Ministerie van Justitie en Veiligheid

Jaarbericht

2023

Integrale aanpak

online fraude

Online fraude is een groot maatschappelijk probleem dat jaarlijks miljoenen Nederlanders raakt en elk jaar meer dan 100.000 mensen slachtoffer maakt. Overheid en bedrijfsleven werken samen aan het verminderen van het aantal slachtoffers en de schade door online fraude. Dat doen ze in de integrale aanpak online fraude op terreinen als kennisagenda, gegevensdeling, interventies, opvolging door politie en openbaar ministerie, weerbaarheid, preventie en hulp aan slachtoffers. In dit eerste jaarbericht blikken de partners in de integrale aanpak terug op 2023.

Met elkaar verder komen

Lisette de Bie (directeur Rechtshandhaving en Criminaliteitsbestrijding) en Jan Dobbelaar (afdelingshoofd Fraude en Bijzonder Strafrecht) zijn namens JenV de opdrachtgevers van het programma, dat in 2023 op stoom kwam. Met hen blikken we terug op de afgelopen periode en kijken we alvast wat vooruit.

Van jong tot oud, van burgers tot bedrijven en overheden: iedereen kan slachtoffer worden van online fraude. Om het aantal slachtoffers snel omlaag te brengen heeft de Minister van Justitie in 2022 het startschot gegeven voor de Integrale Aanpak Online Fraude, een samenwerkingsverband van publieke en private organisaties. Wil je online fraude effectief aanpakken, dan moet je dat samen doen, stelt Lisette: “Banken, verzekeraars, telecombedrijven, webwinkels; ze zijn allemaal onderdeel van de fraudeketen en ze zijn allemaal nodig om grip te krijgen op online fraude. Je moet met elkaar verder willen komen.”

Elkaar leren kennen en begrijpen

De eerste stap naar een succesvolle samenwerking is volgens haar dat je elkaar leert kennen en begrijpen. Ze merkte

Lisette de Bie

‘Kennis helpt enorm om grip te krijgen.’

in het begin dat er bij private partijen nog wel wat scepsis was over de inzet van de politie en het OM in de aanpak van online fraude. Dat beeld is gekanteld, constateert ze: “Als je als bedrijf ooit een mailtje hebt gestuurd over een fraude-geval en je hebt er nooit meer iets van gehoord, dan kan dat je beeld sterk bepalen. Maar als je dan terugkrijgt dat de politie misschien wel miljoenen van dat soort berichten krijgt en gezien de beperkte capaciteit nu eenmaal keuzes moet maken, dan kan dat het wantrouwen wegnemen. Ik merk nu dat er juist veel waardering voor de politie en het OM is. Alle partijen weten nu dat online fraude wel degelijk prioriteit heeft in opsporing en vervolging.”

Jan Dobbelaar

Ze waardeert ook de inzet van alle publieke en private partijen die meedraaien in de integrale aanpak: “Ik ben echt blij met hun inspanningen – en dan noem ik de Nederlandse Vereniging van Banken in het bijzonder. Zij hebben budget uitgetrokken voor de integrale aanpak en hebben een projectleider volledig vrijgesteld hiervoor. Ook andere partijen werken vol overtuiging mee, al is het voor sommige bedrijven wat lastiger om capaciteit vrij te maken.”

Kennis helpt

Ook Jan Dobbelaar is ervan overtuigd dat online fraude alleen goed kan worden aangepakt als de hele keten meedoet. Hij pleit wel voor realiteitszin: “Online fraude is niet simpel aan te pakken. Maar we willen wel er wel heel graag zicht op houden, zodat we zoveel mogelijk mensen en bedrijven ertegen kunnen beschermen. Daar hebben we elkaar voor nodig. Iedereen neemt op zichzelf al maatregelen en waar het beter is de handen ineen te slaan, doen we dat. Het is in ieder geval bewezen dat kennis al enorm helpt om grip te krijgen. Heel simpel: als iedereen weet dat de bank je nooit belt om samen in te loggen, dan trapt er ook niemand meer in.”

Ook de politie en het OM zijn zich ervan bewust dat online fraude veel aandacht nodig heeft. Waar alle vormen van criminaliteit al twintig jaar in omvang afnemen, stijgt online criminaliteit alleen maar. Stel dat de helft van de criminaliteit zich nu online afspeelt, dan kun je plat gezegd stellen dat dit ook de helft van de capaciteit van opsporing en vervolging vraagt. Daar is echt een transitie voor nodig en is gelukkig volop ingezet.”

Schade civielrechtelijk verhalen

Hij verwacht veel van het initiatief dat het mogelijk maakt om materiële en immateriële schade voortaan via het civielrecht te verhalen op de dader (zie ook het interview met Peter Hagenaars en Willem Bloem op pagina 22): “Ik geloof sterk in de kracht daarvan: iemand heeft jou getild, dus wil je je geld terug. Dan kun je zeggen dat de politie en het OM daarvoor verantwoordelijk zijn, maar er is niet genoeg capaciteit om alle zaken via het strafrecht te laten lopen. Voor de dader is het evengoed een tik als er opeens een deurwaarder op de stoep staat.”


‘We focussen op
wat we samen beter
kunnen bereiken
dan apart’

Overheid, banken, opsporingsdiensten, webwinkels, telecomproviders: iedereen is op eigen terrein al bezig met de bestrijding van online fraude? Waarom dan toch een integrale aanpak? Programmamanager Léon Poffé: "We richten op ons gebieden waar samenwerking voor een plus in de aanpak kan zorgen."

De concrete aanleiding voor het programma Integrale Aanpak Online Fraude is een toezegging van de Minister van Justitie en Veiligheid aan de Tweede Kamer om meer de regie te nemen in de aanpak van online fraude. Een fenomeen dat jaarlijks miljoenen mensen raakt. "Soms gaat het om iets kleins", legt Léon uit: "Je koopt online iets voor een paar tientjes en het wordt nooit geleverd. Maar soms veroorzaakt online fraude enorm veel schade; niet alleen financieel, maar ook emotioneel. Denk aan datingfraude waarmee tonnen buitgemaakt wordt en mensen tot in het diepst van hun ziel geraakt worden. Bedrijven waarvan de diensten worden gebruikt bij het plegen van fraude, zoals online verkoopplatforms en banken, zien veel. Want het doel van de fraudeur is geld verdienen en dat geld moet van a naar b. Maar al die partijen zijn maar een onderdeel in die keten en zien dat zij het niet alleen kunnen oplossen. Zij moeten samenwerken met andere delen van de keten en kloppen daarvoor ook aan bij de politiek."

Naast de grote schade die online fraude kan veroorzaken, noemt Léon nog een reden waarom het belangrijk het is om online fraude aan te pakken: "De overheid investeert gigantisch veel geld in de bestrijding van ondermijning. Dat is volledig terecht, want deze zware criminaliteit is enorm schadelijk voor de samenleving. Als je online fraude daartegen afzet, kun je misschien denken dat die minder schadelijk is. Maar criminelen maken geen onderscheid tussen het een en het ander. Online fraude is voor hen een verdienmodel voor de financiering van georganiseerde criminaliteit.
We moeten ons bewust zijn van de relatie daartussen. En we moeten ons meer richten op die samenhang dan op verschillen."

