Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2023–2024

26 643 **Informatie- en communicatietechnologie (ICT)**

29 911 **Bestrijding georganiseerde criminaliteit**

Nr. 1204 **BRIEF VAN DE MINISTER VAN JUSTITIE EN VEILIGHEID**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 28 juni 2024

De online en offline wereld raken steeds meer met elkaar verbonden. Dat is niet anders als het gaat om cybercriminaliteit. Het nut van een open internet, nieuwe applicaties of beveiligde online omgevingen wordt ook gezien en misbruikt door criminelen.[1] Cybercrime in enge zin draait om misdrijven die niet zonder tussenkomst van een computer of andere ICT-middelen gepleegd kunnen worden. Te denken valt aan een aanval met ransomware bij bedrijven of een phishing-mail gericht aan burgers. Om cybercrime goed te kunnen bestrijden zijn preventie, verstoring, opsporing en vervolging van belang en dienen de bevoegdheden daartoe goed geregeld te zijn. Met deze brief informeer ik u, mede namens de Minister voor Rechtsbescherming, over de voortgang van de integrale aanpak cybercrime en de bevoegdheden voor de opsporing in het digitale domein. Deze worden niet alleen ingezet voor de aanpak van cybercrime, maar voor allerlei (ook fysieke) strafbare feiten. Van vrijwel alle strafbare feiten is bewijs namelijk steeds vaker (alleen) in digitale vorm te vinden.

Nederland voert een actief beleid als het gaat om preventie, verstoring, opsporing en vervolging van cybercrime. We boeken in de aanpak steeds meer successen. Zo heeft recent de politie in nauwe samenwerking met 18 landen en verschillende veiligheidsdiensten zoals de FBI en Europol een onderzoek uitgevoerd naar een internationale phishing provider, genaamd Labhost. Er zijn in het buitenland beheerders aangehouden en in Nederland vonden er 15 interventies plaats, waaronder vijf aanhoudingen.[2] In februari 2024 hebben Europol, de Nederlandse politie en politiediensten uit tien landen met een grote verstoringsactie 34 servers

[1] De activiteiten van cybercriminelen kunnen ook ondersteunend zijn aan de meer klassieke vormen van criminaliteit, zoals drugshandel of het witwassen van crimineel geld. In dat geval spreken we van gedigitaliseerde criminaliteit.

[2] Grote provider van phishing pagina's dankzij internationale samenwerking uit de lucht | politie.nl

kst-26643-1204
ISSN 0921 - 7371
's-Gravenhage 2024

uit de lucht gehaald van de ransomware groepering LockBit. Hiermee zijn de criminele activiteiten van de groep ernstig verstoord en aangetast.[3]

Deze successen komen niet uit de lucht vallen. Al vanaf 2018 wordt door de Rijksoverheid aan de preventie, verstoring, opsporing en vervolging van cybercriminaliteit gewerkt binnen de integrale aanpak cybercrime. De online wereld ontwikkelt zich snel en het is belangrijk om deze nauwlettend en proactief te blijven volgen en de aanpak hier op aan te passen indien dat nodig blijkt.

In deze brief worden de laatste trends en ontwikkelingen hieromtrent benoemd. Specifiek zal er aandacht zijn voor de eerste editie van het Cybercrimebeeld Nederland (CCBN) van de politie en het OM.[4] Er wordt een overzicht gegeven van het beleid op de preventie van cybercriminaliteit met extra aandacht voor de weerbaarheid van burgers en het Midden- en Kleinbedrijf (MKB). In het kader van opsporen, verstoren en vervolgen zullen de afspraken uit de Veiligheidsagenda 2023–2026 aan bod komen met een reactie op de resultaten van het WODC onderzoek naar in- en doorstroom van online criminaliteit in de strafrechtketen, dat u op 12 maart jl. is aangeboden. Tenslotte zal er nader worden ingegaan op de Wet Computercriminaliteit III, ransomware en internationale ontwikkelingen.

In deze brief worden ook een toezegging en een tweetal moties afgedaan. Het gaat hier om de toezegging aan de leden Mutluer, Kuik en Rajkowski over het in kaart brengen van de preventie van jeugdcriminaliteit.[5] In de brief wordt verder ingegaan op de uitvoering van de motie van het lid Eerdmans over een gesprek met het OM over meer inzet tegen strafbare zaken op Telegram.[6] Ook bevat de brief de afdoening van de motie van het lid Mutluer om misdaden die online plaatsvinden als high-impact crime te benoemen en behandelen.[7] De ervaring en expertise die zijn opgedaan rond high-impact crimes worden meegenomen in de aanpak van cybercriminaliteit; diverse publieke en private initiatieven om de digitale weerbaarheid te vergroten worden in deze brief toegelicht.

Over de voortgang van de integrale aanpak online fraude ontvangt uw Kamer een separate brief.

