POLITIE & Wetenschap

Op zoek naar de parels bij de lokale aanpak van cybercriminaliteit en gedigitaliseerde criminaliteit

een verkennend onderzoek

Jim Schiks, Msc.
Dr. Susanne van 't Hoff - de Goede
Dr. Rutger Leukfeldt

De Haagse Hogeschool, Centre of Expertise Cybersecurity, lectoraat Cybercrime and Cybersecurity
Nederlands Studiecentrum voor Criminaliteit en Rechtshandhaving (NSCR)

Op zoek naar de parels bij de regionale en lokale aanpak van cybercriminaliteit en gedigitaliseerde criminaliteit.

Een verkennend onderzoek.

Op zoek naar de parels bij de regionale en lokale aanpak van cybercriminaliteit en gedigitaliseerde criminaliteit.

Een verkennend onderzoek.

Auteurs:
Jim Schiks, Msc.
Dr. Susanne van ’t Hoff - de Goede
Dr. Rutger Leukfeldt

De Haagse Hogeschool, Centre of Expertise Cybersecurity, lectoraat Cybercrime and Cybersecurity

Nederlands Studiecentrum voor Criminaliteit en Rechtshandhaving (NSCR)

Politie & Wetenschap
septemer 2022

Samenvatting

Achtergrond

Met de digitalisering van onze samenleving krijgen steeds meer delicten een digitale component. Dergelijke delicten worden ook wel aangeduid als online criminaliteit. Onder online criminaliteit verstaan we in dit onderzoek zowel delicten die worden gepleegd via ICT en ook gericht zijn op ICT (cybercriminaliteit) als delicten waarbij ICT alleen een rol speelt bij de modus operandi (gedigitaliseerde criminaliteit). Slachtofferschap van online criminaliteit is nu al hoog en neemt met de steeds verdergaande digitalisering alleen maar toe. Dergelijke delicten zullen daarom steeds vaker onderdeel worden van het dagelijkse werkaanbod van politiemedewerkers. Feitelijk is 'digitaal' nu 'normaal' geworden en krijgen politiemedewerkers door de hele organisatie heen met allerlei varianten van online criminaliteit te maken. De aanpak van online criminaliteit heeft binnen de politie eerst op nationaal niveau (bijvoorbeeld met de oprichting van het Team High Tech Crime en het Dark Web Team) en later op eenheidsniveau (met de komst van de zogenaamde cybercrime teams) de laatste jaren vorm gekregen. Inmiddels zijn ook binnen de regionale politie-eenheden allerlei initiatieven op het gebied van de aanpak van online criminaliteit. Op dit moment ontbreekt echter zicht op al deze regionale en lokale initiatieven, waardoor het onduidelijk blijft hoe de aanpak van online criminaliteit op lokaal en regionaal niveau vorm krijgt.

Onderzoeksdoel en -vragen

In onderhavig onderzoek staan de initiatieven van de regionale en lokale aanpak van online criminaliteit centraal. Het onderzoek heeft tot doel om een overzicht te maken van veelbelovende initiatieven op het gebied van online criminaliteit, zodat eenheden van elkaar kunnen leren, zodat regionale en lokale initiatieven eventueel op grotere schaal kunnen worden ingezet, maar ook om inzicht te krijgen in de knelpunten binnen de aanpak van online criminaliteit. De onderzoeksvraag van dit onderzoek is tweeledig. Allereerst identificeren we regionale en lokale initiatieven. Vervolgens wordt de inhoud van deze initiatieven onderzocht en gekeken in hoeverre de beschreven initiatieven in andere eenheden of regio's toepasbaar zijn. De onderzoeksvragen van het onderzoek zijn:

1. Welke initiatieven zijn er bij de regionale en lokale afhandeling van online criminaliteit?
2. Wat zijn de kenmerken van deze initiatieven? (aanleiding, activiteiten, doel, onderbouwing, effectiviteit, toepasbaarheid binnen andere eenheden)

Onderzoeksmethoden

Voor het onderzoek zijn drie kwalitatieve onderzoeksmethoden gebruikt: interviews, documentanalyse en een expertbijeenkomst. Interviews zijn gehouden met initiatiefnemers of personen die op andere wijze nauw betrokken zijn bij een initiatief. In aanvulling op de interviews zijn beschikbare documenten rondom de initiatieven geraadpleegd. De resultaten zijn ten slotte besproken met experts, werkzaam bij de politie, de Koninklijke Marechaussee en in de wetenschap, om tot concrete aanbevelingen te komen.

In totaal zijn 37 initiatieven geïdentificeerd tijdens het onderzoek. Uit alle politie-eenheden is ten minste één initiatief gemeld, met uitzondering van de eenheid Noord-Holland. Uiteindelijk zijn 19 initiatieven geïncludeerd in het onderzoek. De overige initiatieven zijn afgevallen omdat zij niet voldeden aan de criteria van een 'parel' of teveel overlap hadden met een eerder gemeld initiatief. Voor de geselecteerde initiatieven zijn gestructureerde interviews afgenomen met initiatiefnemers of personen die op een andere manier nauw betrokken zijn bij het initiatief. Het doel van de interviews was om een beter inzicht te krijgen in de plannen, onderbouwing en uitvoering van geïdentificeerde initiatieven.

Definitie van een 'parel'

Een 'parel' is een regionaal of lokaal initiatief binnen de politie, waarin de aanpak of preventie van online criminaliteit centraal staat. Een parel is op regionaal of lokaal niveau ontstaan, en is (nog) niet geïmplementeerd in alle eenheden. De parel heeft betrekking op online criminaliteit (brede definitie) en op het proces bij de politie, van aangifte tot opsporing, of de bredere inzet van de politie in de preventie of bestrijding van online criminaliteit. Er wordt van een parel gesproken indien het een niet-incidenteel initiatief betreft. Ten slotte worden alleen initiatieven die nog lopen (actief zijn) aangemerkt als parel, zodat er een actueel overzicht ontstaat van de ontwikkelingen binnen de politieorganisatie.

Belangrijkste resultaten

In tabel 1 is een overzicht weergegeven van de 19 initiatieven die in het onderzoek zijn bestudeerd, uitgesplitst naar de politie-eenheid waarbinnen het initiatief plaatsvindt en de fase van het politiewerk waar het initiatief zich op richt. Gelet op de inhoud van de initiatieven, worden er verschillende activiteiten uitgevoerd om de beoogde doelen te bereiken. Ten eerste zijn er initiatieven die zich richten op preventie, welke proberen criminaliteit te voorkomen door middel van een externe samenwerking en de inzet van een escaperoom-bus. Zo wordt er in Limburg samengewerkt met de Risk Factory zodat burgers scenario's doorlopen op het gebied van online veiligheid en probeert het initiatief Bl@ckmail sextortion te voorkomen met behulp van een mobiele escaperoom waarin het gesprek wordt aangegaan met jongeren. Ten tweede zijn er twee initiatieven die zich uitsluitend richten op de opsporing van online criminaliteit. De oprichting van districtelijke cybercrimeteams binnen de districtsrecherche moet daaraan bijdragen. Ten derde proberen de kennis en kunde initiatieven kennis bij te brengen bij politiemedewerkers door middel van escaperooms, fictieve casussen, CTF-challenges, workshops, klassikale lessen en de inzet van een digitale trainingsstraat. De kennis die wordt overgedragen betreft alle onderdelen van het politieproces: het opnemen van aangiften, case screening, digitale opsporingsmogelijkheden, virtuele doorzoekingen, open bronnen onderzoek en het indienen van vorderingen bij bedrijven. Tot slot zijn er initiatieven die zich direct richten op meerdere fasen van het politiewerk tegelijkertijd. Deze initiatieven proberen hierop in te spelen door bijvoorbeeld speciale teams

op te richten die zelf operationeel actief zijn of ondersteuning bieden aan operationele teams. De oprichting en wijze waarop de teams zijn vormgegeven laten zien dat er binnen de verschillende eenheden behoefte is aan (samenwerking tussen) verschillende expertisen. Ook wordt er van buiten de politieorganisatie expertise ingevoegd door bijvoorbeeld de inzet van cybervrijwilligers en IT-coaches. Andere initiatieven die zich op meerdere fasen richten proberen door externe samenwerking bij te dragen aan geformuleerde doelen. Zo zijn er in Zeeland-West-Brabant in een 'cyberdriehoek' structurele overleggen en zijn er overleggen tussen vitale partnerorganisaties in Breda om informatie en kennis met elkaar te delen.

Bevorderende en belemmerende factoren

Respondenten geven bij de helft van de initiatieven aan dat betrokkenen enthousiast, gemotiveerd en energiek zijn. Het gaat dan om enthousiasme onder mensen die (zowel intern als extern) een rol vervullen bij de uitvoering van het initiatief, maar ook om enthousiaste deelnemers van bijvoorbeeld trainingen en workshops. Er lijkt een verband met het hebben van een gezamenlijke doelstelling (n=4). Dit leidt weer tot (een proactieve) samenwerking met partners (n=4). Een andere factor die wordt genoemd is het commitment vanuit de politieorganisatie en de ruimte die projectleiders krijgen om te experimenteren en te leren (n=3). Ook wordt volgens de respondenten de hulp die door de initiatieven wordt geboden – bijvoorbeeld in de vorm van IT-coaches of leden van het cyber support team – goed ontvangen door politiemedewerkers (n=3). Ten slotte worden verschillende positieve effecten gehoord in relatie tot de initiatieven. Zo is volgens respondenten bij het VIN-fraude project de kwaliteit van de aangifte hoger geworden en is er meer kennis over het fenomeen, is er door het Digitaal District een plek gecreëerd waardoor meer initiatieven mogelijk zijn en leggen deelnemers tijdens de KOR3NWOLF casus elkaar spontaan dingen uit.