Waarom deze integrale aanpak?

Andere vormen van criminaliteit worden al integraal aangepakt. Denk aan woninginbraken, waarbij politie en ketenpartners nauw samenwerken, van preventie tot repressie. Ook online fraude verdient zo'n integrale aanpak, stelt Léon, omdat de impact hiervan vergelijkbaar is met die van andere soorten high-impactcriminaliteit: "Met het programma Integrale Aanpak Online Fraude willen we dat alle relevante partners in de fraudeketen de handen ineenslaan. Zij moeten eigenaarschap voelen én tonen. Niet alleen voor hun eigen deelgebied, maar voor de keten als geheel. Iedere schakel in de keten doet binnen zijn eigen stukje al heel veel. Deze

samenwerking gaat daar niet boven hangen, maar focust op wat we samen beter kunnen bereiken dan apart."

In 2022 is het programma gestart, maar in 2023 is het echt op stoom gekomen. Hoe kijk je terug op het afgelopen jaar?

"We weten elkaar steeds beter te vinden. Soms is een publiek-private samenwerking relatief eenvoudig, omdat de partners elkaar kennen en al met elkaar samenwerken, zoals bij infrastructurele projecten. Dan heb je te maken met grondeigenaren, bedrijven die willen bouwen, bestemmingsplannen... Kortom, bekende partners die op bekende terreinen samenkomen. Bij online fraude heb je te maken met partners die sterk van elkaar verschillen. Niet alleen wat betreft belangen, maar ook qua omvang, organisatie en aansturing. In het proces dat we in de zomer van 2022 zijn begonnen, moet je elkaar en elkaars positie dus eerst leren kennen. Je moet in een positie komen dat je elkaar iets durft te vragen, met respect voor de positie van de ander. Dat kost tijd."

Hoe is het programma ingericht?

"We ontwikkelen jaarlijks een actieplan aan de hand van zes thema's. Die thema's komen allemaal terug in dit jaarbericht. Binnen elk thema zorgen we dat we elkaars positie leren kennen en willen we tot maatregelen komen om de

schadelast en het aantal slachtoffers van online fraude te verminderen. Een kerngroep met een beperkt aantal partners stelt het jaarlijkse actieplan op en stuurt op uitvoering ervan. In het treffen van maatregelen tegen online fraude brengen we juist zoveel mogelijk betrokken partners om de tafel. We bieden al die partijen de zekerheid dat alles wat we delen binnenskamers blijft als dat en voorwaarde voor deelname is. Daar maken we harde afspraken over. Dat moet ook wel, want je vraagt partners soms gevoelige informatie van diep uit hun organisatie te delen met andere partners. Dan moeten zij erop aankunnen dat daar zorgvuldig mee wordt omgegaan. Bij de aanpak van bankhelpdeskfraude hebben we heel nadrukkelijk de lijn gekozen dat we alleen met informatie naar buiten gaan als alle partners daar ja op zeggen. Zelfs de kerngroep die de uitvoering van het actieplan aanstuurt, krijgt pas informatie als alle partners daar toestemming voor hebben gegeven."

Online fraude is een veelomvattend fenomeen. Waar richt het programma zich op?

"We kijken waar samenwerking voor een plus in de aanpak kan zorgen. Een aanpak waarmee we vérder komen. Dat geldt zeker voor het delen van persoonsgegevens. In de aanpak van online fraude zeggen partners al snel: 'We mogen geen persoonsgegevens delen van de AVG, dus moet er een wet komen die dat wel mogelijk maakt.' Maar voordat zo'n wet er is, ben je jaren verder, nog afgezien van de vraag hoe die echt bijdraagt aan effectievere bestrijding van online fraude. Als we in deze samenwerking op een uitvoeringsprobleem stuiten, maken we eerst een goede analyse. Veel regelgeving rond gegevensdeling is bijvoorbeeld neergelegd in sectorale wetgeving of een convenant. Het juridische kader kan enorm per situatie verschillen. Daarom harken we eerst alle informatie bij elkaar. Dat doen we niet alleen maar met wetgevingsjuristen van het ministerie, maar bijvoorbeeld ook met hoogleraren privacywetgeving en met privacydeskundigen van partijen als VNO-NCW en de NVB. Samen kijken we wat kan."

Ben je tevreden over het verloop van het project?

"Ja. Niet alles is in 2023 op tijd gelukt, maar we hebben toch veel gerealiseerd. We hebben onze informatiepositie versterkt en werkwijzen ontwikkeld om tot effectieve maatregelen te komen. Dat hebben we allereerst gedaan voor de aanpak van bankhelpdeskfraude en nu doen we dat voor verkoopfraude. De samenwerking is goed: we durven elkaar aan te spreken. De ambitie is om nog veel meer concrete maatregelen de bedenken en uit te voeren. Dat is de stap die we dit jaar willen zetten."

Zicht op fraude

‘Iedereen moet buikpijn krijgen van online fraude’

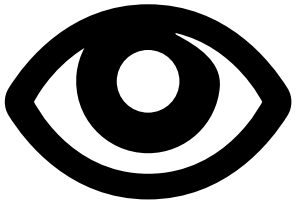
Het bedrijfsleven heeft steeds meer last van online fraude, stelt Karijn van Doorne, trekker van het thema Zicht op Fraude. Volgens haar begint een effectieve bestrijding met een zo compleet mogelijk begrip van het probleem. Dat is precies waar zij met de partners binnen het programma aan wil werken. “We weten nog niet goed genoeg wat er gebeurt.”

Karijn, jij vertegenwoordigt namens VNO-NCW en MKB-Nederland het bedrijfsleven. Wat merken zij van online fraude?

“Onze indruk is dat bedrijven steeds vaker slachtoffer zijn van online fraude. Dit leidt natuurlijk tot financiële schade, maar het zorgt ook voor een flinke deuk in het vertrouwen. De laatste jaren zien we een sterke verschuiving van fysieke criminaliteit naar online criminaliteit. Daarom hebben we samen met de banken een paar jaar geleden al gepleit voor een integrale aanpak van online fraude. Wij vermoeden dat het weleens de grootste vorm van criminaliteit kan zijn.”

Van welke vormen van online fraude heeft jouw achterban vooral last?

“Van allerlei vormen. We zien dat er veel aan- en verkoopfraude is. Maar we zien ook veel bankhelpdeskfraude: een crimineel doet zich voor als de bank en troggelt veel geld af. Verder speelt factuurfraude in het bedrijfsleven een grote rol. Je krijgt dan als ondernemer een valse factuur of van bestaande facturen wordt het rekeningnummer vervalst. Facturen worden tegenwoordig allemaal digitaal verstuurd en daarom kunnen online fraudeurs toeslaan.”



‘We weten nog niet goed genoeg wat er gebeurt, hoe groot het probleem is, wie getroffen worden en wat we eraan kunnen doen.’