Feiten en cijfers over cybercrime 2022–2023

In het afgelopen jaar (2023) was er een toename van cyberaanvallen gericht op data-diefstal en van illegale datahandel. Dat de illegale handel in persoonlijke data groot is bleek uit het internationale onderzoek «Operation Cookiemonster». Hierin heeft de politie samen met de FBI en Europol onderzoek gedaan naar een criminele handelssite, de Genesis market. Op deze website werden niet alleen accountgegevens verkocht maar ook kopieën van de unieke digitale vingerafdruk van personen. Daarmee kunnen hackers iemands digitale leven overnemen. Vermoedelijk waren er wereldwijd meer dan 2 miljoen slachtoffers, waaronder meer dan 50.000 in Nederland. De website is offline gehaald en verdachten in meerdere landen zijn gearresteerd, waaronder in

[3] Servers neergehaald van 's werelds grootste ransomware groepering | politie.nl
[4] «Cybercrimebeeld Nederland 2024», Cybercrimebeeld Nederland (politie.nl)
[5] Toezegging CD Cybercrime 30 maart 2023
[6] Kamerstukken II, 2023/24, 34 843, nr. 103
[7] Kamerstukken II, 2022/23, 29 911, nr. 403

Nederland. Inmiddels zijn in Nederland al verdachten tot gevangenisstraffen veroordeeld.[8]

In een eerste gecoördineerde, internationale operatie van opsporingsautoriteiten zijn sinds dinsdag 28 mei meerdere botnets ontmanteld die een sleutelrol hadden in de wereldwijde cybercriminaliteit. Het gaat hier om Operatie Endgame.[9] In Nederland leidde de operatie met gezamenlijke inspanningen van het Team High Tech Crime van de Eenheid Landelijke Opsporing en Interventies en diverse politie-eenheden, onder leiding van het Openbaar Ministerie, tot het offline halen van 33 servers in verschillende datacentra.

Voor deze operaties heeft de politie een speciale website «Check je hack» ingericht waar mensen kunnen nagaan of zij slachtoffer zijn geweest en zo ja, specifiek advies kunnen krijgen over hoe te handelen. Tot nu toe heeft de website een belangrijke rol gespeeld bij het bereiken van een zeer groot aantal slachtoffers, niet alleen in Nederland, maar wereldwijd. Om dergelijke operationele successen te behalen blijft samenwerking met de private sector essentieel.

In het *Cybercrimebeeld Nederland (CCBN 2024)* wordt een beeld geschetst van het cybercrimedomein vanuit het perspectief van het OM en politie.[10] Een belangrijke bevinding is dat cybercrime vele verschijningsvormen kent die constant in ontwikkeling zijn waardoor een standaard aanpak niet mogelijk is. Verder worden er een aantal trends gesignaleerd: het zorgwekkende aandeel van jonge cybercrimeverdachten, de opkomst van datadiefstal en illegale handel, vermenging met traditionele criminaliteit en de rol van Nederlandse datacenters en hostingbedrijven in de criminele infrastructuur. Ook is er zorg over de impact van cybercrime op slachtoffers en de massaliteit van het slachtofferschap, omdat met een druk op de knop vele slachtoffers tegelijk kunnen worden gemaakt. Voor de aanpak van cybercrime is een brede bestrijding nodig, waar zowel publieke als private partijen een belangrijke rol in spelen. Op een later moment zal, zoals verzocht door de Vaste Kamercommissie Justitie, een uitgebreidere beleidsreactie naar uw Kamer worden verzonden.

Ook in het *Cybersecuritybeeld Nederland 2023* (CSBN 2023) wordt gesignaleerd dat datadiefstal een belangrijk onderdeel vormt van het verdienmodel van cybercriminelen.[11] De veredeling van buitgemaakte informatie met andere informatie én de verkoop daarvan, zijn lucratief voor criminelen.
In de *Rapportage datalekken 2023* van de Autoriteit Persoonsgegevens (AP) wordt dit beeld verder onderbouwd met cijfers.[12] Zo heeft de AP in 2023 1309 datalekmeldingen ontvangen naar aanleiding van een cyberaanval, waarbij ongeveer 20 miljoen individuen als potentiële slachtoffers zijn getroffen. Het aantal meldingen bij de AP over datalekken als gevolg van cyberaanvallen, zoals hacking, phishing of malware incidenten, is gedaald ten opzichte van 2022. De meeste meldingen werden gedaan door de sectoren openbaar bestuur, gezondheidszorg en industrie.

---

[8] Enkele voorbeelden hiervan zijn: RB Rotterdam, 6 februari 2024, ECLI:NL:RBROT:2024:699; RB Den Haag, 9 september 2023, ECLI:NL:RBDHA:2023:14140; RB Midden-Nederland, 12 januari 2024, ECLI:NL:RBMNE:2024:75.

[9] Meerdere botnets ontmanteld in grootste internationale operatie tegen ransomware ooit | politie.nl

[10] «Cybercrimebeeld Nederland 2024», Cybercrimebeeld Nederland (politie.nl)

[11] Cybersecuritybeeld Nederland 2023, NCTV. Cybersecuritybeeld Nederland 2023 | Publicatie | Nationaal Coördinator Terrorismebestrijding en Veiligheid (nctv.nl) (25 april 2024).