Belemmerende factoren worden ook genoemd. Wat betreft een minder goed verloop van de initiatieven valt op dat dit voor verschillende projecten de andere kant van dezelfde munt lijkt te zijn. Er zijn namelijk ook juist afdelingen of personen binnen de politieorganisatie die minder ontvankelijk en conservatiever zijn in relatie tot digitalisering en online criminaliteit (n=5). Zo wordt opgemerkt door respondenten dat enkele afdelingen nog afstand behouden tot digitale thema's en dat sommige medewerkers tijdens trainingen een minder open houding hebben ten aanzien van het thema en daardoor passiever zijn. In relatie tot deze bevinding wordt opgemerkt dat de 'klassieke agenda' (m.a.w. traditionele criminaliteit) uiteindelijk vaak voorrang krijgt op de problematiek rondom online criminaliteit (n=2). Andere belemmeringen zijn dat, ondanks dat men bij enkele initiatieven tevreden is over het commitment vanuit de politieorganisatie, er ook respondenten zijn die aangeven dat er te weinig capaciteit beschikbaar is om het project naar volledigheid uit te kunnen voeren (n=4). Als laatste blijkt dat er soms bij trainingen een betere afstemming nodig is op het niveau van medewerkers (n=2) en dat er behoefte is aan beter verwachtingsmanagement richting betrokken politiemedewerkers rondom de initiatieven (n=2).

Het behalen van doelstellingen

Een groot deel van de initiatieven (n=14) blijkt een vorm van evaluatie te hebben ingebouwd. Het gaat dan vooral om evaluaties die de politie zelf uitvoert. Zo worden er evaluatiegesprekken gevoerd en evaluatieformulieren uitgedeeld aan deelnemers en betrokkenen, zodat feedback wordt verkregen en aanpassingen mogelijk zijn. In de eenheid Zeeland-West-Brabant wordt verwezen naar een monitor cybercrime, die op kwalitatieve en kwantitatieve wijze bijhoudt welke resultaten er binnen de eenheid worden geboekt op het gebied van online criminaliteit (ook in relatie tot de initiatieven).

Er kunnen enkele kritische kanttekeningen worden geplaats bij de wijze waarop de initiatieven worden geëvalueerd. Zo wordt vaak maar een deel van het initiatief geëvalueerd, krijgen sommige nulmetingen geen vervolg en betreffen de evaluaties doorgaans geen (wetenschappelijke) effect-evaluaties. Een aantal initiatieven (n=4) heeft een evaluatie laten uitvoeren door een externe organisatie. Voorbeelden van deze organisaties zijn onderzoeksinstellingen, een consultancy bureau en een universiteit. Ten slotte blijkt dat een deel van de initiatieven (n=6) niet (stelselmatig) bijhoudt of de doelstellingen worden behaald. Verklaringen die hiervoor worden gegeven zijn bijvoorbeeld dat er geen capaciteit voor is of dat men in de opstartfase zit van het project.

Enkele observaties

Initiatieven richten zich vooral op kennis en vaardigheden van politiemedewerkers

Ten eerste valt het op dat er relatief veel initiatieven geïdentificeerd zijn die zich richten op bewustwording en ontwikkeling van vaardigheden en kennis bij politiemedewerkers. In principe zijn deze initiatieven natuurlijk een goede ontwikkeling. Uit dit onderzoek blijkt immers dat er behoefte is vanuit politiemedewerkers aan deze kennis voor de uitoefening van het werk. Daarnaast pleit eerder onderzoek voor kennisverbetering met betrekking tot verschillende onderdelen van het politiewerk in de aanpak van online criminaliteit (Leukfeldt et al., 2012; Huisman et al., 2016; Boekhoorn, 2019) en zijn dergelijke doelstellingen ook opgenomen in strategische en beleidsmatige doelstellingen van de politieorganisatie. Maar blijkbaar is de behoefte aan meer kennis en kunde in de praktijk erg groot. Tijdens de discussiebijeenkomst die na dit onderzoek heeft plaatsgevonden, concluderen ook experts dat het gebrek – en de behoefte - aan kennis en kunde op het gebied van online criminaliteit al geruime tijd aanwezig is in de politieorganisatie. De politieorganisatie is hierin echter niet alleen. Ook andere opsporingsdiensten zoals de Koninklijke Marechaussee ervaren een gebrek aan kennis en kunde op het gebied van digitalisering. Gezien de snelle ontwikkelingen op het gebied van online criminaliteit verdient het volgens experts dan ook de aanbeveling om verder te investeren op kennis en kunde omtrent online criminaliteit en vooral ook om deze kennis up-to-date te houden door continue bijscholing.

Een tweede aspect dat opvalt is dat initiatieven zich ook richten op verbeteringen binnen het proces van opsporing.

Voorbeelden zijn de ‘aanpak geldezels’ en het ‘project VIN-fraude’. Dit is niet nieuw. Het LMIO bestaat bijvoorbeeld al enkele jaren en ook het ECTF heeft een soortgelijke functie. Wel is duidelijk dat de impact van digitalisering op criminaliteit groot is. De politie krijgt steeds meer te maken met nieuwe vormen van gedigitaliseerde criminaliteit waarbij aangiftes uit het hele land komen. Het verdient dan ook de aanbeveling om de aanpak of werkvoorbereiding van dit soort nieuwe fenomenen landelijk aan te sturen, zodat kennis op een centraal punt kan worden ontsloten en lokale opsporingsteams beter in stelling kunnen worden gebracht om de zaken op te pakken. Waar mogelijk door samenwerking met externe partners, aangezien burgers vaak melding doen bij deze organisaties (Van de Weijer et al., 2019) en zij over een goede informatiepositie beschikken. Uiteraard is dan ook beleid nodig met betrekking tot het daadwerkelijk oppakken van zaken die centraal voorbereid zijn en vervolgens in diverse eenheden worden uitgezet.

Verandering in de opsporing

Met de toename van online criminaliteit – en dus ook het dagelijkse werkaanbod van politiemedewerkers – kunnen de in dit onderzoek geïdentificeerde initiatieven in de context van een bredere transitie worden geplaatst. Eerder onderzoek naar verandering binnen de politieorganisatie laat zien dat de politie in haar structuur en cultuur normaliter vaak ‘opmerkelijk resistent’ is tegen dergelijke veranderingen (Landman et al., 2020). De bevindingen van onderhavig onderzoek hieromtrent zijn tweeledig. Enerzijds wordt door initiatiefnemers opgemerkt dat er vaak enthousiast wordt gereageerd op de initiatieven door deelnemers (vaak politiemedewerkers) en betrokkenen bij de uitvoering (politiemedewerkers of externe organisaties). Ook leidinggevenden geven ruimte om aan de slag te gaan met de initiatieven. Anderzijds wordt echter ook gezien dat er verschillende onderdelen en medewerkers weerstand vertonen ten opzichte van (projecten op het gebied van) online criminaliteit en digitalisering.

In het recente onderzoek van Landman et al. (2020) wordt benadrukt dat het van belang is om weerstand tegen verandering onder politiemedewerkers te begrijpen in de context van de politieorganisatie. Factoren omtrent deze context zijn bijvoorbeeld de ‘blauwe identiteit’, de werking van het strafrechtsysteem en de organisatiestructuur binnen de politie. De invloed van innovatieve projecten en trainingen kan worden geremd of teniet gedaan worden door het bredere institutionele en organisatorische systeem waarin politiemedewerkers werken. Verandering dient volgens de auteurs dan ook plaats te vinden middels een strategie van twee sporen: enerzijds door lokale leeromgevingen te organiseren en anderzijds door aanpassingen te verrichten in het systeem en de organisatie. De parel digikamers in Zeeland-West-Brabant illustreert de werking van deze strategie goed: begonnen in een basisteam, uitgegroeid tot een organisatorische verandering binnen de eenheid en tegelijkertijd ook een omgeving die op lokaal niveau weer innovatieve projecten stimuleert. Ook het CyberHQ en Digitaal District zijn voorbeelden waarbij aanpassingen in de organisatiestructuur kunnen leiden tot een omgeving waar meer (verandering) mogelijk is. In deze teams ontstaat namelijk ruimte voor innovatieve projecten die hun uitwerking hebben op de rest van de eenheid.
In het kader van verdere implementatie van de geïdentificeerde projecten geven experts tijdens de discussiebijeenkomst aan dat er niet zozeer hooggespannen verwachtingen hoeven te zijn over een landelijke implementatie van projecten. Lokale of regionale behoeften en projecten hoeven namelijk niet per definitie voor de hele politie te gelden, aangezien er geen garantie is dat op andere plekken hetzelfde enthousiasme of dezelfde resultaten worden behaald rondom een project. De winst van dergelijke initiatieven zou er volgens experts vooral in moeten zitten dat men op lokaal of regionaal niveau bezig is met digitalisering en online criminaliteit. Lokale en regionale initiatieven dienen dan ook vooral een functie te hebben in de verspreiding van kennis en verdere enthousiasmering op het thema. Het huidige rapport kan in die zin functioneren als inspiratie voor andere eenheden en verdere verspreiding stimuleren.

Weinig bekend over de werking van initiatieven

Dit rapport laat zien dat er weinig bekend is over de werking van de initiatieven. Er zijn weliswaar positieve geluiden en voorbeelden, maar concrete effectevaluaties blijven grotendeels uit. Dit is enerzijds begrijpelijk, aangezien de politieorganisatie andere doelstellingen en prioriteiten heeft die met een beperkte capaciteit moeten worden aangevlogen. Anderzijds zorgt de beperkte capaciteit er ook voor dat de middelen op een effectieve wijze ingezet dienen te worden. Het verdient dan ook de aanbeveling om meetbare doelen te formuleren en vervolgens effectevaluaties of mimimaal plan- en procesevaluaties uit te voeren. Experts adviseren hierbij om in te zetten op kleine effecten die de politie zelf kan meten. Denk aan bijvoorbeeld een kennismeting (voor- en nameting), het aantal activiteiten dat men rondom een project verricht of het aantal opsporingsonderzoeken dat wordt opgepakt omtrent een fenomeen. Het verdient ook de aanbeveling om politiemedewerkers hierin te ondersteunen, bijvoorbeeld door een handleiding voor evaluaties op te stellen.