Waar richt het thema *Zicht op fraude* zich op?

“Bij iedere vorm van criminaliteit begint de bestrijding ervan met inzicht in het fenomeen: waar hebben we het over? Pas dan kun je een goede aanpak verzinnen. Daarnaast zijn wij binnen ons thema aan het kijken hoe we de puzzelstukjes waar betrokken partijen al over beschikken in elkaar passen. Zo delen we kennis van trends en modus operandi met elkaar. Dadergroepen veranderen snel en dat geldt ook voor de manier waarop ze toeslaan. Tijdens COVID-19 zag je bijvoorbeeld een scherpe stijging van Whatsappfraude, terwijl in de aanloop naar de feestdagen veel malafide webshops worden opgezet. Het is belangrijk om dit soort kennis met elkaar te delen. Iedere afzonderlijke partij kan daarmee naar de eigen achterban terugkeren om samen passende barrières op te werpen.”

Waar hebben jullie het afgelopen jaar aan gewerkt?

“We zitten nog in de opstartfase, maar we zitten regelmatig met elkaar in een kamer om trends en ontwikkelingen te delen die de verschillende partners zien. Dat doen we ‘met de deur dicht’; we hebben goede afspraken gemaakt over vertrouwelijkheid, want het kunnen wel bedrijfsgevoelige gegevens zijn. Het punt is dat we niet met honderden online verkoopwinkels om de tafel kunnen zitten om informatie uit te wisselen. Daarom willen we dat geautomatiseerd gaan

doen. Denk aan informatie over aan- en verkoopfraude, zonder namen en rugnummers te noemen, want dat mag niet. Maar ook aan het waarschuwen van partijen in de keten als een partij slachtoffer is geworden van een nieuwe vorm van online fraude. Dan kunnen de anderen tijdig voorzorgsmaatregelen nemen. Bij de bouw van dit systeem laten we ons inspireren door het systeem dat de NCTV heeft ontwikkeld voor het delen van informatie rond cyberdreigingen."

Wat hoop je te bereiken met jullie inzet rond dit thema?

"Uiteindelijk moet het meer inzicht gaan opleveren in de wereld van online fraude die tot nu toe te veel buiten het zicht van de radar is gebleven. We weten nog niet goed genoeg wat er gebeurt, hoe groot het probleem is, wie getroffen worden en wat we eraan kunnen doen. Je moet ergens beginnen en we hebben ervoor gekozen om aan- en verkoopfraude als eerste aan te pakken. Deze vorm is ook aangewezen als een van de vijf grootste online fraudevormen. Ik hoop dat het systeem voor het uitwisselen van informatie snel in de lucht is. In de tussentijd zitten we niet stil. We denken aan het oprichten van een *trusted community* van pakweg de vijf grootste online verkooppunten. Misschien wel het belangrijkste dat ik hoop te bereiken is dat iedereen – particulier, bedrijf, overheid – buikpijn krijgt van online fraude en actie onderneemt. Ik zie het besef van urgentie nog niet overal. Heeft een bedrijf eenmaal een groot fraudegeval meegemaakt, dan worden er betere checks ingevoerd en wordt het vierogenprincipe voortaan toegepast. Particulieren moeten zich ook beter laten informeren en meer bedachtzaam worden."

Wat zie jij als de grootste uitdaging?

"Als een bedrijf is opgelicht, wil het de naam en het rekeningnummer van de fraudeur het liefst op een lijst zetten, zodat ook andere bedrijven gewaarschuwd zijn. Maar die informatie mag je als bedrijf niet delen. Er is nu een project waarbij je op Marktplaats een waarschuwing krijgt te zien dat je mogelijk te maken hebt met een fraudeur als je zaken wilt doen met een verkoper waartegen meermaals aangifte is gedaan. Dat zou eigenlijk veel vaker moeten kunnen. Momenteel is de politie altijd een cruciale schakel en moet er meermaals aangifte zijn gedaan. Terwijl je als gedupeerde al na één keer aan de bel wil trekken om herhaling te voorkomen. In Groot-Brittannië is er een onderling systeem van bedrijven waar deze gegevens onder allerlei privacyvoorwaarden wel aan elkaar beschikbaar kunnen worden gesteld. Misschien moeten we iets dergelijks ook maar eens in dit programma gaan verzinnen. Het bedrijfsleven heeft in ieder geval de wens om onderling meer informatie te mogen delen."

Geraliseerd in 2023

Zicht op fraude

→ Inrichting werkgroep politie, OM, banken en bedrijfsleven om informatie over MO's uit te wisselen op basis afspraken over o.a. vertrouwelijkheid

→ Besluit om in Q1 2024 'Zicht op digitale criminaliteit' live te laten gaan. Dit moet in 2024 verschillende factsheets opleveren.

→ Onderzoeken en monitors worden aangeboden op de 'ledenapagina' van www.integraleaanpakonlinefraude.nl.

→ De bouw van www.integraleaanpakonlinefraude.nl heeft geleid tot een combinatie van website en samenwerkingsruimte.

Gegevensdeling

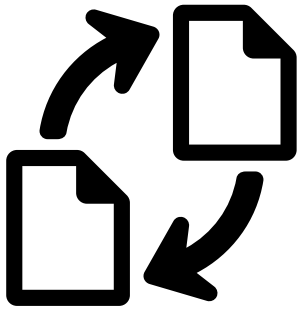
‘Gegevensdeling is niet alleen een juridisch vraagstuk’

Partijen in de fraudeketen zien obstakels rond gegevensdeling als een van de grootste belemmeringen om online fraude effectief aan te pakken. Maar welke obstakels zijn dat? En hoe kunnen we zorgvuldig persoonsgegevens delen als we tijdig maatregelen willen nemen? Leonore Duiker, privacyjurist bij JenV, licht de aandacht voor dit thema binnen de integrale aanpak toe: “Het gaat altijd om de balans tussen de informatiebehoefte van partijen en de bescherming van de persoonlijke levenssfeer van betrokkenen.”

Leonore, waarom is gegevensdeling zo ingewikkeld?

“De essentie van de AVG is dat je voor het delen van persoonsgegevens een juridische grondslag moet hebben. Op die wet wordt veel gemopperd, maar als we het nationaal goed regelen, hoeft het geen probleem te zijn. Gegevensdeling is

geen doel op zich, het is een belangrijk onderdeel van onze rechtstaat dat je niet zomaar persoonsgegevens mag delen. En zeker geen persoonsgegevens van strafrechtelijke aard. Partijen moeten de noodzaak aantonen en de waarborgen voor een betrokkene goed regelen. Er zijn meerdere mogelijkheden om op nationaal niveau grondslagen te creëren. Voor de telecomsector zijn die bijvoorbeeld beschreven in de Telecommunicatiewet en voor de financiële instellingen is dat de Wet op het financieel toezicht. Voor elke grondslag moet je de principes van de AVG heel duidelijk beschrijven. Maar gegevensdeling is niet alleen een juridisch vraagstuk. Het is een veelkoppig monster en dat maakt het ingewikkeld."