[12] Rapportage datalekken 2023, Autoriteit Persoonsgegevens april 2024. Rapportage datalekken 2023.pdf (autoriteitpersoonsgegevens.nl)

In het *WODC onderzoek «Ransomware-aanvallen op instellingen en bedrijven in Nederland»* uit 2023 komt geen eenduidig beeld naar voren over de kenmerken van ransomware-aanvallen, type slachtoffers, hoe vaak ze voorkomen en de impact die ze hebben.[13] Volgens rapportages van verzekeraars (op basis van enquêtes) is 26% van de Nederlandse bedrijven in 2022 getroffen door ransomware. In 2021 en 2022 zijn er respectievelijk 107 en 110 aangiftes van ransomware binnengekomen bij de politie. De politie vermoedt dat slechts 2% tot 4% van de slachtoffers aangifte doet. Dat dit percentage laag is komt ook naar voren uit de *CBS Cybersecuritymonitor* waar slechts 13% van de bedrijven aangeeft hulp te hebben gezocht bij de politie.[14]

Europol geeft in het *Internet Organised Crime Threat Assessment 2023 (IOCTA 2023)* aan dat online cybercrime diensten alomtegenwoordig zijn en dat men zich binnen criminele netwerken steeds meer gaat specialiseren op een specifiek aspect van cybercrime.[15] Zo verkopen zogenaamde *Initial Access Brokers* toegang tot bedrijfsnetwerken aan cybercriminelen die deze toegang weer benutten voor phishing activiteiten of grootschalige online fraude. Ook Europol signaleert een toename van cybercriminaliteit voor datadiefstal en datahandel; online criminele markten staan vol met aanbiedingen van gestolen identiteitsgegevens of informatie om toegang tot systemen te krijgen. Om met elkaar te communiceren en kennis te delen wordt veelal gebruikt gemaakt van Telegram en dark web forums; ook jongeren gebruiken dit voor hun eerste stappen op het criminele pad. Transacties worden bijna geheel exclusief gedaan door middel van cryptovaluta. Criminelen maken vervolgens gebruik van verschillende verhullende technieken om de financiële transacties zo veel mogelijk anoniem te maken voordat ze de cryptovaluta laten omzetten in normale valuta.

Uit de *Veiligheidsmonitor van het Centraal Bureau voor de Statistiek 2023* volgt dat in 2023 16 procent van de bevolking slachtoffer is geweest van een of meer online delicten of incidenten.[16] De monitor ziet op een breder spectrum dan dat van cybercrime in enge zin alleen. Van online oplichting en fraude werden zij het vaakst slachtoffer (9 procent), gevolgd door hacken (6 procent), online bedreiging en intimidatie (3 procent) en overige online delicten (minder dan 1 procent). Het slachtofferschap van online criminaliteit is licht gedaald ten opzichte van de Veiligheidsmonitor van 2021.

Preventie van cybercrime

De inzet van preventie tegen cybercrime 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 ontmoedigen en recidive te beperken, en systemen en producten waar burgers en bedrijven gebruik van maken veiliger maken (situationele preventie).

---

[13] Dialogic, Blom, T., Sahebali, W., et al. (2023). Ransomware-aanvallen op instelllingen en bedrijven in Nederland. WODC, Den Haag.

[14] https://www.cbs.nl/nl-nl/longread/rapportages/2023/cybersecuritymonitor-2022?pk_campaign=social_share (30 april 2024).

[15] Europol (2023), Internet Organised Crime Threat Assessment (IOCTA) 2023, Publications Office of the European Union, Luxembourg.

[16] CBS Veiligheidsmonitor 2023, Veiligheidsmonitor 2023 | CBS

Vergroten basisweerbaarheid burgers

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. Het Ministerie van Justitie en Veiligheid heeft hiervoor middelen begroot oplopend van € 0,6 miljoen euro in 2023 naar € 2 miljoen structureel vanaf 2027.

Campagnes «Laat je niet interneppen» en «Dubbel beveiligd is dubbel zo veilig»

In 2023 is de campagne «*Laat je niet interneppen*» in samenwerking tussen de Ministeries van JenV en BZK gestart om mensen te waarschuwen voor het gebruik van social engineering door online criminelen.[17] Social engineering omvat de technieken die criminelen inzetten om door middel van psychologische manipulatie mensen en bedrijven te verleiden om toegang tot systemen te krijgen, malware te installeren of in het bezit te komen van persoonlijke gegevens van slachtoffers. Met die persoonlijke gegevens worden vervolgens criminele activiteiten verricht. Naast bewustmaking worden mensen en bedrijven ook voorzien van handelingsperspectieven om slachtofferschap te voorkomen of te beperken door een einde aan de situatie te maken. Later dit jaar zal deze campagne weer van start gaan. In februari 2024 heeft het Ministerie van JenV de campagne «*Dubbel beveiligd, is dubbel zo veilig*» gelanceerd, gericht op het beveiligen van internetaccounts door het gebruik van tweefactorauthenticatie.[18]

Voor beide campagnes is er een toolkit beschikbaar gesteld die kan worden ingezet om hieraan bij te dragen. Op 5 juni jl. hebben de Ministeries van JenV en BZK de inspiratiedag «Samen tegen Cybercrime» georganiseerd om de noodzaak en het belang van cybercrimepreventie te benadrukken en de samenwerking tussen publieke en private partijen te versterken.

Campagne Doe Je Updates

Bijna driekwart van de Nederlanders heeft één of meerdere slimme apparaten in huis. Rond de 80% van deze mensen is zich ervan bewust dat deze apparaten gehackt kunnen worden en dat ze voorzien moeten worden van updates om hacken te voorkomen. Toch stelt meer dan de helft van de mensen updates uit, vergeet ze uit te voeren of heeft daar geen tijd voor of zin in, bijvoorbeeld omdat zij het gedoe vinden. Daarmee zijn Nederlanders kwetsbaar voor internetcriminelen. Het Ministerie van Economische Zaken en Klimaat richt zich daarom sinds 2019 met campagnes op consumenten die slimme apparaten (verbonden met Internet) kopen of in bezit hebben. In juni 2024 zal de zesde editie van de campagne *Doe je updates* starten.