Inhoud

1. Inleiding

1.1 Achtergrond

Met de digitalisering van onze samenleving krijgen steeds meer delicten een digitale component. Dergelijke delicten worden ook wel aangeduid als online criminaliteit. Onder deze noemer vallen tal van delicten, bijvoorbeeld het inbreken in een computer van een ex-partner, het platleggen van de website van een school middels een DDoS-aanval, maar ook het plegen van fraudes via online verkoopsites (Leukfeldt et al., 2015). Delicten die gericht zijn op ICT en waarbij ICT van wezenlijk belang is voor de uitvoering ervan – zoals hacken – noemen we ook wel cybercriminaliteit of cyber dependent crime (McGuire & Dowling, 2013a). Delicten waarbij ICT alleen een rol speelt binnen de modus operandi noemen we gedigitaliseerde criminaliteit of cyber enabled crime (McGuire & Dowling, 2013b, Beerthuizen et al., 2020). Overigens maken criminelen zelf geen onderscheid tussen deze twee categorieën, zij gebruiken zowel offline als online methoden om hun doel te bereiken en omarmen de mogelijkheden die digitalisering hun biedt (Roks et al., 2020). Daarbij is te zien dat sommigen zich specialiseren in het plegen van cybercriminaliteit, terwijl anderen het gebruiken als uitbreiding van hun criminele repertoire en gedigitaliseerde vormen van criminaliteit plegen (Leukfeldt, 2016). Voor de leesbaarheid van dit rapport gebruiken we voor beide typen delicten de term ‘online criminaliteit’.

Online delicten zullen steeds vaker onderdeel worden van het dagelijkse werkaanbod van politiemedewerkers. Slachtofferschap van dergelijke delicten is nu al hoog en neemt met de steeds verdergaande digitalisering alleen maar toe (CBS, 2020). Dat “de wereld naar de wijk is gekomen” blijkt ook uit de Strategische Agenda Politieacademie 2018-2022 waarin “politiewerk verbonden met wijk, web en wereld” een belangrijke pijler is. Feitelijk is ‘digitaal’ nu ‘normaal’ geworden en krijgen politiemedewerkers door de hele organisatie heen met allerlei varianten van online criminaliteit te maken – op nationaal, regionaal en lokaal niveau. De aanpak van online criminaliteit heeft eerst op nationaal niveau (bijvoorbeeld met de oprichting van het Team High Tech Crime en het Dark Web Team) en later op eenheidsniveau (met de komst van de zogenaamde cybercrime teams) de laatste jaren vorm gekregen (Struiksma et al., 2012; Boekhoorn, 2019). Ook binnen de eenheden zijn allerlei initiatieven op het gebied van de aanpak van online criminaliteit. Op dit moment ontbreekt zicht op al deze regionale en lokale initiatieven. Onderhavig onderzoek beoogt om de ‘parels’ op regionaal en lokaal niveau te identificeren en te beschrijven. Dit levert enerzijds een beeld op van regionale en lokale initiatieven. Veelbelovende initiatieven kunnen dan in andere eenheden of op nationaal niveau worden geïmplementeerd. Anderzijds geeft de analyse ook een beeld waar het eigenlijk nog niet goed gaat of waar men op regionaal of lokaal niveau juist kansen ziet. De initiatieven zijn immers gestart om in een behoefte te voorzien of om het politiewerk te verbeteren. Een initiatief kan daarmee als een signaal worden gezien van de uitdagingen waar politiemedewerkers op de werkvloer mee te maken krijgen.

1.2 Onderzoeksdoel- en vragen

In dit onderzoek stellen we de initiatieven van de regionale en lokale aanpak van online criminaliteit centraal. Het onderzoek heeft tot doel om een overzicht te maken van veelbelovende initiatieven op het gebied van online criminaliteit, zodat eenheden van elkaar kunnen leren, zodat regionale en lokale initiatieven eventueel op grotere schaal kunnen worden ingezet, maar ook om inzicht te krijgen in de knelpunten binnen de aanpak van online criminaliteit. Welke initiatieven moesten worden opgezet om die aanpak te verbeteren?

Deze initiatieven op regionaal of lokaal niveau worden in dit rapport ook wel parels genoemd. Deze term zal eerst gedefinieerd worden. Met een parel wordt een regionaal of lokaal initiatief binnen de politie bedoeld, waarin de aanpak of preventie van online criminaliteit centraal staat. Een parel is op regionaal of lokaal niveau ontstaan, en is (nog) niet geïmplementeerd in alle eenheden. De parel heeft betrekking op online criminaliteit (brede definitie) en op het proces bij de politie, van aangifte tot opsporing, of de bredere inzet van de politie in de preventie of bestrijding van online criminaliteit. Er wordt van een parel gesproken indien het een niet-incidenteel initiatief betreft (dus niet eenmalig een cursusdag). Ten slotte worden alleen initiatieven die nog lopen (actief zijn) aangemerkt als parel[1], zodat er een actueel overzicht ontstaat van de ontwikkelingen binnen de politieorganisatie. Online criminaliteit en de bijbehorende politieprocessen zijn immers aan verandering onderhevig.
De onderzoeksvraag van dit onderzoek is tweeledig. Allereerst identificeren we regionale en lokale initiatieven. We nemen daarbij ook initiatieven mee die gezien worden als alternatieve interventies. Vervolgens wordt de inhoud van deze initiatieven onderzocht en gekeken in hoeverre de beschreven initiatieven in andere eenheden/regio's toepasbaar zijn. De onderzoeksvraag en -deelvragen van dit onderzoek zijn:

Welke initiatieven zijn er bij de regionale en lokale afhandeling van online criminaliteit?

Wat zijn de kenmerken van deze initiatieven?

a. Wat is de aanleiding geweest voor het initiatief?
b. Welke activiteiten worden er uitgevoerd binnen dit initiatief?
c. Wat is het doel van het initiatief?
d. Op welke vorm(en) van online criminaliteit richt het initiatief zich?
e. Hoe is het initiatief onderbouwd?
f. In hoeverre worden de gestelde doelen op dit moment al gehaald?
g. Hoe ziet de samenwerking met interne en externe stakeholders eruit?
h. Hoe verloopt de implementatie van het initiatief tot nu toe?
i. In hoeverre zijn de initiatieven toepasbaar binnen andere eenheden?

1 Met uitzondering van initiatieven die beperkt zijn in hun doorgang door COVID maatregelen.

1.3 Leeswijzer

Dit rapport over de parels in de regionale en lokale aanpak van online criminaliteit ziet er als volgt uit. Eerst geeft hoofdstuk 2 inzicht in de wijze waarop de aanpak van online criminaliteit binnen de politie is georganiseerd, op basis van literatuur en beleidsdocumenten. In hoofdstuk 3 wordt de methodische verantwoording van het onderzoek besproken, waaronder de wijze waarop de 'parels' in dit onderzoek zijn geïdentificeerd. Vervolgens worden de resultaten van het onderzoek weergegeven in hoofdstuk 4. De geïdentificeerde parels worden hier individueel besproken. Zo kan in hoofdstuk 5 antwoord worden gegeven op de eerder geformuleerde onderzoeksvragen. Het rapport eindigt met een discussie waarin de beperkingen en implicaties van het onderzoek aan bod komen.

2. De context: de organisatie van de bestrijding van online criminaliteit

In dit hoofdstuk wordt een overzicht gegeven van literatuur over de wijze waarop de aanpak van online criminaliteit binnen de politie is georganiseerd. Zo kunnen de initiatieven die in dit onderzoek worden geïdentificeerd in een bredere context worden begrepen. Eerst zal paragraaf 2.1 bespreken op welke wijze de aanpak van online criminaliteit is georganiseerd binnen de politieorganisatie. Vervolgens komt in paragraaf 2.2 de stafrechtelijke afhandeling van aangiften van online criminaliteit aan bod.

2.1 Aanpak online criminaliteit binnen de politie

Om inzicht te krijgen in de wijze waarop de politie online criminaliteit aanpakt, is inzicht nodig in de organisatiestructuur van de politie. Dat doen we hier heel beknopt. Er zijn drie verschillende niveaus te onderscheiden die met elkaar samenwerken: nationaal, regionaal en lokaal. Sinds de reorganisatie in 2013 is de politie onderverdeeld in tien regionale eenheden, een landelijke eenheid en een politiedienstencentrum (Politie, z.d.). Een regionale eenheid bestaat vervolgens uit enkele districten, waarin verschillende basisteams actief zijn. De bestrijding van online criminaliteit door de politie is op deze verschillende niveaus georganiseerd. Een compleet en recent overzicht van de verschillende plekken in de organisatie waar de politie zich bezighoudt met online criminaliteit ontbreekt echter tot op heden. Op basis van literatuur, enkele interne documenten van de politie en online openbare bronnen kan enkel een globaal beeld worden geschetst van de wijze waarop de aanpak[2] van online criminaliteit is georganiseerd.

Op landelijk niveau is in 2007 Team High Tech Crime (THTC) opgericht[3] dat zich bezig houdt met de aanpak van online criminaliteit die complex en van nationaal en internationaal belang is (Struiksma, Mestdagh & Winter, 2012). De kennis die THTC heeft delen zij op regionaal niveau met de cybercrimeteams om de bestrijding van cybercrime vorm te geven (Politie, 2018b). Naast THTC beschikt de Landelijke Eenheid over een Darkweb team, dat opsporingsonderzoeken verricht op het Darkweb (Politie, 2018a).

Uit het Voorstel Intensivering Aanpak Cyber (Politie, 2018b) blijkt dat landelijk geprioriteerde zaken en fenomeenonderzoeken worden verdeeld onder de regionale eenheden in het Landelijk Operationeel Cybercrime Overleg (LOCO). Het LOCO bestaat uit teamleiders van de regionale cybercrimeteams (zie volgende alinea) en THTC. Het Platform Intensivering Aanpak Cybercrime (PIAC) zorgt op landelijk niveau voor afstemming over de ontwikkelingen op het gebied van cybercriminaliteit en bestaat uit alle project- en teamleiders van de regionale cybercrimeteams. Verder zorgt het Expertisecentrum Cybercrime en Digitale Opsporing (ECDO) voor expertise voor het gehele digitale opsporingswerkveld, waar online criminaliteit onderdeel van uitmaakt.