'Gegevensdeling is een veelkoppig monster en dat maakt het ingewikkeld.'

Kun je dat toelichten?

"Om te beginnen: we hebben geen ervaring in de praktijk op basis waarvan we kunnen zeggen: hier zou gegevensdeling effectief zijn geweest. Want als je het niet kunt uitproberen, kun je ook niet zeggen of het werkt. Binnen de integrale aanpak houden we ons daarmee bezig. TNO onderzoekt momenteel wat het zou opleveren als partijen in de fraudeketen hun databestanden zouden combineren. Helpt dat partijen om fraude te detecteren en tijdig maatregelen te nemen? Verder zien we dat gegevensdeling zeer beperkt mogelijk is en dat de juridische kaders én de aanpak per sector verschillen. Er zijn ook weinig overkoepelende ICT-voorzieningen. We zien daarnaast dat de vergunningverlening door de Autoriteit Persoonsgegevens niet past op de integrale aanpak van online fraude; fraudeurs kennen immers geen grenzen. Ik denk dat je ook wel kunt zeggen dat partijen bang zijn om gegevens te delen of juist te veel delen. Ze nemen ieder hun eigen maatregelen en delen bijvoorbeeld geen informatie met de politie omdat ze denken dat het niet mag. Daardoor blijft er veel informatie bij partijen achter. De politie ziet het niet, omdat er te weinig aangifte wordt gedaan. In het project kijken we ook hoe we het aantal aangiften omhoog kunnen krijgen."

Hoe pakken jullie het thema gegevensdeling binnen de integrale aanpak aan?

“We werken samen met partijen die dagelijks te maken hebben met online fraude, zoals banken, verzekeraars, telecombedrijven en webwinkels. In de Kamerbrief van de minister is een aantal fraudevormen aangewezen die prioriteit hebben, maar fraudeurs zijn inventief en we moeten dus niet te star zijn in het vinden van oplossingen. We verdiepen ons allereerst in wat volgens de verschillende partijen nu de problemen rond gegevensdeling zijn. Verder hebben we in 2023 vooral gepraat over wat voor verschillende soorten gegevensdelingen nu de beste oplossingsrichtingen zijn en welke pilots nodig zijn. Als partijen vinden dat wetgeving nodig is om problemen op te lossen, welk pad moet je dan bewandelen? Of zit de oplossing meer in de organisatorische sfeer en wat zijn dan de randvoorwaarden daarvoor? Ik blijf er daarbij op hameren dat gegevensdeling niet kan zonder dat je voldoet aan de waarborgen voor de betrokkenen. Dat is denk ik een les die we uit het recente verleden moeten trekken.”

Wat hoop je met de integrale aanpak rond gegevensdeling te bereiken?

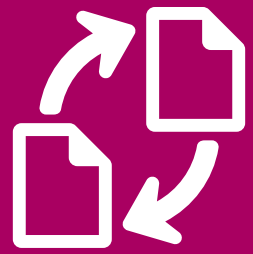
“Allereerst dat we het verleden erkennen: er wordt al sinds 2009 over het belang van gegevensdeling gepraat, maar het is nog nooit gelukt om met sluitende oplossingen te komen. Wat maakt dit tot zo’n lastig thema? Daar moeten we van leren. Uiteindelijk willen we dat partijen tijdig maatregelen kunnen treffen om slachtoffers te voorkomen. Het gaat altijd om de balans tussen de informatiebehoefte van partijen en de bescherming van de persoonlijke levenssfeer van betrokkenen. Als wij met goede oplossingsrichtingen komen, is het vervolgens aan de bestuurders om hun werk te doen. Tegelijkertijd zie ik dat partijen ook hun eigen aandeel leveren. Zo zijn duizenden mensen bij banken, verzekeraars en webwinkels dag in, dag uit bezig met het beperken van schade als gevolg van online fraude.”

Hoe verloopt de samenwerking?

“Goed. Iedereen is bereid mee te denken, contacten te leggen, kennis aan te boren en bij te dragen aan het thema. We werken in subgroepen rond deelthema’s. Zo heeft een subgroep de problemen en mogelijke oplossingen rond het gebruik van ‘verdachte (suspicious) devices’ in kaart gebracht. De subgroepen ontmoeten elkaar zeker een keer per maand. Ik vind het prettig om te merken dat er energie in zit. Vergeet niet dat dit een langlopend dossier is; we praten er sinds 2009 over het belang van informatie-uitwisseling voor de aanpak van georganiseerde criminaliteit, waaronder fraude. Tijd dat we tot gerichte acties komen.”

Geraliseerd in 2023

Gegevensdeling



→ Voor het vinden van oplossingen van knelpunten bij gegevensdeling vanuit casuïstiek is een aanpak ontwikkeld die vanuit analyse van het knelpunt via het onderzoeken van effectiviteit, het bepalen van het toepasselijke juridische kader (inclusief extern privacy advies) oplossingsrichtingen genereert. Die kunnen vervolgens worden getest in een onderzoeksetting of pilots om uiteindelijk geïmplementeerd te worden. Daarmee worden de actiepunten gevolgd in een vaste structuur die ook nodig is voor een oplossingsrichting via wetswijziging. Deze aanpak is in 2023 gestart m.b.t. 'suspicious devices'. De aanpak heeft hierbij de complexiteit van de vraagstukken verhelderd. In Q1 2024 worden vervolgstappen genomen.

→ Met de Autoriteit Persoonsgegevens is gesproken over de werkwijze van de Integrale Aanpak Online Fraude en in het bijzonder de aanpak voor gegevensdeling.

→ De start van het in Q2 op te leveren 'privacy kader' behandelt ook de juridische waarborgen bij gegevensdeling.

→ Een 'privacy expertgroep' onder leiding van een onafhankelijke voorzitter is ingericht om juridische vraagstukken met partners te beantwoorden.

Barrières en interventies

‘We maken het fraudeurs in alle fasen van de fraudeketen moeilijk’

Om burgers en bedrijven tegen online fraude te beschermen, wordt hard gewerkt aan technische barrières en interventies. Kirstin de Jong is vanuit de Nederlandse Vereniging van Banken (NVB) trekker van dit thema binnen de Integrale Aanpak Online Fraude. “We willen elkaar allemaal versterken om het aantal slachtoffers van online fraude te verminderen.”

Kirstin, met welke partijen werken jullie samen in de Integrale Aanpak?’

“In 2023 zijn we begonnen met het uitdiepen van het onderwerp bankhelpdeskfraude. Binnen dat onderwerp hebben we zoveel mogelijk partijen betrokken die in de keten van dit type online fraude een rol spelen. Naast de banken zijn dat onder meer de Nationale Politie, het Openbaar Ministerie, de telecomsector, Microsoft en Fox-IT. Dit jaar gaan we van start met het onderwerp verkoopfraude. Daar betrekken we de

grote online verkopers bij, zoals Amazon, Bol.com, Coolblue, Otto en Wehkamp. Ook de vervoerders, zoals DHL en Post NL doen mee. Vervoerders zitten iets verderop in de keten, maar zijn ook belangrijk om erbij te betrekken. En verder zijn onder andere de payment service providers, organisaties voor achteraf betalen, de deurwaarders en de politie betrokken. Zo zoeken we bij elk type fraude naar de meest effectieve coalitie."