Tool Cyberweerbaarheid

Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties heeft in samenwerking met het Centrum voor Criminaliteitspreventie en Veiligheid

[17] Laat je niet interneppen (veiliginternetten.nl)
[18] Dubbel beveiligd is dubbel zo veilig (veiliginternetten.nl)

(CCV) de Tool Cyberweerbaarheid ontwikkeld voor baliemedewerkers van maatschappelijke en sociale instellingen, waaronder bibliotheken. Dit is een help-de-helper tool waarmee vragen en problemen van burgers op het gebied van cyberveiligheid beantwoord en opgelost kunnen worden.

Vergroten basisweerbaarheid overheid en ondernemers

Met de Nederlandse Cybersecurity Strategie (NLCS) 2022–2028 streeft het kabinet naar een digitaal veilig Nederland en werkt het aan toekomst waarin de scheefgroei tussen digitale dreiging en digitale weerbaarheid zo klein mogelijk is.[19] De Ministeries van Justitie en Veiligheid, Binnenlandse Zaken en Koninkrijksrelaties, en Economische Zaken en Klimaat werken bovendien nauw samen aan het vormgeven van communicatie richting andere overheden, burgers en bedrijven. Momenteel wordt vanuit de Rijksoverheid ook een aantal kennisproducten ontwikkeld om overheidsorganisaties te helpen weerbaar te worden tegen een eventuele ransomware-aanval.[20]

Basisweerbaarheid midden- en kleinbedrijf

De preventie van cybercrime voor het midden- en kleinbedrijf is een geprioriteerd thema binnen het Actieprogramma Veilig Ondernemen 2023–2026 van het Nationaal Platform Criminaliteitsbeheersing. Doel van het Nationaal Platform Criminaliteitsbeheersing is om publiek-private samenwerking te stimuleren op nationaal, regionaal en lokaal niveau. Ten aanzien van de preventie van cybercrime in het bedrijfsleven werken publieke en private partijen samen om het Nederlandse ondernemersklimaat digitaal veiliger te maken en de ondernemer hulp van een betrouwbare partner «dicht bij huis» te bieden. Het Digital Trust Center voorziet bedrijven van betrouwbare en onafhankelijke informatie over digitale kwetsbaarheden en van concreet handelingsadvies, en stimuleert cybersecurity samenwerkingsverbanden tussen bedrijven. Daarnaast wordt vanuit het platform Samen Digitaal Veilig gewerkt aan het verhogen van kennis en bewustwording van ondernemers via de brancheorganisatie.

City Deal Lokale Weerbaarheid Cybercrime

De City Deal Lokale Weerbaarheid Cybercrime zet zich in om gemeenten in Nederland te ondersteunen bij het versterken van de cyberweerbaarheid van bedrijven en kwetsbare inwoners. De afgelopen jaren zijn ruim dertig City Deal-projecten tot stand gekomen die op proces geëvalueerd zijn door drie HBO-lectoraten. Deze evaluaties worden gebruikt om te bepalen welke projecten landelijk verspreid worden. Hierin wordt synergie gezocht met landelijke programma's, waaronder *Preventie met gezag*.[21] Naast het ontwikkelen van nieuwe innovatieve projecten voor de jeugd, het midden- en kleinbedrijf, senioren en laaggeletterden wordt in 2024 en 2025 nadrukkelijk ingezet op het verspreiden van succesvolle City Deal-projecten. Platforms Veilig Ondernemen verspreiden kansrijke interventies richting het midden- en kleinbedrijf en formeel en informeel georganiseerde regionale samenwerkingsverbanden rondom openbare orde en veiligheid ontvangen middelen om gemeenten aan te jagen projecten gericht op kwetsbare burgers te implementeren. De City Deal loopt eind 2025 af. Daarom wordt nu gekeken hoe de kansrijke interventies vanaf 2026 en verder geborgd kunnen worden.

---

[19] Nederlandse Cybersecuritystrategie 2022–2028 (overheid.nl)
[20] Kamerstukken II 2023/24, 26 643, nr. 1149.
[21] Kamerstukken II 2023/24, 28 741, nr. 113

Alert Online

In de cybersecurity-maand oktober wordt via het publiek-private partnernetwerk van Alert Online, een initiatief van het Ministerie van Economische Zaken en Klimaat, aandacht gevraagd voor cybersecurity en cybercrimepreventie. De partners van Alert Online organiseren deze maand onder de vlag van Alert Online evenementen, trainingen of oefeningen voor hun medewerkers, relaties en/of klanten om zo cybersecurity onder de aandacht te brengen. Dit moet bijdragen aan het bewustzijn dat leidt tot grotere digitale weerbaarheid.

Daderpreventie jongeren

Tijdens het Commissiedebat Cybercrime in 2023 (Kamerstuk 26 643, nr. 1015) heb ik aan de leden Mutluer, Kuik en Rajkowski de toezegging gedaan om de interventies om te voorkomen dat jongeren het criminele cybercrime pad op gaan te benoemen. Deze licht ik hieronder graag nader toe.

Het is van belang dat onze jongeren, met name zij die ICT-vaardig zijn, hun vaardigheden op een positieve manier inzetten en niet actief worden als cybercrimineel. Vanuit de City Deal Lokale Weerbaarheid Cybercrime zijn de afgelopen jaren daarom verschillende projecten ontwikkeld om jongeren op het rechte pad te houden. Drie pilots die zich specifiek richten op daderpreventie onder jongeren zijn in april 2024 van start gegaan.