De aanpak van online criminaliteit is op landelijk niveau ook belegd bij bestaande nationale diensten en initiatieven binnen de politie. Zo is het Landelijke Internationale Rechtshulp Centrum (LIRC), als centraal punt voor in- en uitgaande rechtshulpverzoeken van en naar het buitenland, een belangrijk punt voor de opsporing van grensoverschrijdende online criminaliteit. Andere diensten die op landelijk niveau zijn georganiseerd zijn backstopping en een keuringsdienst. Backstopping zorgt voor afschermingsproducten voor heimelijk werken (van panden tot aan legitimatiebewijzen) en de keuringsdienst keurt technische hulpmiddelen. Ten slotte zijn er diverse publiek-private samenwerkingen waar de Nationale politie deel van uitmaakt. Voorbeelden zijn de Electronic Crimes Taskforce (ECTF), het Nationaal Cyber Security Centrum (NCSC), het Digital Trust Center (DTC) en het Landelijk Meldpunt Internet Oplichting (LMIO) (Politie, 2018b; Boes & Leukfeldt, 2017). Ook werkt de Nationale politie op internationaal niveau samen met partners als Europol, Interpol en de FBI (Politie, z.d.).

Op regionaal niveau zijn in 2016 cybercrime teams opgericht voor drie regionale eenheden (Politie, 2016). De regionale cybercrime teams zijn onderdeel van de Dienst Regionale Recherche en dienen zich te richten zich op de opsporing, preventie, verstoring, signalering en advisering op het gebied van online criminaliteit. De cybercrimeteams richten zich vooral op cybercriminaliteit (Politie, 2018b), waarbij ICT zowel middel als doelwit is en van wezenlijk belang is voor de uitvoering van het delict. De regionale cybercrimeteams delen hun kennis op lokaal niveau met districtsrecherches en basisteams (Politie, 2017). Inmiddels beschikken alle regionale politie-eenheden over een cybercrimeteam. Uit het Voorstel Intensivering Aanpak Cyber (Politie, 2018b) blijkt dat de cybercrimeteams lokaal geprioriteerde zaken, landelijk geprioriteerde zaken en fenomeenonderzoeken op gaan pakken. De lokaal geprioriteerde zaken zullen worden opgepakt via de regionale stuur- en selectie tafels of in overleg met de regionale cybercrime Officier van Justitie.

Ten slotte worden op lokaal niveau opsporingsonderzoeken naar online criminaliteit verricht door de districtsrecherche en basisteams (Leukfeldt, Veenstra, Domenie & Stol, 2012). De districtsrecherche en basisteams zouden zich moeten richten op de aanpak van gedigitaliseerde criminaliteit (Politie, 2018b), waaronder wordt verstaan ‘alle vormen van traditionele criminaliteit die worden gepleegd met behulp van ICT, maar niet gericht zijn tegen ICT’. Verder zijn er op lokaal niveau digitale wijkagenten, die zich bezighouden met opsporing op het web (CCV, 2019). Ook worden initiatieven op gemeentelijk niveau opgestart. Zo is de politie in Breda in samenwerking met de gemeente en andere partners een opleiding gestart voor buurtambassadeurs cybercrime, die burgers weerbaarder moeten maken op internet (CCV, 2019). Er zijn dus verschillende lokale initiatieven voor de aanpak van online criminaliteit, maar een overzicht hiervan ontbreekt.

2 Onder ‘aanpak’ van online criminaliteit worden opsporing, verstoring en preventie van online criminaliteit verstaan.

3 THTC is opgericht als onderdeel van de Dienst Landelijke Recherche binnen de Landelijke eenheid van de politie.

2.2 Strafrechtelijke afhandeling van online criminaliteit binnen de politie

Zowel Leukfeldt en collega's (2012) als Boekhoorn (2019) bestudeerden de afhandeling van online criminaliteit door de politie. Opsporingsonderzoeken inzake online criminaliteit kunnen op twee manieren tot stand komen: door middel van haalzaken of brengzaken. Bij haalzaken start de politie op eigen initiatief, bijvoorbeeld aan de hand van intelligence, een onderzoek. Bij brengzaken dragen slachtoffers, benadeelden of getuigen zaken zelf bij de politie aan in de vorm van een melding of aangifte. In deze paragraaf wordt meer inzicht gegeven in de afhandeling van aangiften van online criminaliteit binnen de politie.

Eerder onderzoek heeft de strafrechtelijke afhandeling van online criminaliteit in kaart gebracht in 2012 (Leukfeldt et al., 2012). Het rapport concludeerde dat er ten tijde van het onderzoek een gebrek aan inzicht was in de doorstroom van aangiften cybercrime in de strafrechtketen. Er is sinds 2012 veel gebeurd. Zo waren ten tijde van het onderzoek de speciale cybercrimeteams op regionaal niveau nog niet opgericht. Een recent onderzoek van Boekhoorn (2019) geeft inzicht in de strafrechtelijke afhandeling van online criminaliteit binnen enkele regionale eenheden sinds de oprichting van de regionale cybercrimeteams. Op basis van beide onderzoeken wordt nu globaal het proces van slachtofferschap tot veroordeling van online criminaliteit geschetst.

Voordat delicten van online criminaliteit de strafrechtketen instromen moet er eerst sprake zijn van waargenomen slachtofferschap (Leukfeldt et al., 2012). Misdrijven waarvan geen slachtofferschap wordt waargenomen stromen doorgaans[4] niet de strafrechtketen in. Als er sprake is van waargenomen slachtofferschap kan een slachtoffer ervoor kiezen om aangifte te doen bij de politie. Om de aangiftebereidheid onder burgers te vergroten en het aangifteproces te vergemakkelijken heeft de politie een 'multichanelstrategie' ontwikkeld (Boekhoorn & Tolsma, 2016). De strategie houdt in dat er verschillende kanalen zijn waar slachtoffers aangifte kunnen doen, afhankelijk van het type delict. Aangifte kan worden gedaan via internet, telefonisch, op het politiebureau of op de locatie waar slachtofferschap van het delict plaats heeft gevonden.

De burger, het bedrijf of de organisatie dat de melding doet bij de politie komt zo in contact met een medewerker van Intake & Service (Boekhoorn, 2019). De intake-medewerkers bepalen vervolgens of een aangifte wel of niet wordt geregistreerd (Leukfeldt et al., 2012). Een intakemedewerker kan er bijvoorbeeld voor kiezen om een aangifte niet op te nemen omdat het verzoek van de burger niet tot de kerntaken van de politie behoort. Een knelpunt in de intake is dat men bij Intake & Service – zoals ook uit eerder onderzoek is gebleken (o.a. Toutenhoofd-Visser et al., 2009; Leukfeldt et al., 2012; Huisman et al., 2016) – relatief onbekend is met vormen van online criminaliteit (Boekhoorn, 2019). Hierdoor worden mogelijke cyberzaken niet herkend, is de kwaliteit van aangiften laag en ontbreekt belangrijke informatie in de aangifte.

4 Haalzaken uitgezonderd, zoals het oprollen van marktplaatsen op het darkweb (Politie, 2021).

Geregistreerde aangiften worden vervolgens beoordeeld door een zogenoemde case-screener (Leukfeldt et al., 2012; Boekhoorn, 2019). De case-screener beoordeelt of de opgenomen aangifte in behandeling wordt genomen en, zo ja, door welk team (Boekhoorn, 2019). Cybercrime-zaken kunnen worden toegewezen aan de Dienst Landelijke Recherche (DLR), Dienst Regionale recherche (DRR), districtsrecherche of basisteams (Van Bree et al., 2016). Criteria voor het in behandeling nemen zijn of de aangifte voldoende opsporingsindicatie bevat, beleidsindicatoren, juridische haalbaarheid en de verantwoordelijkheid van het slachtoffer (Leukfeldt et al., 2012). In een van de regionale eenheden is voor de case-screening een 'Cybercenter' ingericht dat zorgt voor de screening, veredeling en het vervolgens kant-en-klaar aanleveren van de cyberzaken aan de basisteams. In andere eenheden voltrekt de screening zich bij het Operationeel Coördinatie Knooppunt als onderdeel van de basisteams (Boekhoorn, 2019). Indien de aangifte in behandeling wordt genomen wordt deze eventueel verrijkt met opsporingsinformatie (Leukfeldt., 2012). Bij de verrijking van aangiften spelen naast case-screeners ook informatieanalisten van de Dienst Regionale Informatie Organisatie (DRIO) een rol (Boekhoorn, 2019).

Vervolgens worden geselecteerde aangiftes doorgestuurd naar een opsporingsteam (Leukfeldt et al., 2012). Gezien de beperkte capaciteit van opsporingsteams maken ook zij weer afwegingen om al dan niet een opsporingsonderzoek op te starten. Criteria die hierbij een rol spelen zijn de prioriteit van de zaak, de beschikbare capaciteit om de zaak op te pakken en de werkbelasting van de zaak. Wanneer een opsporingsonderzoek is afgerond wordt deze doorgestuurd naar het Openbaar Ministerie (OM).

De parketsecretaris van het OM beoordeelt het opsporingsonderzoek op juridische haalbaarheid (de kans op vervolging en/of veroordeling). De zaak wordt vervolgens teruggestuurd naar de politie of afgehandeld met behulp van de beschikbare afdoeningswijzen voor strafzaken. Een zaak kan worden geseponeerd, een strafbeschikking kan worden opgelegd, een transactie kan worden aangeboden en een zaak kan voor de rechter worden gebracht (Leukfeldt et al., 2012). Uit het recente onderzoek van Boekhoorn (2019) is gebleken dat er door het OM relatief vaak besloten wordt tot een (technisch) sepot en dat bij vervolging en sanctionering vaak zonder tussenkomst van de rechter een strafbeschikking wordt uitgedeeld of een transactie wordt aangeboden. In 2018 werd 50% van de totale instroom van cyberzaken bij het OM geseponeerd, en van de zaken waarin wel sprake is van strafvervolging was 60% OM-afdoeningen en 40% ZM-afdoeningen[5].

5 Afdoeningen via de rechter.

3. Methoden

Dit onderzoek richt zich op lokale initiatieven binnen de politie waarin de preventie, verstoring of opsporing van online criminaliteit centraal staat. In dit hoofdstuk worden de onderzoeksmethoden beschreven die gebruikt zijn ter beantwoording van de onderzoeksvragen.

