne Framed is nu door ruim de helft van de Nederlandse scholen aangevraagd en inmiddels hebben ruim 100.000 leerlingen hieraan meegedaan.

(B)adwords

In het project «(B)adwords» worden door advertenties bij het gebruik van bepaalde online zoekwoorden jongeren geïnformeerd over strafbaarheid van cybercrime, consequenties en legale alternatieven. Het project is gericht op risicojongeren die nieuwsgierig zijn naar laagdrempelige

cybercriminaliteit zoals DDoS-aanvallen. Dit project wordt versterkt en uitgebreid.

HackShield

De cybersecuritygame HackShield, die kinderen van 8 tot 12 jaar opleidt tot *junior cyber agents* wordt breder beschikbaar gemaakt. Eind 2021 telde Nederland 68.000 *agents* in 103 deelnemende gemeenten.

Hack_Right

Hack_Right is een alternatief of aanvullend straftraject voor jongeren en jongvolwassenen die voor het eerst een cyberdelict hebben gepleegd. Het doel van Hack_Right is om recidive te voorkomen en het talent van jongeren verder te ontwikkelen binnen de kaders van de wet. Hack_Right bestaat op hoofdlijnen uit vier onderdelen: juridische en ethische grenzen, impactbesef, excuus en schadeherstel, digitaal talent en digitale weerbaarheid. Tijdens een Hack_Right traject voert de deelnemer ook één of meerdere opdrachten en werkzaamheden uit bij een bedrijf of organisatie dat gespecialiseerd is in ICT. Sinds 2022 zijn Reclassering Nederland, de Raad voor de Kinderbescherming en Halt eigenaar van de methodiek Hack_Right. Hack_Right heeft als effectieve aanpak veel potentie, maar wordt nog beperkt ingezet. De komende twee jaar is van belang dat Hack_Right, daar waar passend en van meerwaarde, vaker wordt ingezet, opdat de methodiek ook richting de toekomst behouden en geborgd kan worden.

Mijn Cyberrijbewijs

Burgers digitaal weerbaar maken is een essentieel onderdeel van de aanpak ter voorkoming van cybercrime en digitale criminaliteit. Hierop inzetten is nodig op alle niveaus. Voor kinderen uit groep 7 en 8 van het basisonderwijs heb ik met die reden Mijn Cyberrijbewijs gelanceerd. Mijn Cyberrijbewijs is mede gebaseerd op het onderzoek Online Ontspoord, waarin het Rathenau Instituut de aard en de omvang van online schadelijk en immoreel gedrag in kaart heeft gebracht. Mijn Cyberrijbewijs geeft leerlingen kennis en inzicht in de kenmerken van het internet waardoor online gedrag makkelijk ontspoort, en beoogt ze daarmee digitaal weerbaar te maken, waaronder tegen hacken.

Ondersteuning van slachtoffers

Net als andere strafbare feiten kan cybercrime een grote impact hebben op slachtoffers. Om herhaald slachtofferschap en de impact van criminaliteit te beperken biedt Slachtofferhulp Nederland (SHN) juridische, praktische en emotionele ondersteuning, ook specifiek voor slachtoffers van cybercrime. Daarnaast biedt het platform voor helpers en professionals van SHN informatie voor de omgeving van het slachtoffer over hoe zij het slachtoffer het beste kunnen ondersteunen. Dat is in het bijzonder van belang voor slachtoffers van cybercrime, omdat onderzoek uitwijst dat zij relatief vaak te maken krijgen met onbegrip vanuit hun omgeving en met herhaald slachtofferschap. Recent onderzoek onderstreept daarnaast het belang van lotgenotencontact voor slachtoffers.[29] SHN biedt daarom lotgenotengroepen voor slachtoffers aan.

[29] P. van de Ven, *The role of social support in the aftermath of victimization. Interpersonal aspects of coming to terms with a victimization experience* (diss. Tilburg), Zoetermeer: NBD Biblion 2022.

Een cybercrimedelict kan veel slachtoffers raken. Soms is de identiteit van slachtoffers niet of zeer moeilijk te achterhalen. Het is ook bij onbekende slachtoffers van belang dat de veroordeelde wordt aangesproken voor de schade die hij heeft veroorzaakt. Er wordt bekeken of in dit soort gevallen de veroordeelde vaker kan worden verplicht financieel bij te dragen aan een instelling die de belangen van slachtoffers van strafbare feiten behartigt. Dit is een element van de aanbevelingen uit het adviesrapport van de commissie Donner over het stelsel van compensatie van slachtoffers van strafbare feiten en zal worden betrokken bij de integrale inhoudelijke beleidsreactie op de voorstellen van het adviescollege.

Slachtoffernotificatie

De politie en het OM verkennen in samenwerking met het NCSC hoe het notificeren van slachtoffers uit strafrechtelijke informatie praktisch vorm kan krijgen. De mogelijkheden om overige slachtoffers en doelwitten te notificeren vanuit andere dan strafrechtelijke bron wordt in breder verband onderzocht. Deze verkenningen zijn uiterlijk 2025 afgerond.

Opsporen, vervolgen, verstoren

Verhoging ambitie Veiligheidsagenda

Voor de periode 2023–2026 is een stapsgewijze verhoging van de kwantitatieve ambitie van de opsporing (het aantal opsporingsonderzoeken naar cybercrime) voorzien. Bovendien wordt binnen die verhoging meer aandacht besteed aan de opsporing van criminele samenwerkingsverbanden.

Versterking capaciteit, kennis en kunde Openbaar Ministerie

Het OM breidt de komende jaren haar kennis en kunde uit, mogelijk gemaakt door de middelen uit het coalitieakkoord, en onderzoekt de mogelijkheid om middels een «fasttrack» zaken versneld af te doen.