Vanuit de politie speelt het *Cyber Offender Prevention Squad* (COPS) team een belangrijke rol in het ontwikkelen van interventies op het gebied van daderpreventie. *HackShield*, een game waarin jongeren bewust worden gemaakt over online dader- en slachtofferschap, en *Mijn Cyberrijbewijs*, een lesprogramma voor groep 7 en 8 van het primair onderwijs, dragen hier aan bij. Ook wordt de interventie *Re_B00TCMP* sinds 2023 breed landelijk ingezet. Middels deze interventie worden ICT-vaardige jongeren met risico om de criminaliteit in te gaan voorgelicht over de gevolgen van daderschap en wordt hen vanuit zowel publieke als private organisaties carrièreperspectief aangeboden.

Leerlingen hebben vaak geen idee wat er online precies strafbaar is. Om leerlingen meer bewust te maken over wat ongeoorloofd handelen online is heeft de politie de gratis mobiele game *Framed* ontwikkeld. Framed is een mobiele game die leerlingen op hun eigen smartphone spelen. De mysterieuze leerling Anne daagt ze via sociale media uit tot het maken van moeilijke keuzes. Elke keuze levert een ander pad op in het spel met eigen consequenties. Zo leren ze op een speelse manier, vanuit hun eigen leefwereld dat online gedrag ernstige gevolgen kan hebben. Achteraf krijgt iedereen een fictief «strafblad» en worden de ervaringen besproken zodat de bewustwording beklijft en de nieuwe kennis blijft hangen. De campagne Framed is het vierde en laatste (school)jaar ingegaan. Meer dan de helft van alle middelbare scholen heeft zich aangemeld voor het gratis lespakket en meer dan 158.000 leerlingen hebben Framed gespeeld.

Hack_Right is een door de politie en het OM ontwikkelde keteninterventie voor jongeren die voor een eerste cyberdelict worden vervolgd. In deze interventie werken private en publieke organisaties samen om recidive te voorkomen en het cybertalent van jongeren verder te ontwikkelen binnen de kaders van de wet. Gedurende het programma doorloopt de jongere modules die gaan over online grenzen van wat wel of niet mag, slachtoffers, impactbesef en herstel. Ook wordt de jongere geholpen met het verkennen en ontwikkelen van zijn of haar digitale talenten op een positieve manier. Bij minderjarigen worden de ouders of verzorgers

betrokken. Gedurende Hack_Right krijgt de jongere twee begeleiders: één begeleider vanuit Halt, de Raad voor de Kinderbescherming of Reclassering Nederland en één begeleider vanuit de private sector, veelal een cybersecurity bedrijf. Hack_Right wordt tot en met 2026 gesubsidieerd door het Ministerie van Justitie en Veiligheid. Aan het eind van de subsidieperiode wordt bekeken of Hack_Right voldoende instroom heeft om definitief te worden ingebed in het interventiepalet van de uitvoerders.

Opsporen, verstoren en vervolgen van cybercrime

Veiligheidsagenda

Cybercrime is reeds lange tijd een prioriteit in de Veiligheidsagenda. De huidige Veiligheidsagenda 2023–2026 laat een stijgende ambitie zien voor het aantal opsporingsonderzoeken.[22] Voor de operationele afstemming van fenomeenonderzoeken naar cybercrime is het Landelijk Operationeel Cybercrime Overleg (LOCO) actief, waarin de landelijke en regionale eenheden en parketten van de politie en het Openbaar Ministerie deelnemen. Hier worden gezamenlijke prioriteiten bepaald, zaken verdeeld en wordt kennis en ervaring uitgewisseld.

Fig. 1 Afspraken Veiligheidsagenda Cybercrime

Afspraken:

	2023	2024	2025	2026
Aantal verdachten van 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

In de eerste tussenstand van de afspraken van de Veiligheidsagenda komt naar voren dat de doelstelling omtrent het aantal verdachten dat ingezonden werd naar het Openbaar Ministerie ruim is gehaald. Daar staat tegenover dat het aantal fenomeenonderzoeken en high tech crime onderzoeken niet volledig is gehaald.[23]

Fig. 2 Resultaten Veiligheidsagenda cybercrime (realisatie 2022, norm 2023 en realisatie 2023)

Cybercrime				
Aantal verdachten cybercrime regulier	356	310	336	108%
- Waarvan alternatieve of aanvullende interventies	17	78	36	
- Waarvan criminele samenwerkingsverbanden	60	31	50	
Aantal fenomeenonderzoeken	49	41	36	88%
- Waarvan alternatieve of aanvullende interventies	9	20	14	
Aantal high tech crime onderzoeken	10	20	14	70%
Totaal aantal onderzoeken Cybercrime	*415*	*371*	*389*	*105%*

[22] Kamerstukken II 2022–2023, 28 684, nr. 717
[23] Jaarverslag Ministerie van Justitie en Veiligheid 2023, Kamerstuk 36 560 VI, Nr. 1

Beleidsreactie onderzoek in- en doorstroom online criminaliteit in de strafrechtketen