3.1 Dataverzamelingsmethoden

De onderzoekseenheid van het huidige onderzoek betreft initiatieven binnen de politie op het gebied van online criminaliteit. Voor het onderzoek zijn drie kwalitatieve onderzoeksmethoden gebruikt: interviews, documentanalyse en een expertbijeenkomst. Interviews zijn gehouden met initiatiefnemers of personen die op andere wijze nauw betrokken zijn bij een initiatief. In aanvulling op de interviews zijn – indien beschikbaar voor de onderzoekers – relevante documenten betreffende de initiatieven geraadpleegd. Tot slot is een expertbijeenkomst gehouden om de resultaten van het onderzoek te duiden en om tot aanbevelingen te komen voor de politie.

3.2 Selectie van parels

Voor de selectie van initiatieven (en respondenten) is een combinatie van een doelgerichte- en sneeuwbalsteekproef gebruikt. Er is sprake van een doelgerichte steekproef omdat alleen initiatieven zijn geïncludeerd die voldoen aan de definitie van een parel (zoals geformuleerd in paragraaf 1.2). Er zijn drie verschillende wervingsmethoden gebruikt. Ten eerste is een oproep gedaan tijdens een PIAC-overleg (zie paragraaf 2.1) waar alle project- en teamleiders van de cybercrimeteams bij aanwezig waren. In de oproep is gevraagd om initiatieven – die voldoen aan de definitie van een parel – te melden bij de onderzoekers. Vervolgens zijn alle teamleiders van de cybercrimeteams in de verschillende eenheden nogmaals individueel benaderd met de vraag om relevante initiatieven aan te leveren. Ten slotte is tijdens interviews doorgevraagd naar andere initiatieven die bij respondenten bekend waren (sneeuwbalmethode).

In totaal zijn 37 initiatieven geïdentificeerd tijdens het onderzoek. Uit alle politie-eenheden is ten minste één initiatief gemeld, met uitzondering van de eenheid Noord-Holland. Uiteindelijk zijn 19 initiatieven geïncludeerd in het onderzoek. De overige initiatieven zijn afgevallen na een screening die plaatsvond op het moment dat de onderzoekers het initiatief ter kennis namen. Initiatieven die niet zijn geïncludeerd voldeden niet aan de criteria van een 'parel' of hadden teveel overlap met een eerder gemeld initiatief. Een alfabetische lijst van de geïncludeerde initiatieven is opgenomen in bijlage 1. In tabel 1 is een overzicht weergegeven van deze geïncludeerde initiatieven, uitgezet naar de eenheid en fase van het politiewerk waar de parel zich op richt. De tabel fungeert tevens als index om de initiatieven terug te vinden in dit rapport.

Tabel 1: Een overzicht van geïncludeerde initiatieven per politie-eenheid[1] en fase in het politiewerk

	Preventie	Aangifte	Opsporing	Kennis & kunde
1. Noord-Nederland				Cybercrisisoefening met BT
				Digitale vaardigheden Friesland
2. Oost-Nederland				IT-coaches district Twente
				Digitaal flexteam IJsselland
	Project Vriend in Nood-fraude			
3. Midden-Nederland	Digitaal District			
4. Amsterdam	Bl@ckmail			Cyber support team
				Workshop cybercrime
	Cyberspecials			
5. Den Haag	Cyberdriehoek			
6. Rotterdam		Aanpak geldezels		
7. Zeeland-West-Brabant			District cyberteams	
	Cyber HQ			
	Digikamers			
	Digitaal weerbaar Breda			
8. Limburg	Risk Factory			KOR3NWOLF
		Dagelijkse Cyberquery		

1 De politie-eenheden Noord-Holland en Oost-Brabant zijn niet opgenomen in dit overzicht omdat er geen (geschikte) parels zijn aangedragen.

3.3 Interviews

Voor de geselecteerde initiatieven zijn interviews afgenomen met initiatiefnemers of personen die op een andere manier nauw betrokken zijn bij het initiatief. Het doel van de interviews met initiatiefnemers was om een beter inzicht te krijgen in de plannen, onderbouwing en uitvoering van geïdentificeerde initiatieven. Er zijn gestructureerde interviews gehouden, waarbij de vragen grotendeels van te voren waren vastgelegd. De belangrijkste onderwerpen tijdens de interviews waren de 'beschrijving', 'onderbouwing', 'samenwerking' en 'implementatie' van het initiatief. Een volledig overzicht van de topics en interviewvragen is opgenomen in bijlage 2.

Er zijn in totaal 21 interviews afgenomen. Voor elk initiatief is steeds een interview gehouden, met uitzondering van een initiatief waar drie (korte) interviews zijn afgenomen. De keuze om slechts een interview af te nemen per initiatief komt voort uit de verkennende aard van het onderzoek. Het doel is immers om een indicatie te krijgen van de initiatieven en niet om deze grondig te evalueren. Bijna alle interviews hebben digitaal plaatsgevonden via Microsoft Teams. Een enkel interview heeft telefonisch plaatsgevonden. Alle interviews zijn opgenomen met toestemming van de respondenten. De interviews duurden gemiddeld 1 uur en 12 minuten en varieerden van 31 minuten tot 2 uur en 9 minuten. De meeste interviews vonden plaats met een persoon, een enkel interview vond plaats met twee of drie respondenten tegelijk om extra aanvullingen te geven. Na afloop zijn de interviews door de onderzoekers uitgetypt en verwerkt tot een verslag. De audio en video opnamen zijn na het uitwerken verwijderd. Het uiteindelijke verslag is ter validatie voorgelegd aan de respondenten. In een enkel geval zijn feitelijke onjuistheden gecorrigeerd op basis van de feedback van respondenten. De beperkingen van de gebruikte onderzoeksmethoden worden uitgebreid besproken in de conclusie en discussie (hoofdstuk 5).

3.4 Expertbijeenkomst

De resultaten van het onderzoek zijn tijdens een discussiebijeenkomst voorgelegd aan experts werkzaam bij de politie, de Koninklijke Marechaussee en in de wetenschap. Doel van de bijeenkomst was om de resultaten van het onderzoek te bediscussiëren, zodat implicaties en concrete aanbevelingen voor de politieorganisatie konden worden gedaan. De expertbijeenkomst duurde 1 uur en 15 minuten en vond online plaats via Microsoft Teams. Experts zijn geselecteerd via het netwerk van de onderzoekers en leden van de leescommissie. Het was van belang dat de experts in diverse werkvelden werkzaam waren en affiniteit hadden met het politiewerk, online criminaliteit of verandering binnen organisaties. Een overzicht van de deelnemers die aan de expertbijeenkomst hebben deelgenomen is opgenomen in bijlage 3 van dit rapport.

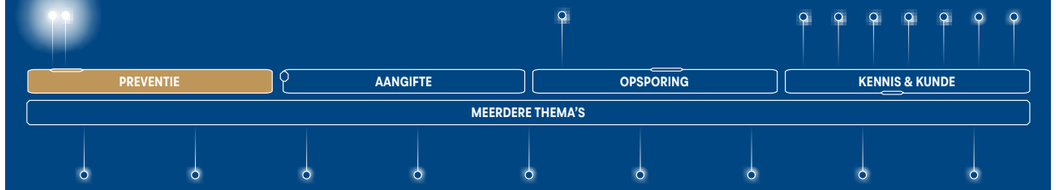
4. Resultaten

In dit hoofdstuk worden de resultaten van het onderzoek weergegeven in relatie tot de eerder geformuleerde onderzoeksvragen (zie paragraaf 1.2). Elk initiatief dat in dit onderzoek is geïncludeerd wordt apart besproken, vanuit het oogpunt van de respondent(en) die in relatie tot het initiatief zijn geïnterviewd. De volgorde waarin de initiatieven worden weergegeven is in lijn met de verschillende fasen van het politiewerk. Eerst worden initiatieven besproken met betrekking tot de preventie van online criminaliteit (paragraaf 4.1). Daarna gaan we in op initiatieven rondom de opsporing van online criminaliteit (paragraaf 4.2). Vervolgens bespreken we initiatieven die zich richten op de kennis en kunde van politiemedewerkers op het gebied van online criminaliteit (paragraaf 4.3). Het hoofdstuk sluit af met initiatieven die zich richten op meerdere fasen van het politiewerk (paragraaf 4.4).

4.1 Preventie

Er zijn in totaal twee initiatieven geïdentificeerd die zich uitsluitend richten op het voorkomen van online criminaliteit: 'BI@ckmail' en 'Samenwerking Risk Factory' (zie figuur 1). De initiatieven worden nu individueel besproken.

Figuur 1: initiatieven op het gebied van preventie van online criminaliteit



4.1.1 Bl@ckmail

Eenheid Amsterdam

Introductie

Het initiatief 'Bl@ckmail' bestaat uit een mobiele escaperoom waarin het gesprek kan worden aangegaan met jongeren over cybercrime en sextortion. De respondent is sinds 2016 werkzaam voor de eenheid Amsterdam als coördinator cybercrime. Deze functie valt onder de afdeling TDO (Team Digitale Opsporing) en het regionale cybercrimeteam.

Aanleiding

De eenheid heeft gekozen[6] verantwoordelijk te worden voor het fenomeen sextortion omdat de cyber officier van justitie dit een belangrijk onderwerp vond vanwege de impact die het delict heeft op jonge kwetsbare slachtoffers. Op het gebied van sextortion zijn binnen de eenheid Amsterdam verschillende werkgroepen georganiseerd, zo ook een werkgroep op het gebied van preventie. De Bl@ckmail escaperoom bus is een van de middelen die bij moet dragen aan de preventie van sextortion. Een collega van de afdeling communicatie heeft contact gehad met collega's uit de eenheid Rotterdam, waar een voormalige alcohol bus was omgebouwd tot escaperoom in het kader van de preventie van drugs. De bus is veel ingezet op evenementen en festivals. Zo kwam de communicatiemedewerker op het idee om hetzelfde concept toe te passen op sextortion.