'We zoeken bij elk type fraude naar de meest effectieve coalitie.'

De focus richt zich dus eerst op bankhelpdesk-fraude. Hoe groot is het maatschappelijk probleem van deze vorm van fraude?

"Groot. Bankhelpdeskfraude is momenteel het grootste probleem qua schadelast. De totale schade was in 2023 ruim 28 miljoen euro. Er zijn enorm veel slachtoffers gemaakt. Om meer grip op deze vorm van fraude te krijgen, hebben de partners de handen ineengeslagen om een criminal journey en een barrièremodel te maken. Daardoor krijgen de organisaties beter inzicht in hoe de oplichters te werk gaan en welke maatregelen er genomen kunnen worden."

Hoe maak je die criminal journey?

"Daarvoor zetten we de fraude-experts van alle organisaties die zijn aangesloten bij elkaar. Samen brengen we de werkwijze van de fraudeur in zes stappen in kaart. De eerste fase is de oriëntatiefase, waarin de fraudeur verschillende soorten informatie verzamelt en een handelswijze uitdenkt. Dan begint de voorbereidingsfase, waarin de identiteit wordt verhuld en er ondersteunende middelen worden aangeschaft, zoals telefoons. Daarna wordt er contact met slachtoffers gelegd, waarna het slachtoffer ervan wordt overtuigd dat diens geld niet veilig is. De laatste fasen van de criminal journey zijn dat het geld wordt overgeheveld van het slachtoffer naar de fraudeur en de fraudeur het geld besteedt aan bijvoorbeeld goederen of diensten. De partners met wie we

samenwerken, beschikken elk over stukjes informatie uit verschillende fasen van de fraudeketen. Zo krijgen we een mooi compleet overzicht van hoe die keten eruitziet."

En dan kijken jullie vervolgens per fase van de criminal journey welke barrières en interventies kunnen worden ingezet?

"Klopt. Dus niet alleen aan het eind, waar gelden naar de fraudeur worden overgemaakt, maar ook aan het begin als de fraudeur zich nog aan het oriënteren is. Om fraudeurs niet wijzer te maken dan ze al zijn, kan ik daar helaas niet veel over vertellen. Heel algemeen gesteld bedenken we technische barrières en interventies om het de fraudeurs in alle fasen van het fraudeketen moeilijk te maken. We richten ons expliciet op de fraudeur; een ander thema in de integrale aanpak is specifiek gericht op hulpverlening aan slachtoffers van bankhelpdeskfraude. Voor bankhelpdeskfraude hebben we de criminal journey afgerond en hebben we op basis daarvan een barrièremodel ontwikkeld. Het barrièremodel laat zien welke barrières ketenpartners in de verschillende fase van de fraudeketen kunnen opwerpen tegen criminele activiteiten."

Hoe verloopt de samenwerking?

"Goed. We werken in een vertrouwelijke setting samen en delen onder geheimhouding informatie met elkaar. Door het delen van informatie ontstaan er creatieve ideeën voor effectieve barrières en interventies. Onder meer tijdens een tweedaagse in het najaar van 2023. Het is prettig om te merken dat iedereen samen dit grote maatschappelijke probleem wil oplossen. Partners weten elkaar nu sneller te vinden, zijn zich bewust van hun rol en verantwoordelijkheid in de fraudeketen en nemen die verantwoordelijkheid ook. Informatie wordt nu sneller gedeeld dan dat het zonder dit samenwerkingsverband zou zijn gebeurd."

Geraliseerd in 2023

Barrières en interventies

→ Voor de uitwerking van de actiepunten over fraudevormen is gekozen om in 2023 een aanpak uit te werken en deze toe te passen op één fraudevorm, namelijk bankhelpdeskfraude. Hiervoor is een ‘criminal journey’ uitgewerkt op basis waarvan een barrièremodel is uitgewerkt en interventies zijn gekozen die nu worden ontwikkeld.

→ Voor 2024 zijn de verkoopfraude en aankoopfraude al benoemd om met dezelfde aanpak uitgewerkt te worden.

→ In het kader va n de Global Anti Scam Alliance zijn ‘best practices’ en ‘lessons learned’ uitgewisseld. Ook is er contact gelegd met andere EU-landen en met het VK om ervaringen over integrale aanpakken uit te wisselen.

Opvolging door politie en openbaar ministerie

‘We moeten continu blijven kijken of we het juiste doen’

Peter Hagenaars

De politie en het openbaar ministerie (OM) hebben de handen ineengeslagen om daders van online fraude aan te pakken. Onder de noemer Operatie Centurion worden zaken met prioriteit aangepakt. In de integrale aanpak leggen beide organisaties de verbinding met private partijen om nog beter grip te krijgen op online fraude. We praten met Peter Hagenaars (Nationale Politie) en Willem Bloem (OM) over hun samenwerking én die met private partners: “We hebben elkaar keihard nodig.”

De coronapandemie bracht versnelling in een trend die al eerder was ingezet: de criminaliteit verplaatst zich van de straat naar het online domein. Die online criminaliteit varieert van een simpele oplichting waarmee mensen voor een paar tientjes worden getild tot grootschalige cybercriminaliteit die een gevaar vormt voor de nationale veiligheid. “Het linkje in je e-mail kan afkomstig zijn van iemand op een zolderkamer die er simpelweg geld mee verdient”, zegt Willem. “Maar het kan ook door een criminele actor zijn verstuurd in opdracht van een statelijke partij. Het geeft aan hoe breed het veld is waar wij mee te maken hebben. De integrale aanpak

richt zich primair op een aantal online fraudevormen, maar in de praktijk zien we dat criminelen opportunistisch zijn en traditionele criminaliteit en online criminaliteit in elkaar overlopen."

Peter: "We kijken naar de ontwikkelingen in de samenleving en proberen daar een sluitende aanpak voor te vinden. We zien al ruim tien jaar dat de criminaliteit zich verplaatst van de fysieke naar de online wereld. En de impact is groot. Waar een traditionele inbraak een beperkt aantal slachtoffers maakt, kan een online fraudeur gemakkelijk duizend slachtoffers maken. Bij sommige vormen zien we een oververtegenwoordiging van een bepaalde groep slachtoffers. Zo zijn senioren extra kwetsbaar voor bankhelpdeskfraude. Het is echt een smerige vorm van criminaliteit die tot schrijnende situaties leidt. Een op de vijf slachtoffers ervaart emotionele problemen. Er zijn mensen die jarenlang hun pensioenpotje hebben gevuld en hun geld in één klap kwijt zijn."

Begin dit jaar werden vijf verdachten aangehouden in een grote bankhelpdeskfraudezaak. Ook werd bekend dat deze vorm van online fraude sterk is gedaald. Krijgen jullie meer grip op online fraude?"