Onlangs is het rapport van het onderzoek over in- en doorstroom van online criminaliteit, waaronder gedigitaliseerde criminaliteit, in de strafrechtketen voltooid en daarna op 12 maart jl. aan de Tweede Kamer gestuurd.[24] Het betreft een uitgebreid rapport op basis van een vernieuwende onderzoeksmethode. Het biedt daarom niet alleen waardevolle inzichten om ons beleid te toetsen en te versterken, maar het kan tevens een inspiratie zijn voor komende onderzoeken. De bevindingen uit dit rapport zijn tot stand gekomen op basis van gegevens uit de periode van 2018 tot en met 2020. De politie en het OM hebben de afgelopen jaren niet stilgezeten en er zijn sinds 2020 forse verbeterstappen gemaakt voor zowel cybercrime als gedigitaliseerde criminaliteit. Dat betekent echter niet dat onze aandacht kan verslappen. Cybercrime en gedigitaliseerde criminaliteit maken veel slachtoffers en de aanpak ervan blijft vaak lastig. Het rapport noemt onder meer de complexiteit van opsporingsonderzoek en het internationale karakter als oorzaken daarvoor. Hieronder wordt meer in detail een reactie gegeven op de conclusies en aanbevelingen in het rapport.

Verbeteringen registratie en expertise

Een deel van de conclusies betreft het verbeteren van registraties en aangiften. De politie is inmiddels enkele jaren bezig met het mogelijk maken van het digitaal doen van aangifte; zo is het inmiddels mogelijk om aangifte te doen van ransomware (voor natuurlijke personen) en diverse vormen van online fraude. Zoals afgesproken in de Veiligheidsagenda 2023–2026 blijft de politie werken aan het mogelijk maken van het digitaal aangifte doen voor meer delicten. Dat maakt aangifte doen laagdrempeliger en vermindert de tijd die het kost voor het slachtoffer. Het aantal en type aangiften verrijken ook het veiligheidsbeeld en geven een beter zicht op de omvang van de problematiek. De digitale aangiftemogelijkheden ondersteunen ook de intake- en servicemedewerkers bij de politie als zij een aangifte opnemen.

Daarnaast hebben de politie en het Openbaar Ministerie de afgelopen jaren stevig ingezet op het vergroten van kennis en kunde van medewerkers door het aanbieden van aanvullende cursussen en onderdelen in de basisopleidingen. Er wordt breed geïnvesteerd in de digitale vaardigheid van politiemedewerkers in alle politie onderdelen, waaronder de opsporing en de gebied gebonden politie. Ook de in 2019 opgerichte cybercrimeteams in de regionale eenheden hebben de expertise vergroot. Medewerkers van deze teams ondersteunen in voorkomende gevallen bij complexe aangiften.

Prioriteitstelling en internationale samenwerking

Het aantal door de politie geregistreerde misdrijven van cybercrime en gedigitaliseerde criminaliteit ligt fors lager dan het slachtofferschap dat naar voren komt uit de Veiligheidsmonitor. Een volledig sluitende verklaring daarvoor is niet te geven. Wel is duidelijk dat online criminaliteit veel vaker voorkomt dan dat het bij de politie wordt gemeld. Het rapport meldt bovendien dat er door de politie vaak geen prioriteit aan online criminaliteit wordt gegeven, onder meer omdat deze zaken vaak als complex zouden worden ervaren, er weinig opsporingsindicaties zijn of doordat een regionale eenheid zelf een onvolledig beeld heeft. Deze

[24] https://repository.wodc.nl/handle/20.500.12832/3346; Kamerstuk 26 643, nr. 1144 d.d. 12 maart 2024

uitdagingen zijn eerder al onderkend en zijn een belangrijke reden om via de Veiligheidsagenda deze zaken als prioriteit voor de opsporing vast te stellen.

De complexiteit van zaken is een bekend aandachtspunt bij online criminaliteit. Door de grenzeloosheid van het internet zijn dader, slachtoffer en digitaal bewijs vaak niet in hetzelfde land aanwezig, wat internationale samenwerking en de daarbij behorende tijdrovende procedures nodig maakt. Bovendien maken de vluchtigheid van digitaal bewijs en gemakkelijk toegankelijke anonimiseringstechnieken het lastig voor de opsporing om daders op te sporen.

De afgelopen jaren is hard gewerkt om deze uitdagingen aan te pakken. Het Team High Tech Crime van de Eenheid Landelijke Opsporing en Interventies richt zich op de meest complexe, high tech en/of internationale opsporingsonderzoeken. Daarnaast zijn voor cybercrime in 2019 gespecialiseerde regionale teams ingericht, zodat meer capaciteit beschikbaar is, de kennis binnen de regio kan worden gebundeld en ook op regionaal niveau eenheidsoverstijgende fenomeenonderzoeken op het gebied van cybercrime kunnen worden uitgevoerd. Daarbij kunnen de inzichten en ervaringen die het landelijke Team High Tech Crime opdoet aan de regio's worden verspreid. De teams werken met elkaar samen als landelijk netwerk. Het Openbaar Ministerie beschikt bij het Landelijk Parket en bij de regionale parketten over in cybercrime gespecialiseerde medewerkers, zoals Officieren van Justitie, beleidsmedewerkers, secretarissen en adviseurs digitale opsporing. Er is bovendien sprake van een hechte internationale samenwerking, onder meer met ondersteuning van het *European Cybercrime Centre* en de *Joint Cybercrime Action Task Force* van Europol en het *European Judicial Cybercrime Network* bij Eurojust.