Beschrijving project

Inhoud

Bl@ckmail is een mobiele escaperoom bus en bestaat uit vier korte spellen die gespeeld worden door de deelnemers. Het kan worden gezien als een middel om het gesprek aan te gaan met jongeren over cybercrime en sextortion. Er kunnen drie tot vier personen tegelijk in de escaperoom bus. Eerst krijgen de deelnemers in een korte briefing (5 minuten) informatie over de escaperoom, cybercrime en sextortion. Vervolgens gaan de jongeren de bus in. De escaperoom is binnen een kwartier uit te spelen en bestaat uit 4 spellen waarbij 4 codes moeten worden gevonden. Door slim te overleggen en goed te zoeken komen deelnemers in de bus tot de oplossing. Een van de spellen is digitaal memory (met social media logo's) een andere opdracht betreft met een UV-lamp op een scherm schijnen om codes naar voren te laten komen. Om het spel heen is een casus bedacht van een dame die wordt afgeperst met naaktbeelden. Het idee is dat als de deelnemers de 4 codes binnen de tijd vinden ze ervoor zorgen dat de foto's niet worden geüpload op internet.

Achteraf is er een briefing waarin begeleiders het gesprek aan gaan met jongeren over het onderwerp. Het plan is om wijkagenten, jeugdagenten of jongerenwerkers als begeleiders het gesprek te laten aangaan. Bij de opzet van het initiatief is een kerngroep betrokken waar naast de politie ook partners zoals het Openbaar Ministerie (OM), gemeenten, HelpWanted en Spiritcupido (heet tegenwoordig Levvel, hulporganisatie in Amsterdam) in zitten. Door corona is de bus nog niet concreet ingezet, wel zijn er twee pilots gedraaid. Er is een keer een proef-case geweest met een groep jongeren en ook voor collega's is de bus een keer ingezet.

Doel

Het doel van het project is het voorkomen van sextortion slachtoffers door het voeren van een preventiecampagne. Deze doelen zijn niet concreet vastgelegd.

Doelgroep

De escaperoom bus is bedoeld voor jongeren van 14 tot 24 jaar oud. Er zijn ook aanvragen vanuit de lagere school (groep 7 en 8), maar men vindt de bus meer geschikt voor een wat oudere leeftijd vanwege het onderwerp. Het rondsturen van naaktbeelden vindt volgens de respondent minder frequent plaats op de basisschool t.o.v. een middelbare school. Een oudere doelgroep zou kunnen, maar de huidige deelgroep is een kwetsbare doelgroep waar men zich op basis van cijfers over sextortion[7] en onderzoeken van bijvoorbeeld HelpWanted[8] op wil richten.

Niveau

Het project is gestart in de eenheid Amsterdam en de bus is van de eenheid Amsterdam. Verder is de bus ook voor andere eenheden beschikbaar en zijn er al aanvragen vanuit andere eenheden. Binnenkort wordt gekeken of de coördinatie van dit soort voertuigen landelijk onder de paraplu van het Mobiel Media Lab[9] kan komen te vallen.

Onderbouwing

Verwachte werking

Men verwacht dat de escaperoom bus bijdraagt aan de doelen omdat men gelooft in het principe van preventie. Ook onderzoeken ondersteunen het belang van preventie. Het fenomeen sexting[10] hoeft en zal volgens de respondent niet voorkomen worden, omdat dit hoort bij een gezonde seksuele ontwikkeling in de huidige tijd. Door gesprekken aan te gaan over het onderwerp kunnen jongeren wel bewust gemaakt worden van de mogelijke gevolgen en kunnen gevoelens van schaamte worden weggenomen. Verder is het project gebaseerd op cijfers vanuit de politieorganisatie waarin de prevalentie en kwetsbare doelgroepen van sextortion in kaart zijn gebracht. Daarnaast wordt verwezen naar de effectiviteit van 'serious gaming'

6 Elke politie-eenheid is verantwoordelijk voor een specifiek cybercrime fenomeen. Politie-eenheden konden volgens de respondent uit een lijst van fenomenen zelf aangeven met welk fenomeen ze aan de slag wilden gaan.

7 De cijfers komen van analisten binnen de informatieorganisatie van de politie.

8 Helpwanted.nl is een website over online seksueel misbruik van kinderen en jongeren tot 26 jaar en onderdeel van het Expertisebureau Online Kindermisbruik.

9 Het Mobiel Media Lab is een vrachtwagen van de politie die door Nederland rijdt en gebruikt wordt als onderzoeksruimte om ervaringen en meningen van burgers te achterhalen.

10 Sexting betreft het versturen van seksueel getinte of pikante foto's of video's, vaak via een mobiele telefoon.

elementen om mensen iets te laten leren. Ten slotte is het concept gebaseerd op het voorbeeld uit Rotterdam. Hierover ontving men positieve berichten, onder andere dat deelnemers erg enthousiast waren.

Bijhouden werking
Er wordt op dit moment niet bijgehouden of de doelen worden bereikt. Het project is nog in de startfase, door corona kon de bus namelijk nog niet in worden gezet. De respondent vindt het interessant om te kijken hoe in de toekomst meetbaar gemaakt kan worden of de doelen van het initiatief worden bereikt. Wel geeft de respondent aan dat dit iets is waar binnen de politie minder aandacht voor is en dat preventie uiteindelijk lastig is om te meten.

Verdere onderbouwing
Men geeft aan dat het project nog concreter kan worden opgezet met een projectplan. Verder zou men de bus graag door verschillende collega's onder verschillende doelgroepen willen inzetten om te kijken wat werkt.

Samenwerking

Er vindt samenwerking plaats met verschillende interne en externe betrokkenen:
- Intern (binnen de politie): Wijk- en jeugdagenten, communicatiemedewerker en de afdeling EPJO[11]
- Extern (buiten de politie): Openbaar Ministerie (OM), gemeenten, jongerenwerkers, scholen, Helpwanted en Levvel[12]
.

Wijk- en jeugdagenten zijn betrokken omdat zij uiteindelijk de escaperoom kunnen begeleiden en het gesprek met de jongeren aan kunnen gaan. Het idee is dat de bus ook bij jongerenwerkers wordt neergezet en dat jongerenwerkers ook het gesprek aangaan met jongeren. Met scholen is contact om te kijken of de bus daar kan worden ingezet. HelpWanted en Levvel hebben ervaringsdeskundigen die af en toe wat komen vertellen en die de escaperoom hebben getest. Het OM, gemeenten en jongerenwerk zijn betrokken bij kerngroep overleggen rondom dit thema, waar de escaperoom bus wordt besproken.

Afspraken
Er zijn geen concrete afspraken gemaakt rondom de escaperoom bus. Wel zijn er afspraken over het kerngroep overleg over sextortion. De duur van de samenwerking is nog onduidelijk, wel is de intentie uitgesproken binnen de kerngroep om door te gaan met de overleggen, maar minder frequent (voorheen 8, nu 4 keer per jaar) omdat men elkaar inmiddels weet te vinden.

Kwaliteit samenwerking
De kwaliteit van de samenwerking wordt door de respondent als prettig en goed omschreven, omdat iedereen hetzelfde doel voor ogen heeft. Verder kan gebruik worden gemaakt van het netwerk van partners zoals Levvel om binnen te komen bij scholen. Het zijn daarnaast geen commerciële partijen die een ander belang hebben. Een verklaring voor de goede samenwerking is dat iedereen de ernst en impact van het onderwerp inziet. Daarnaast hoeft men geen informatie uit te wisselen over individuen, waardoor geen convenanten nodig zijn.

Verbeterpunten samenwerking
Zodra er meer mogelijk is en de corona maatregelen worden afgebouwd zou men graag meer concrete afspraken willen maken over bijvoorbeeld gezamenlijke inzet van de bus op evenementen.

Implementatie praktijk

Het initiatief is op verschillende punten (nog) niet vormgegeven zoals men dit heeft beoogd, omdat een en ander noodgedwongen moest worden bijgesteld. In eerste instantie was het idee om op grote evenementen en festivals te gaan staan met de bus, maar dit moest worden bijgesteld door corona. Vervolgens wilde men bij scholen gaan staan, maar vanwege de beperkte capaciteit (3 à 4 personen tegelijk) probeert men nu te kijken of de bus niet beter bij jongerenorganisaties kan worden ingezet. Aanpassingen die zijn gemaakt aan de escaperoom zelf zijn bijvoorbeeld de duur (eerst 20 minuten, later 15 minuten), het aantal personen (eerst 5, nu 3 à 4) en een partytent die is toegevoegd aan de bus omdat de bus te klein is om de briefing in de bus te houden. Aanpassingen zijn gemaakt aan de hand van de proefcases die hebben plaatsgevonden.

Op dit moment zijn goede punten van het initiatief volgens de respondent het enthousiasme onder mensen die de bus in moeten gaan zetten en het enthousiasme onder de doelgroep tijdens de proefcases.

Implementatie schaal & intensiteit
De respondent zou graag zien dat het initiatief op grotere schaal kan plaatsvinden. Op dit moment kunnen slechts 3 à 4 personen in de bus, waardoor het bijvoorbeeld lastig is om gehele klassen of scholen de escaperoom in een korte tijd te laten spelen.

Toekomstplan
In de toekomst hoopt men ten eerste dat de bus zoveel mogelijk ingezet kan worden. Daarnaast zou men graag bij het Mobiel Media Lab willen aanhaken zodat het initiatief gemakkelijk landelijk uit te rollen is en zodat er een gezamenlijke inzet plaats kan vinden (bussen naast elkaar en dan bijvoorbeeld bespreken in het mobiel media lab). Verder zou men de bus graag willen inzetten bij jongerenwerkers.

Toepasbaarheid andere eenheden
De bus kan worden ingezet in andere eenheden. Men heeft namelijk financiële middelen gekregen op de voorwaarde dat de bus ingezet kon worden binnen andere eenheden. Om de bus in te kunnen zetten is wat documentatie nodig en een gesprek met de initiatiefnemers voor toelichting. Het doel is om ervoor te zorgen dat de mobiele escaperoom door iedereen laagdrempelig kan worden ingezet.

11 EPJO (educatie programma jongeren) is onderdeel van de politie en wordt omgeschreven als een interactief schoolprogramma gericht op misdaadpreventie. Vanuit dit programma worden lessen op school gegeven door heel het land.

12 Levvel is een organisatie die specialistische hulp (zoal opvoedondersteuning, specialistische jeugdhulp en complexe psychiatrische zorg) biedt voor jongeren en gezinnen in lastige situaties.