Digitale aangifte

De politie maakt het vanaf 2023 voor meer cybercrimefenomenen mogelijk om online melding of aangifte te doen.

Doorontwikkelen niet-strafrechtelijke interventies

De politie en het OM zetten met publieke en private partners in op het ontwikkelen van niet-strafrechtelijke interventies te bestrijding van cybercrime, waaronder ransomware.

Internationaal verkrijgen van elektronisch bewijs

Nederland heeft op 12 mei 2022 het 2e protocol bij het Cybercrimeverdrag bij de Raad van Europa ondertekend, waarmee de mogelijkheden voor het verkrijgen van elektronisch bewijs uit het buitenland worden verbeterd. In EU-verband wordt daarnaast gesproken over de zogenaamde E-evidenceverordening en -richtlijn, gericht op het eenvoudiger kunnen vorderen van gegevens in het buitenland in het kader van opsporingsonderzoek. De gesprekken hierover bevinden zich in de triloogfase. In 2022 is in het kader van de Verenigde Naties gestart met onderhandelingen over een nieuw verdrag over cybercrime in VN-kader. Volgens de huidige plannen lopen de onderhandelingen door tot eind 2023.

Evaluatie Wet computercriminaliteit III

De Wet computercriminaliteit III bevat de bevoegdheid tot het op afstand binnendringen in geautomatiseerd werk, die de politie onder strikte voorwaarden en waarborgen kan inzetten om onder meer gegevens te verzamelen en/of ontoegankelijk te maken. Recentelijk heeft het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) de evaluatie van de bevoegdheid gepubliceerd.[30] Naast de wetsevaluatie brengt ook de Procureur-Generaal bij de Hoge Raad een rapport uit over de bevoegdheid. Deze documenten, alsook de verslagen van de Inspectie JenV hierover, zullen worden betrokken in de beleidsreactie op de evaluatie die de Kamer naar verwachting in het voorjaar van 2023 ontvangt.

Misbruik hostingproviders

Providers van hostingdiensten wordt gevraagd voldoende maateregelen te nemen om te zorgen dat zij niet, zonder het zelf te weten, criminaliteit faciliteren. De Gedragscode Abusebestrijding bevat dergelijke maatregelen. In Europees verband is ingezet op het versterken van de verantwoordelijkheid van hostingproviders, zodat ook minder welwillend providers verplicht worden maatregelen te nemen. Momenteel werkt het Ministerie van Justitie en Veiligheid aan Europese en Nederlandse ondersteuning van het project Cleannetworks.net, dat tot doel heeft hostingproviders actiever van (mogelijk) misbruik te informeren en een keurmerk te ontwikkelen. Bovendien wordt de gedragscode abusebestrijding benut bij de Rijksbrede inkoop van clouddiensten. Daarnaast zijn de politie en het OM actief, zowel door het informeren van providers als door het strafrechtelijk aanpakken van providers die moedwillig criminaliteit faciliteren.

Versterken informatiepositie

Onderzoek gedragsinterventies midden- en kleinbedrijf

In opdracht van het Ministerie van Justitie en Veiligheid voert het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) een onderzoek uit naar het realiseren van gedragsinterventies die ransomware in het midden- en kleinbedrijf moeten verminderen.

Alliantie Digitaal Samenleven

De Alliantie Digitaal Samenleven verkent doorlopend hoe burgers kunnen worden gestimuleerd om zich online veiliger te gedragen en hoe de bestaande hulpvraag en het hulpaanbod op gebied van online veiligheid beter op elkaar kunnen worden afgestemd.

Ontwikkeling intelligencefunctie en informatiebeelden politie

De intelligencefunctie van de politie ontwikkelt zich stapsgewijs richting een permanente positie op het gebied van zicht op, en inzicht in cybercrime en gedigitaliseerde criminaliteit, op basis van zowel intern als extern beschikbare gegevens, waaronder de inzichten en ervaringen uit de opsporingspraktijk. De politie gaat jaarlijks een veiligheidsbeeld opstellen voor cybercrime en gedigitaliseerde criminaliteit. In het beeld worden de belangrijkste criminele fenomenen en criminele modi operandi geschetst, en wordt een inschatting gegeven van het risico hiervan voor de samenleving.

[30] Kamerstuk 34 372 nr. 30.

Monitor Online Criminaliteit

Het CBS werkt aan een nieuwe Monitor Online Criminaliteit. Daarin wordt onderzoek gedaan naar diverse vormen van online criminaliteit. De eerste rapportage wordt in april 2023 verwacht. Het is de intentie de Monitor Online Criminaliteit elke twee jaar de laten uitvoeren. Aan de hand van de eerste rapportage wordt bezien hoe de nieuwe monitor vorm krijgt.

Monitor jeugdcriminaliteit

Het WODC voert periodiek zelfrapportage-onderzoek uit onder jeugdigen in het kader van de monitor jeugdcriminaliteit. Hiermee wordt niet alleen een beeld verkregen van de traditionele, maar ook van de online criminaliteit onder jeugdigen. Op 24 juni 2021 is uw Kamer geïnformeerd over de resultaten van 2020.

Onderzoek in- en doorstroom cyberdaders

Het onderzoek naar de in- en doorstroom van verdachten van online criminaliteit binnen de strafrechtketen zal meer zicht bieden op de actuele instroom en doorstroom van zaken en verdachten van online criminaliteit. Daarnaast is het doel meer inzicht te vergaren in knelpunten binnen de strafrechtketen, good practices en verbetermogelijkheden. Op basis van dit onderzoek kan worden bepaald welke verbeteringen kunnen worden doorgevoerd om de strafrechtpleging van verdachten van online criminaliteit te bevorderen. Het onderzoek is naar verwachting medio 2023 gereed.