Peter: "We hebben afgelopen jaren in ieder geval een slag gemaakt. Er is flink geïnvesteerd in de strafrechtketen om goede prestaties te leveren met opsporing en vervolging. Het omslagpunt is bereikt: vandaag de dag zijn meer mensen

'Criminelen zijn opportunistisch en traditionele en online criminaliteit lopen in elkaar over.'

slachtoffer van online criminaliteit dan van fietsendiefstal. Alle reden dus om meer werk te maken van de aanpak van online criminaliteit. Dat het serieuze criminaliteit is, blijkt ook uit de straffen die worden opgelegd: gevangenisstraffen van vier jaar of meer, onvoorwaardelijk, zijn geen uitzondering. We zijn al langer bezig om beide organisaties erop in te richten, ook door nieuwe vaardigheden aan te leren. Het helpt ook dat we zaken beter inzichtelijk kunnen maken voor de collega's van het OM en onze blauwe teams. Doordat we financiële opsporingsinformatie via het Verwijzingsportaal Bankgegevens nu automatisch kunnen routeren naar de juiste lokale teams, kunnen we veel sneller vervolgacties

plannen. Vaak zie je dat de lokale teams de verdachten in kwestie al wel kennen uit eerdere incidenten."
Willem: "Tegelijkertijd hebben we nog wel een grote opgave. Kijk je naar de ontwikkelingen rond nieuwe technologieën, dan zal geloofwaardige oplichting voor daders alleen nog maar eenvoudiger worden. Denk bijvoorbeeld aan deepfakes waarbij AI is gebruikt."

In de integrale aanpak zoeken jullie nadrukkelijk de samenwerking met private partijen. Wat is de inzet daarvan?

Willem: "We volgen een brede strategie, waarin politie en OM natuurlijk een belangrijke rol hebben in het opsporen en vervolgen van online fraude. Maar we kijken ook naar de rol en verantwoordelijkheid van partijen die al eerder in het proces iets kunnen doen. Misschien kunnen ze eerder signalen oppikken of zelf ingrijpen, waardoor het strafrecht niet eens hoeft te worden ingezet."
Peter: "Dat de strafrechtketen een beperkte capaciteit heeft, is bekend. Dus moet je zuinig zijn in welke zaken je ook echt het strafrechtelijke kanaal in laat gaan. Daarom is er de afgelopen jaren meer oog gekomen voor alternatieve interventies. Denk aan een stopgesprek met de dader of

Willem Bloem

een directe aansprakelijkheidsstelling volgens het privaatrecht. De dader krijgt dan een deurwaarder aan de deur. Het voordeel van zo'n aanpak is dat het vaak jonge daders zijn bij wie een tik op de neus nog weleens helpt om een criminele carrière te verstoren. Slachtoffers hebben waardering voor die aanpak: de dader moet dan toch betalen en vaak zit er ook een vergoeding voor immateriële schade aan vast. Bijkomend voordeel is dat deze aanpak de strafrechtketen niet belast. Binnen de integrale aanpak doen we ervaring op met dit soort alternatieve interventies."
Willem: "Belangrijk is dat we continu blijven kijken of we met onze aanpak het juiste doen. Werkt de alternatieve aanpak, in welke zaken kunnen we ze inzetten en wanneer zetten we wel het strafrecht in? Daar zit natuurlijk een spanningsveld in en het is zaak om daar een goede balans in te vinden."

Wat verwachten jullie van de private partijen binnen de integrale aanpak?

Peter: "Alles wat private partijen aan de voorkant kunnen voorkomen of oplossen, hoeft niet bij ons terecht te komen. Maar het is natuurlijk een utopie dat banken, payment service providers, webwinkels, telecombedrijven en andere partners alles kunnen tegenhouden. Ik ben in ieder geval enthousiast over de samenwerking met banken en telecomproviders. Zij hebben veel gedaan om schade te beperken, bijvoorbeeld door betalingslimieten te verlagen, tijdsvertragingen in te bouwen en spoofing tegen te gaan. Dat helpt enorm. Wij zouden graag de banden met de grote techbedrijven en socialmediabedrijven willen aanhalen. De uitnodiging om met elkaar in gesprek te gaan, staat. Maar de komst van wetgeving als stok achter de deur is wat mij betreft ook een belangrijk onderwerp."
Willem: "Uiteindelijk is 'geven en nemen' de kern van een publiek-private samenwerking. Iedere partij aan tafel moet het gevoel hebben dat er iets uit te halen valt. Ook in de integrale aanpak heeft iedereen zijn eigen belang. Maar we hebben ook een gezamenlijk doel: het terugdringen van online fraude. Voor de een is dat primair een commercieel belang en de ander wil een betere bescherming van burgers. Maar het is wel belangrijk om dat gemeenschappelijk belang met elkaar te voelen. Als politie en OM leveren we onze bijdrage en die is belangrijk, maar het strafrecht lost geen problemen op. Daar hebben we elkaar keihard voor nodig."
Peter: "We doen wat we kunnen en dat zit vooral aan het einde van de keten. Wij moeten ervoor zorgen dat er consequenties verbonden zijn aan het strafbaar handelen van daders. Maar dat kunnen we alleen goed als we samen met partners werken aan preventie en verstoring van dit soort criminele activiteiten. En daar kunnen private en andere publieke partijen bij uitstek voor zorgen. Als we die samenhang met elkaar vorm kunnen geven, dan hebben we iets moois in handen."

Geraliseerd in 2023

Opvolging door politie en openbaar ministerie

→ Berichten uit opsporing en vervolging worden voortdurend binnen de integrale aanpak uitgewisseld.

→ Vanuit de integrale aanpak is voor de actiepunten met betrekking tot een digitaal aangifteloket voor bedrijven aangesloten bij het bredere traject binnen de politie om meldingen en aangiften beter online te ondersteunen en in de organisatie te routeren.

→ Mogelijkheden voor civielrechtelijke afdoening vormen nu onderwerp van een breed onderzoek dat nu plaatsvindt door de Haagse Hogeshool.

Weerbaarheid en preventie

‘We moeten trends blijven signaleren en blijven waarschuwen’

Hoe kunnen we burgers en bedrijven weerbaarder maken tegen online fraudeurs? En hoe is te voorkomen dat mensen de stap naar online criminaliteit zetten? Daarop richt de actielijn Weerbaarheid zich. Kerngroeplid Astrid de Jong kan niet genoeg benadrukken hoe belangrijk dit thema is: “2,2 miljoen slachtoffers per jaar? Ik denk dat het werkelijke cijfer nog veel hoger ligt.”.

Astrid, je bent al jaren bezig om mensen en bedrijven weerbaarder te maken tegen online fraude. Wat is nieuw in de integrale aanpak?

“Het vernieuwende is dat het nu op landelijk niveau gebeurt met publieke en private partners samen. Een paar jaar geleden hebben we in de regio Rotterdam sessies georganiseerd voor publieke en private partijen rond dit thema. We concludeerden toen dat we moeten samenwerken om slachtofferschap van online fraude te voorkomen en barrières moesten

opwerpen voor de daders. Alle partijen vonden het dringend noodzakelijk, maar vonden het ook gek dat het niet landelijk werd aangepakt. Het is mooi dat we het nu heel krachtig op landelijk niveau oppakken en dat heel veel partners zich daaraan gecommitteerd hebben."