4.1.2 Samenwerking Risk Factory

Eenheid Limburg

Introductie

In dit project werkt het cybercrimeteam van de eenheid Limburg samen met de Risk Factory. Hierbij worden scenario's ontwikkeld op het gebied van online weerbaarheid om slachtofferschap onder verschillende doelgroepen te voorkomen. Er is gesproken met vier respondenten. Twee respondenten zijn op dit moment betrokken bij het project en werken als operationeel expert en accountmanager publiek-private samenwerking bij het cybercrimeteam. De derde respondent was betrokken bij de opstart van het project en was toentertijd als rechercheur werkzaam bij het cybercrimeteam. Ten slotte is gesproken met een respondent die vanuit zijn functie als operationeel expert de brede samenwerking tussen de politie en Risk Factory heeft opgestart.

Risk Factory

De Risk Factory is een initiatief van de veiligheidsregio Limburg-Noord, waarbij kinderen en senioren risico's beleven op het gebied van gezondheid en veiligheid en leren hoe in deze situaties te handelen. De eerste Risk Factory is geopend in Twente, de tweede is geopend in Limburg-Noord en inmiddels is er ook een geopend in Brabant.

Vanuit de politie is men een samenwerking aangegaan (in de vorm van een convenant), waarbij de politie meedenkt en helpt bij het ontwikkelen van scenario's. Per onderwerp wordt bekeken welke expertise vanuit de politie naar voren geschoven kan worden.

Aanleiding

Een van de respondenten hoorde dat er een Risk Factory in Limburg-Noord was geopend en dat online risico's (zoals pesten en online gedrag) voor kinderen aan bod kwamen. Toen heeft de respondent binnen het cybercrimeteam besproken of de politie hier een bijdrage aan kon leveren, omdat men zicht heeft op de ontwikkelingen op het gebied van cybercriminaliteit. Ook kon de politie hiermee inspelen op preventie, een van de pijlers waar het cybercrimeteam zich op richt. Uiteindelijk is contact opgenomen met de projectleider van de Risk Factory en zijn afspraken gemaakt over de wijze waarop het cybercrimeteam van de politie iets kon betekenen. Tussen 2018 en 2019 is men vanuit het cybercrimeteam aangehaakt bij de Risk Factory.

Beschrijving project

Inhoud

Het initiatief bestaat uit een samenwerking tussen het cybercrimeteam van de politie-eenheid Limburg en de Risk Factory. De Risk Factory[13] is een initiatief van de veiligheidsregio Limburg-Noord[14], waarbij kinderen en senioren risico's beleven op het gebied van gezondheid en veiligheid en leren hoe zij moeten handelen in deze situaties.

Bij de Risk Factory worden scenario's gespeeld door diverse leeftijdsgroepen. Tijdens de interviews was de Risk Factory tijdelijk gesloten vanwege de corona-maatregelen. In de samenwerking op het gebied van cybercriminaliteit is de politie op verschillende manieren betrokken: (1) bij de ontwikkeling van scenario's, (2) het bijhouden van de actualiteit van de scenario's en (3) meelopen en behoeften in kaart brengen.

Er zijn sinds de samenwerking twee scenario's op het gebied van online weerbaarheid ontwikkeld waar de politie bij betrokken is geweest. Een eerste scenario is ontwikkeld voor senioren. Vanuit de politie heeft men gekeken welke delicten veel voorkomen op basis van meldingen en aangiften. Toen is gekozen voor een scenario over online oplichting (via nep-betaalverzoeken en vriend in nood-fraude). Men heeft voor het scenario een computerprogramma laten ontwikkelen. Tijdens dit programma melden deelnemers zich aan op een tweedehandswebsite en worden zij spelenderwijs op risico's gewezen. Zo wordt besproken welke gegevens mensen op internet achterlaten en worden de deelnemers tijdens het programma benaderd door een oplichter voor de verkoop van een product. Senioren worden zo wegwijs gemaakt om gezond om te gaan met internet. Een tweede scenario gaat over sexting en is bedoeld voor jongeren. Tijdens het scenario bevindt de deelnemer zich op school en wordt diegene geconfronteerd met de verspreiding van naaktfoto's onder klasgenoten. Onderwerpen zoals groepsdruk en hulpverleningsinstanties worden tijdens het scenario besproken.

Een tweede rol die men vervult is het bijhouden of de informatie tijdens de scenario's nog actueel is. Zo was er een ander scenario op het gebied van online veiligheid dat is overgenomen van de Risk Factory Twente, waarbij men gekeken heeft of de informatie actueel is en aanbevelingen heeft gedaan. Ten slotte heeft een van de respondenten een avond georganiseerd voor begeleiders van de scenario's, waarin is gekeken waar de behoeften bij begeleiders zitten en informatie is gegeven over de onderwerpen in de scenario's. Ook wil men kijken waar de behoeften bij de doelgroepen liggen, door een keer mee te draaien tijdens een scenario.

Doel

Als overkoepelend doel van de Risk Factory is de bewustwording op het gebied van positieve gezondheid en veiligheid opgenomen in een convenant. Specifiek vanuit het cybercrimeteam van de politie is het doel om bij te dragen aan de preventie van cybercriminaliteit. Een ander doel dat wordt genoemd is mensen bewust maken van de risico's die er op het internet bestaan.

Doelgroep

De doelgroep van de Risk Factory op het gebied van online veiligheid zijn op dit moment kinderen (uit groep 8) en ouderen. In de toekomst wil men de doelgroep uit gaan breiden met arbeidsmigranten, scholieren en speciaal onderwijs.

Niveau

Er is een verschil tussen het verzorgingsgebied van de Risk Factory en het cybercrimeteam. De Risk Factory is een initiatief

13 Zie www.riskfactorylimburgnoord.nl voor meer informatie over de Risk Factory.

14 De Veiligheidsregio Limburg-Noord is een samenwerkingsverband tussen deelnemende gemeenten en erop gericht om inwoners en bezoekers van Noord- en Midden-Limburg beter te beschermen tegen (gezondheid)risico's, rampen en crises (zie https://www.vrln.nl/ voor meer informatie).

van veiligheidsregio Limburg-Noord en het cybercrimeteam van de politie werkt op eenheidsniveau vanuit heel Limburg. De doelgroep van de Risk Factory is daarom in principe inwoners uit Limburg-Noord. Echter zijn er inmiddels ook overeenkomsten gesloten met seniorenorganisaties die actief zijn in heel Limburg.

De scenario's richten zich op zowel cybercriminaliteit in enge zin als meer gedigitaliseerde vormen van criminaliteit. Nu gaat het om de delicten online oplichting, betaalverzoekfraude en sextortion. Men geeft echter aan dat online criminaliteit dusdanig snel ontwikkeld dat indien een ander onderwerp actueler is men op een nieuw onderwerp in kan gaan spelen.

Onderbouwing

Verwachte werking

Er zijn verschillende verwachtingen die men heeft waarom de samenwerking met de Risk Factory een manier is om bij te dragen aan de preventie van cybercriminaliteit. Ten eerste is het een manier waarbij mensen risico's kunnen ervaren in een veilige omgeving waar mensen niet echt slachtoffer worden. Daarnaast gaan er grote groepen naar de Risk Factory, waardoor op een relatief makkelijke manier veel mensen bereikt kunnen worden. Ook worden er binnen de Risk Factory meerdere onderwerpen tegelijk behandeld (ook brandveiligheid, pestgedrag, persoonlijke verzorging etc.) waardoor mensen niet alleen op gebied van online weerbaarheid scenario's doorlopen, wat volgens een van de respondenten anders wellicht minder aanslaat. Ten slotte is er bewust voor gekozen om alleen aandacht te geven op actuele vormen van cybercriminaliteit, omdat mensen niet teveel tegelijk aangeboden dient te worden, wat anders niet blijft hangen en niet in het programma past. Verder is er volgens de respondent vanuit de Risk Factory samen met de universiteit Nijmegen onderzoek gedaan waaruit blijkt dat de doelgroep het best bereikt wordt door ze te laten ervaren. De Risk Factory is er daarom op gericht om mensen te laten ervaren wat veiligheid is. Met sextortion spelen kinderen bijvoorbeeld een spel om te ervaren wat het is en ouderen plaatsen een advertentie op de computer.

Bijhouden werking

Vanuit de politie zijn geen SMART geformuleerde doelstellingen bepaald in relatie tot het initiatief. Dit is volgens de respondent zo omdat de politie vooral een adviserende functie vervult en geen capaciteit of middelen hiervoor heeft vrijgemaakt. Verder wordt opgemerkt dat het onderzoekstechnisch lastig is om te meten in hoeverre het brengen van kennis vanuit de politie uiteindelijk bijdraagt aan de preventie van slachtofferschap of aan weerbaarheid. Vanuit de veiligheidsregio Limburg-Noord wordt wel in samenwerking met de Radboud Universiteit bekeken in hoeverre de Risk Factory bijdraagt aan de veiligheid in Limburg-Noord.

Samenwerking

De samenwerking tussen verschillende partners die zijn betrokken bij de Risk Factory is formeel vastgelegd in een convenant, waar ook de politie deel van uitmaakt. De volgende partners spelen een rol in de samenwerking:

- Intern (binnen de politie): cybercrimeteam, analisten, wijkagenten, afdeling zeden, afdeling communicatie en leidinggevenden.
- Extern (buiten de politie): de veiligheidsregio Limburg-Noord, vrijwilligers van de Risk Factory, universiteiten (zoals Radboud Universiteit), ouderenverenigingen, een IT-bedrijf, scholen, Gemeentelijke Gezondheidsdiensten, de brandweer, het Vincent van Gogh instituut, Regionaal Orgaan Verkeersveiligheid Limburg, Crisisbeheersing, provincie Limburg en het Vincent van Gogh instituut.

Vanuit de politie zijn op dit moment de twee respondenten betrokken vanuit het cybercrimeteam. Verder hebben medewerkers van de afdeling zeden ook input geleverd voor het sextortion scenario. Ook zijn er analisten voor informatie over veelvoorkomende aangiften en meldingen onder de doelgroepen en maken wijkagenten aan de doelgroepen kenbaar dat er een Risk Factory is. Extern zijn universiteiten betrokken voor onderzoek en ontwikkeling, ouderenverenigingen om deelnemers te werven, de provincie Limburg voor een deel van de financiering en de veiligheidsregio als initiatiefnemer van het project. Andere organisaties zijn betrokken bij de ontwikkeling van de scenario's door kennis te leveren vanuit hun specifieke expertise.