Publiek-private samenwerking

Naast internationale samenwerking wijst het rapport op het belang van publiek-private samenwerking. De digitale wereld is grotendeels in handen van private partijen en zij hebben vaak diverse mogelijkheden om de veiligheid te bevorderen en de opsporing te ondersteunen. Publiek private samenwerking is sinds de start van de aanpak van cybercrime een onderdeel van de strategie en de afgelopen jaren heeft de politie de publiek-private samenwerking steeds verder geïntensiveerd zowel op landelijk als regionaal niveau. Een goed voorbeeld daarvan is het project NoMoreLeaks, een project waarmee de politie data kan delen met private partijen om misbruik met inloggegevens te voorkómen. Een ander voorbeeld is het project Melissa dat hieronder verder wordt toegelicht.

Project Melissa (publiek-privaat samenwerkingsverband)

Project Melissa is het samenwerkingsverband tussen publieke (Politie, OM en Nationaal Cyber Security Centrum) en private cybersecurity partijen om ransomware te bestrijden. De partijen wisselen op structurele basis informatie met elkaar uit en delen actuele ontwikkelingen. In het convenant tussen de samenwerkende partijen *dat in oktober 2023 is getekend* zijn juridische, organisatorische en technische afspraken vastgelegd. De samenwerking is in 2021 gestart en was behulpzaam bij verschillende succesvolle verstoringsoperaties. Recent heeft het samenwerkingsverband van project Melissa mogelijk duizenden ransomwareslachtoffers weten te voorkomen door een gezamenlijke analyse over

ransomwaregroep Cactus.[25] Daarnaast zijn er op grond van gezamenlijke inzichten White papers gepubliceerd, bijvoorbeeld over datadiefstal. De intentie is om deze publiek-private samenwerking verder uit te bouwen.

Wet Computercriminaliteit III

In 2022–2023 is de hackbevoegdheid uit de Wet Computercriminaliteit III geëvalueerd door het WODC. De evaluatie ziet op de eerste twee jaar van inwerkingtreding van deze bevoegdheid. De evaluatie van de andere elementen uit die wet loopt nog. Over de hackbevoegdheid zijn meerdere rapporten gepubliceerd; hierover heb ik u in december vorig jaar mijn beleidsreactie gestuurd[26].

Op 24 mei 2024 heeft de Inspectie J&V mij het verslag van het toezicht op de wettelijke hackbevoegdheid politie 2023 toegestuurd. Dit verslag gaat als bijlage bij deze brief. De Inspectie heeft haar toezicht in 2023, zoals ook aangekondigd in de vorige rapportage, gericht op de inrichting en implementatie van het kwaliteitssysteem. Het toezicht vindt doorlopend plaats, ook gedurende de transitie waarin een kwaliteitssysteem wordt ingevoerd (toetsing *ex nunc*). Hierbij is sprake van een constructieve operationele dialoog tussen de Inspectie, de politie en het OM, die in 2024 ook op strategisch niveau zal worden gevoerd. Hierin kan de Inspectie als toezichthouder gedurende het proces haar bevindingen en gesignaleerde risico's tijdig delen. De politie is hierdoor in staat om deze bevindingen direct toe te passen en niet pas nadat er een rapportage is verschenen. De Inspectie ziet kwaliteitszorg als basis voor het uitvoeren van de hackbevoegdheid door de politie en voor het eigen inspectietoezicht. Na de volledige invoering van het kwaliteitssysteem kan de Inspectie daadwerkelijke inhoud geven aan het systeemtoezicht dat van meet af aan de bedoeling is geweest. De Inspectie stelt vast dat op basis van verricht werk in 2023 en in het begin van 2024 een volledig procesplan is opgesteld voor de invoering van het kwaliteitssysteem dat voorziet in een procesmatige en gestructureerde aanpak. Ook constateert de Inspectie dat de politieleiding achter dit plan en een kwaliteitssysteem staat en dat in een intentieverklaring heeft uitgesproken. Voorts ziet de inspectie dat het inrichten van het kwaliteitssysteem geen eenmalige actie is voor de politie; er is voorzien in een doorlopende ontwikkeling van het systeem. De inspectie concludeert dat hiermee een goede basis is gelegd waarmee uiteindelijk een effectief kwaliteitssysteem kan worden gerealiseerd. De Inspectie voorziet evenwel dat gebrek aan capaciteit een knelpunt kan worden bij de uitvoering van het verbeterplan.

Ik ben blij met de bevindingen van de Inspectie en de positieve toon over zowel de inhoud als het verwachte effect van ingezette acties bij de politie. Op basis hiervan heb ik goede verwachtingen dat een adequaat kwaliteitssysteem bij de politie wordt ingevoerd en dat de Inspectie in de toekomst op basis daarvan de stap kan zetten van nalevingstoezicht naar systeemtoezicht. De politie roep ik op het gevoel van urgentie voor deze beweging vast te houden en ondanks de druk van het primaire proces voortvarend de invoering van het kwaliteitssysteem ter hand te nemen.