Volgens de meest recente cijfers van het CBS vallen jaarlijks 2,2 miljoen Nederlanders ten prooi aan online criminelen...

"Ik denk dat het cijfer nog veel hoger ligt. Bedrijven die getroffen worden door ransomware, doen bijvoorbeeld vaak geen aangifte. Als je je bedrijf weer snel in de lucht wil krijgen, denk je kennelijk dat het handiger is om maar snel losgeld te betalen. Veel burgers schamen zich daarnaast zo erg dat ze niet eens tegen hun naaste familie durven te vertellen dat ze zijn opgelicht. Ze voelen zich dom, maar dat zijn ze niet; ze zijn slachtoffer van doortrapte fraudeurs. Toevallig vertelde een jonge collega mij laatst dat hij ook ergens was ingetrapt. We werkten toch echt al een tijdje samen, maar hij durfde het nooit te vertellen. Het probleem is dat fraudeurs wendbaar zijn. Ik denk dat Whatsappfraude inmiddels door veel mensen wel op tijd wordt herkend. Met de mogelijkheden van AI krijg je straks misschien wel een levensecht beeld van je dochter op je telefoon, inclusief de stem die bij haar past. We moeten trends dus blijven signaleren en waarschuwen en daar hebben we alle partijen bij nodig."

De actielijn richt zich onder meer op de rol van de gemeenten. Waarom zijn zij zo belangrijk in het voorkomen van slachtofferschap?

"Gemeenten zijn verantwoordelijk voor de openbare orde en veiligheid. Bij incidenten op straat weet iedereen precies hoe er gehandeld moet worden. Maar digitale veiligheid was tot voor kort een nieuw thema voor gemeenten. Wij ondersteunen initiatieven in gemeenten om burgers bewust te maken van risico's. Zo hebben we onlangs in een gemeente de seniorenbonden ondersteund zodat zij zelf voorlichting kunnen geven. Bibliotheken zijn in gemeenten het informatiepunt voor mensen die daar hun digitale zaken willen rege-

'We moeten trends blijven signaleren en blijven waarschuwen.'

len. Het thema digitale veiligheid was daar niet automatisch aan gekoppeld. Ik heb mijn moeder zover gekregen dat zij niet zomaar op iedere link klikt. We helpen gemeenten om die rol ook te vervullen. Denk ook aan hulp bij het instellen van tweefactorverificatie."

Slachtofferschap voorkomen is een belangrijke doelstelling van deze actielijn. Hoe zit het met het voorkomen van daderschap?

"Ook daar richten we ons op. We hebben laatst samen met een aantal gemeenten en de politie een Re_bootcmp georganiseerd voor jongeren met bovengemiddelde IT-vaardigheden. Het risico bestaat dat zij verleid worden om hun skills op een verkeerde manier in te zetten. Met allerlei challenges, verhalen van ethische hackers en bijdragen van gerenommeerde IT-bedrijven willen we duidelijk maken dat er aan de goede zijde van het spectrum ook een behoorlijke boterham te verdienen valt."

Wat staat er op het to do-lijstje van 2024?

"We zijn binnen de landelijke aanpak van plan om stevig aan de slag te gaan met gegevensdeling, in samenwerking met de actielijn die zich op dit thema richt. Het is een ontzettend ingewikkeld thema. Verder komen er allerlei bewust-wordingscampagnes aan waar wij op aansluiten. We bou-wen binnen de regio Rotterdam ook voort op onderzoek door de Saxion Hogeschool en de Haagse Hogeschool naar bewustwording bij kwetsbare doelgroepen. Daaruit kwam bijvoorbeeld naar voren dat jonge meiden zeer vatbaar zijn voor online campagnes voor sieraden, make-up en kleding. Er is toen een campagne bedacht waarbij zij op Instagram, TikTok of Snapchat een advertentie te zien kregen. Nadat ze op de link hadden geklikt, werd hun telefoon zwart en begon die te trillen. Daarna kregen zij een waarschuwing in beeld en konden ze een quiz invullen om te leren hoe zij zich beter kunnen beschermen tegen online criminelen. Op basis van onderzoek en actuele fenomenen ontwikkelen we gerichte campagnes en interventies per doelgroep."

Geraliseerd in 2023

Weerbaarheid en preventie

→ Aangesloten wordt bij bestaande structuren van overleggen en netwerken waarbij de meeste communicatieadviseurs al in opereren om ‘dubbel werk’ te voorkomen.

→ In de voorbereiding van de Week van de Veiligheid is door verschillende partners van de integrale aanpak het onderwerp online fraude bij de organisatie van de diverse evenementen naar voren gebracht.

→ De Integrale Aanpak Online Fraude heeft met politie en Nederlandse Vereniging van Banken een gezamenlijke stand bij de 50PlusBeurs bemenst.

→ De integrale aanpak heeft zich aangesloten bij de reeds gemaakte inventarisatie van preventiemaatregelen bij gemeenten.

→ Eind 2023 ging de grote publiekscampagne ‘veilig interneppen’ van start om mensen weerbaar te maken voor ‘social engineering’.

Hulp aan slachtoffers

‘Als je elkaar kent, weet je elkaar beter te vinden’

Online fraude veroorzaakt op grote schaal leed bij slachtoffers. Wie getroffen wordt, weet vaak niet goed wat te doen. De actielijn Hulp aan slachtoffers zet in op een goede begeleiding van slachtoffers, psychosociaal, praktisch en technisch. Doel is ook om te voorkomen dat mensen opnieuw slachtoffer worden. Julia Smeekes, coördinerend beleidsadviseur bij JenV: "Het moet niet uitmaken waar slachtoffers zich voor het eerst melden; als ze maar goed geholpen worden."

Julia, jij bent trekker van de actielijn Hulp aan slachtoffers. Welke impact heeft online fraude op slachtoffers?

"De gevolgen zijn ingrijpend. Op het webinar van de integrale aanpak eind vorig jaar vertelde cybercrimespecialist bij de politie Jildau Borwell over haar onderzoek hiernaar. Haar conclusie was dat de impact van online criminaliteit op slachtoffers op veel vlakken nog groter kan zijn dan de traditionele high-impactcriminaliteit. Slachtoffers schamen zich vaak voor wat er gebeurd is en hun gevoel van veiligheid kan enorm aangetast worden. Want online fraude gebeurt via de digitale middelen die je de hele dag om je heen hebt. En dan hebben we het nog niet eens over de financiële schade; het kan om een klein bedrag gaan, maar mensen kunnen ook enorm veel geld kwijtraken. Dit heeft dan weer zijn eigen effecten op mensen."

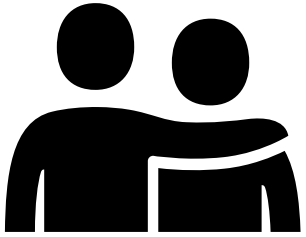
Wat willen jullie met deze actielijn bereiken?

"We willen allereerst de ondersteuning aan slachtoffers verbeteren. Er is gelukkig geen tekort aan meldpunten waar zij terecht kunnen als ze online zijn opgelicht. Alleen is het voor slachtoffers niet direct inzichtelijk welke ondersteuning ze kunnen krijgen en bij wie ze daarvoor moeten zijn. In de integrale aanpak kijken we hoe we de hulp aan slachtoffers zo goed mogelijk kunnen organiseren. Daarvoor moeten we goed samenwerken met de hulppunten die er al zijn. We hebben daarvoor een werkgroep ingericht die regelmatig bijeenkomt. Het Centrum voor Criminaliteitspreventie en Veiligheid faciliteert en coördineert deze. Daar zitten vertegenwoordigers in van al die meld- en hulppunten: de NVB namens de banken, de politie, Slachtofferhulp Nederland. Maar ook de Fraudehelpdesk, het Centraal Meldpunt Identiteitsfraude, de Consumentenbond, de Autoriteit Consument en Markt en de Autoriteit Financiële Markten. Al die partijen hebben zich gecommitteerd om de samenwerking te verstevigen."

Waar hebben jullie de afgelopen periode aan gewerkt?

"Om de samenwerking tussen de verschillende meld- en hulppunten goed vorm te geven, heeft de Consumentenbond in 2023 een panelonderzoek uitgevoerd. Daarin is slachtoffers gevraagd waar zij zich hebben gemeld en hoe zij de

ondersteuning door de verschillende meldpunten hebben ervaren. Wisten ze de juiste ingang te vinden, werden ze goed geholpen? Dit onderzoek gaf ons een actueel inzicht in waar we staan. Toen hebben we gekeken welk beeld de verschillende meldpunten hebben van elkaar. Een terugkerend geluid was dat er veel behoefte was om elkaar beter te leren kennen. Want als je elkaar kent, weet je elkaar beter te vinden en kan je slachtoffers beter naar de juiste hulp verwijzen. Een deel van deze contacten bestond al, maar ze zijn geïntensiveerd. Meldpunten zijn bij elkaar op bezoek geweest. En binnenkort gaat de werkgroep op bezoek bij het hulploket van de Consumentenbond om daar te spreken met de mensen die slachtoffers te woord staan. Verder heeft het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) een factsheet ontwikkeld. Daarin staat precies welke vragen je het slachtoffer kunt stellen, naar welke soort hulp je slachtoffers kan verwijzen en wie hulp biedt. Verder heeft het CCV op basis van interviews aanbevelingen gedaan voor verbeteracties in het landschap van meldpunten. Die aanbevelingen hebben we verwerkt in het actieplan voor 2024."



'Waar het slachtoffer als eerste binnenkomt moet niet uitmaken.'

Kun je daar voorbeelden van noemen?

"Een belangrijke aanbeveling is dat we ervoor moeten zorgen dat het slachtoffer niet onnodig wordt belast doordat het langs verschillende meldpunten moet gaan en daar steeds hetzelfde moet vertellen. Het blijft zeer waarschijnlijk dat je als slachtoffer langs meerdere loketten moet omdat er niet één organisatie is die alle hulp biedt. Maar de intake is een voorbeeld van iets dat beter georganiseerd kan worden. Waar het slachtoffer als eerste binnenkomt, moet niet uitmaken: als hij of zij maar goed verder wordt geholpen. Daarnaast willen we dit jaar een tool ontwikkelen waarmee je als slachtoffer zelf kunt vinden waar je je moet melden voor welke vorm van online fraude. Belangrijk daarin is dat we niet

moeten vergeten dat er al heel veel is waar we gebruik van kunnen maken. Zo willen we informatie integreren in Mijn Slachtofferzaak.nl. Het gaat dan om informatie over wat je als slachtoffer kan doen en bij welke organisaties je terechtkunt. Na aangifte bij de politie kun je via dit portal de voortgang van jouw aangifte volgen en lees je wat je aanvullend kan doen."

Is de informatievoorziening door de verschillende meldpunten eenduidig?

"Ook dat is iets waar we het komende jaar aan werken. We lopen er nu tegenaan dat het informatieaanbod best gefragmenteerd is. Als slachtoffer kun je overal stukjes informatie vinden, maar niet op één plek. Je moet zelf flink op zoek, bijvoorbeeld naar informatie over mogelijkheden om je financiële schade te verhalen. Belangrijk is ook dat de medewerker van het meldpunt het slachtoffer niet 'loslaat' op het moment dat deze een melding doet. Je moet dan al met de volgende stap bezig zijn; de doorverwijzing naar de andere partij. Bij een 'koude' doorverwijzing vertel je waar het slachtoffer moet zijn voor die hulp. Mooier is nog om het slachtoffer 'warm' door te verwijzen. Daarmee gaan we dit jaar aan de slag. Kan het slachtoffer dat zich meldt bijvoorbeeld ondersteund worden in het doen van aangifte? En – nog een stap verder – in het opstarten van een procedure voor schadeverhaal? Ook kijken we samen met de actielijn Gegevensdeling of meldingen automatisch kunnen worden doorgezet met een heel beperkt aantal gegevens. De Autoriteit Consument en Markt kan bijvoorbeeld veel met fraudemeldingen doen in het kader van preventie. Het zou niet nodig moeten zijn dat het slachtoffer daarvoor opnieuw een telefoontje moet plegen of een formulier moet invullen."

Hoe verloopt de samenwerking?

"Daar ben ik heel tevreden over. Als we bijvoorbeeld samen met het CCV een werkgroep organiseren, dan is iedereen erbij en levert ook een bijdrage vanuit de eigen organisatie. Op die positieve energie bouwen we verder. De leden van de werkgroep hebben een belangrijke rol om ervoor te zorgen dat verbeteringen in hun eigen geledingen worden geïmplementeerd. Denk het bekendmaken van de factsheet over meldpunten en de vuistregels die het CCV ontwikkelt."

Geraliseerd in 2023

Hulp aan slachtoffers

→ De consumentenbond heeft een breed panelonderzoek naar online fraude en slachtofferschap uitgevoerd waarin ook melden en meldpunten zijn meegenomen. De resultaten zijn breed in de integrale aanpak en met aanmeldpunten besproken.

→ Er is een netwerk van bestaande meldpunten tot stand gebracht waarin acties uit de integrale aanpak op het gebied van hulp aan slachtoffers worden besproken.

→ Er is een gezamenlijke factsheet gemaakt voor de medewerkers van de meldpunten om slachtoffers beter te informeren.

→ De juridische en organisatorische voorwaarden voor de totstandkoming van een ‘anti phishing shield’ naar Belgisch model worden door de ministeries van JenV en EZK en de politie onderzocht.

Voor meer informatie:

integraleaanpakonlinefraude@minjenv.nl

integraleaanpakonlinefraude.nl

Integrale aanpak

online fraude