Overleg met OM inzake de inzet tegen strafbare zaken op Telegram

Na het Commissiedebat seksueel geweld en kindermisbruik op 6 maart jl. (Kamerstuk 34 843, nr. 110) is een motie van het lid Eerdmans aangenomen waarin ik ben opgeroepen om in mijn regulier overleg met het OM

[25] Persbericht: samenwerkingsverband melissa vindt diverse nederlandse slachtoffers van ransomwaregroepering cactus – Cyberveilig Nederland
[26] Tweede Kamer vergaderjaar 2023–2024, 34 372, nr. 31

te spreken over de inzet tegen strafbare zaken op Telegram.[27] Ik heb het onderwerp besproken tijdens mijn reguliere overlegvergadering met het College van procureurs-generaal. Duidelijk is dat er een onderscheid gemaakt dient te worden tussen openbare en besloten Telegram groepen. In het verleden is meermalen getracht om Telegram te bewegen tot het sluiten van openbare kanalen. Dit zou een eenvoudige en laagdrempelige manier zijn om strafbare gedragingen te stoppen en verschillende rechtsbelangen te beschermen. Telegram blijkt in de praktijk helaas onvoldoende mee te werken. Op dit moment wordt dit nader geëvalueerd, deels in Europees verband.

Internationale trajecten

Counter Ransomware Initiatief

Het Counter Ransomware Initiatief is een samenwerkingsverband van meer dan 50 landen en de EU om kennis en ervaring over de bestrijding van ransomware uit te wisselen. Thema's zijn informatie-uitwisseling, cyberverzekeringen, losgeldbetalingen en de rol die crypto-valuta speelt bij cybercriminaliteit. Tijdens de jaarlijkse bijeenkomst in november 2023 is in een gezamenlijke verklaring een krachtig signaal afgegeven tegen de betaling van losgeld door overheidsdiensten. Nederland neemt actief aan het initiatief en de daaronder ingerichte werkgroepen deel.

Cybersancties

In EU verband bestaat al enkele jaren de mogelijk om entiteiten of personen onder het EU-cybersanctieregime een sanctie op te leggen. Deze sancties kunnen bestaan uit een inreisverbod en/of het bevriezen van tegoeden. Door het OM en de politie wordt onderzocht of EU cybersancties als aanvullende verstoringsmogelijkheid kunnen worden ingezet in de aanpak van cybercriminelen. Voor het instellen van EU-sancties is steun van alle EU-lidstaten een voorwaarde.

VN Cybercrime verdrag onderhandelingen

Momenteel wordt in het kader van de Verenigde Naties onderhandeld over een mogelijk nieuw verdrag op het gebied van cybercrime. Met dit verdrag zou de internationale samenwerking op het gebied van preventie, verstoring, opsporing en vervolging van cybercrime verbeterd moeten worden. Er zijn vier onderwerpen die met name van belang zijn in de onderhandelingen: de strafbaarstellingen, (samenwerking op) interceptie, samenwerking op de uitwisseling van elektronisch bewijs, en mensenrechten en fundamentele vrijheden (inclusief gegevensbescherming). De inzet van Nederland en de Europese Unie is er vooral op gericht dat het verdrag een gebalanceerd geheel vormt; het conceptverdrag bevat opsporingsbevoegdheden rondom interceptie en daar dienen voldoende waarborgen tegenover te staan daar waar het mensenrechten betreft. Er wordt geprobeerd zoveel mogelijk aan te sluiten bij de bepalingen uit het reeds bestaande Verdrag van Budapest van de Raad van Europa. De onderhandelingen bewegen zich momenteel richting de eindfase.

Toegang tot elektronisch bewijs: e-evidence in de EU

Nederland heeft een constructieve rol gespeeld bij de totstandkoming van de E-evidenceverordening van de EU en het 2_e protocol bij het Cybercrimeverdrag van de Raad van Europa. Beide nieuwe internationale instrumenten beogen de internationale samenwerking in opsporingson-

[27] Kamerstukken II, 2023/24, 34 843, nr. 103

derzoeken sneller en efficiënter te maken, onder meer door snellere procedures voor het verkrijgen van digitaal bewijs uit andere landen.

De kern van regelingen is dat waar nu sprake is van een via Nederlandse justitiële coördinatiecentra (Landelijk internationaal rechtshulpcentrum LIRC) gecentraliseerde werkwijze, wordt overgegaan naar een situatie waarin buitenlandse justitiële autoriteiten rechtstreeks aankloppen bij de (private) dienstaanbieder in Nederland en omgekeerd. Momenteel wordt de implementatie van de regelingen voorbereid. Daarnaast worden aanbieders van digitale diensten verplicht zich met een vestiging of vertegenwoordiging in één van de EU lidstaten aan te melden, en zich zodanig in te richten en te organiseren dat aan de bevelen gehoor kan worden gegeven. Overigens blijft het ook mogelijk bestaande rechtshulp instrumenten zoals het Europees opsporingsbevel (EOB) of multilaterale en bilaterale verdragen te blijven gebruiken.

Toegang tot elektronisch bewijs: EU-VS e-evidence onderhandelingen

In oktober 2023 zijn de onderhandelingen tussen de EU en de VS over grensoverschrijdende toegang tot elektronisch bewijs voor justitiële samenwerking in strafzaken weer opgestart. Met de Europese eEvidence regels kunnen Europese justitiële autoriteiten al rechtstreeks gegevens vorderen van dienstenaanbieders die diensten leveren aan personen in de EU, ook al is de hoofdvestiging van de betrokken dienstaanbieder in de VS. De toegevoegde waarde van een overeenkomst tussen de EU en de VS is hoofdzakelijk om eventuele rechtsconflicten op te heffen. De Europese Commissie voert de onderhandelingen in nauw overleg met de Raad. Het streven is om voor het einde van 2024 tot een overeenkomst te komen.

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