Afspraken

Afspraken zijn gemaakt op basis van convenanten tussen verschillende partners die bij de Risk Factory betrokken zijn, zoals de politie, GGZ (Geestelijke gezondheidszorg) en de AMBO (Algemene Nederlandse Bond voor Ouderen). Het convenant wordt voor een aantal jaar opgesteld en kan steeds worden verlengd.

Kwaliteit samenwerking

Er wordt vooral samengewerkt met de projectleider vanuit de Veiligheidsregio, wat door alle respondenten als een prettige samenwerking wordt omschreven. Redenen voor deze prettige samenwerking zijn dat er proactief informatie wordt gedeeld, veel enthousiasme en energie vanuit de projectleider uitgaat en er op basis van vertrouwen wordt gewerkt. Er zijn geen verbeterpunten die de respondenten hebben voor de samenwerking.

Implementatie praktijk

Er hebben gedurende de samenwerking verschillende aanpassingen plaatsgevonden. Zo is de doelgroep uitgebreid, heeft men een groter bereik gecreëerd en zijn er verschillende delicten waar de scenario's zich op richten. Aanleidingen voor aanpassingen kunnen bijvoorbeeld cijfers zijn over veranderingen in aangiften of nieuwe delicten die zich voordoen.

Implementatie schaal & intensiteit
Men vindt het lastig om aan te geven of het project op de juiste schaal is geïmplementeerd. Omdat het een specifiek onderwerp is denkt men wel dat het betrekken van het regionale cybercrimeteam handig is omdat daar de expertise zit op het onderwerp.

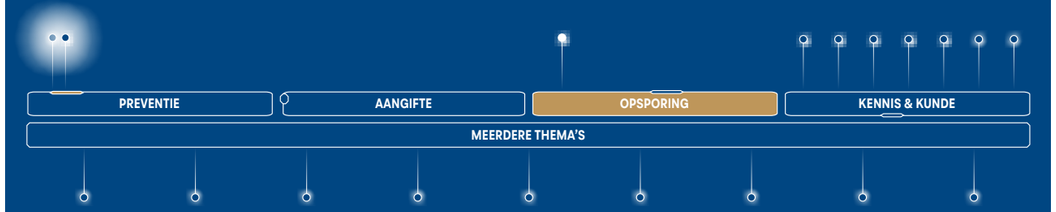
Met betrekking tot de intensiteit is de doelgroep een gehele ochtend of middag bij de Risk Factory en worden verschillende scenario's (waaronder de online scenario's) doorlopen. Het online scenario duurt 20 tot 25 minuten en is volgens de respondenten goed omdat het anders te lang zou duren voor de doelgroepen. Voor de corona-maatregelen kwamen groepen meerdere keren per week langs.

Toepasbaarheid andere eenheden
Men geeft aan dat het concept goed toepasbaar is in andere politie-eenheden, mits er een Risk Factory in de regio is. Omdat er op regionaal niveau verschillen kunnen zitten in de prevalentie van delicten denkt men dat het goed is om regionaal samen te werken. Het uitwisselen van scenario's tussen veiligheidsregio's is mogelijk, met kleine aanpassingen van de scenario's met betrekking tot het lokale karakter (zoals plaatsnamen). Vanuit de politie zijn vooral capaciteit, kennis en enthousiasme nodig om het concept te implementeren. Daarnaast zijn in Limburg enkele middelen gebruikt zoals logomateriaal, folders en een afgeschreven politieauto/-motor.

4.2 Opsporing

Er is één initiatief geïdentificeerd dat zich uitsluitend richt op de opsporing van online criminaliteit: 'Districtelijke cyberteams' (zie figuur 2). Het initiatief wordt nu besproken.

Figuur 2: initiatief omtrent de opsporing van online criminaliteit



4.2.1 Districtelijke cyberteams

Eenheid Zeeland-West-Brabant

Introductie

Het project 'districtelijke' cyberteams bestaat uit de oprichting van cybercrimeteams van minimaal 5FTE binnen de districtsrecherche om cybercrimezaken te draaien. Daarnaast dienen de districtelijke cyberteams bij te dragen aan de kennis en kunde, informatiepositie en olievlekwerking binnen het district rondom het thema. Er zijn drie respondenten tegelijkertijd geïnterviewd voor het project. Een respondent is teamleider van Team Digitale Opsporing (TDO) en het Cyber HQ, de andere twee respondenten zijn vanuit hun functie betrokken bij de coördinatie van twee verschillende districtelijke cyberteams.

Aanleiding

Vanuit twee verschillende ontwikkelingen is het project 'districtelijke cyberteams' in de eenheid Zeeland-West-Brabant ontstaan. Enerzijds is rond 2017 – tegelijkertijd met de oprichting van de regionale cybercrimeteams – in district Zeeland al een districtelijk cyberteam opgericht. In dit district zag men namelijk een groot aanbod van cyberzaken en werd gezien dat er al meebewogen moest met de regionale ontwikkelingen. De pilot in district Zeeland is in 2018 formeel geëvalueerd binnen de politie. Ook werd in gesprekken tussen de teamleider van het regionale cybercrimeteam, de teamchef van de eenheid en andere deskundigen geconstateerd dat 'de beweging rondom digitalisering in de haarvaten van de gehele organisatie op gang moest komen'. In 2019 is daarom een strategie

geschreven voor de eenheid, gericht op drie pijlers: digitalisering, digitale opsporing en cybercrime. In de strategie zat de oprichting van districtelijke cybercrimeteams verweven, op basis van de ervaringen die waren opgedaan in district Zeeland. De belangrijkste samenwerkingspartners bij de opzet van het project waren de portefeuillehouder digitalisering politiewerk en cybercrime, de staf ondersteuning en inhoudsdeskundigen.

Beschrijving project

Inhoud

De kern van het project bestaat uit het vrijmaken van capaciteit binnen de districten voor het draaien van operationele zaken omtrent cybercrime. Verder bestaat het project uit het maken van een kwaliteitsslag op de informatiepositie, het uitdragen van kennis en kunde binnen het district en het aanhaken bij andere initiatieven binnen de eenheid (zoals de digi kamers, OSINT en gedigitaliseerde criminaliteit). In elk district zit ook een liaison die is verbonden aan het Cyber HQ (zie paragraaf 4.4.6) en zich bezighoudt met kennisoverdracht, expertise opdoen en verbinding maken. Zo dient de netwerkstructuur binnen de eenheid in gang gebracht te worden. Binnen de eenheid is afgesproken dat per 2021 bij elk district minimaal 5FTE moet zijn gelabeld aan cybercrime. De districten zijn vrijgelaten hoe ze hier verder invulling aan geven.

In district Zeeland heeft men als volgt het district cyberteam vormgegeven. Er is 2FTE toegewezen aan de werkvoorbereiding van cyberzaken. Verder bestaat het operationele deel van het team uit 2 medewerkers van de DR (districtsrecherche) en 3 medewerkers uit de basisteams die rouleren om ervaring op te doen met cyber. Het is de bedoeling dat wanneer zij teruggaan naar de basisteams de ervaringen en kennis kunnen delen. Het operationele team en de werkvoorbereiding zijn fysiek in hetzelfde gebouw ondergebracht. Ten slotte is er een leestafel voor de cyberaanpak waarin men een keer per week bij elkaar komt om met andere disciplines (tactiek, financieel, case screening en digitaal) bespreekt wat er is gevonden in een zaak.

Het cybercrimeteam in district Hart van Brabant is onderverdeeld in een voorportaal en een cybercrimeteam. Het voorportaal bestaat uit 2 medewerkers, waarvan 1 medewerker vanuit de DR en 1 medewerker vanuit een basisteamrecherche. Om het half jaar is er een nieuwe medewerker zodat de kennis verder wordt uitgedragen richting de basisteams. In het voorportaal komen de aangiftes binnen, worden deze opgewerkt, de eerste gegevens veiliggesteld en beoordeeld of een aangifte haalbaar is. Vervolgens wordt deze doorgezet naar een VVC (basisteamrecherche) of naar het cybercrimeteam. Het operationele cybercrimeteam binnen het district bestaat uit 4 medewerkers. Dit zijn rechercheurs van de DR. Ten slotte is er elke ochtend een briefing met het districtelijk cyberteam, waar ook een digitaal rechercheur aansluit.

Doel

De primaire taak van het districtelijke cyberteam is om reguliere opsporingsonderzoeken te draaien op het gebied van cybercriminaliteit. Een ander doel is om ervoor te zorgen dat er een olievlekwerking ontstaat binnen het eigen district op de drie pijlers (digitalisering, gedigitaliseerde criminaliteit en cybercrime). Dit betekent dat er successen en ervaringen opgedaan dienen te worden en dat de rest van het district geënthousiasmeerd dient te worden om feeling te krijgen met het thema. Een overkoepelend doel van het districtelijke cybercrimeteam is ten slotte om een operationeel netwerk te creëren dat met elkaar samenwerkt in de aanpak van cybercriminaliteit.

Niveau

De districtelijke cyberteams werken op districtelijk niveau, maar doordat er meerdere teams zijn is er een dekking op eenheidsniveau.

De districtelijke cyberteams richten zich op de meer technische delicten die uit een cybercrime query volgen. De query is gebouwd op bepaalde maatschappelijke klassen uit Basisvoorziening Handhaving (BVH). Wanneer delicten te technisch zijn wordt er overgeschakeld naar het TDO.

Onderbouwing

Verwachte werking

Er wordt verwacht dat het districtelijk cybercrimeteam bijdraagt aan de eerder geformuleerde doelen omdat districten zich in de haarvaten van de politie bevinden. Ook wordt gedacht dat het dichterbij brengen van het onderwerp bij de districten goed werkt. Daarnaast wordt een districtsrecherche door de toewijzing van 5FTE verantwoordelijk gemaakt en is het minder makkelijk om de verantwoording voor dergelijke zaken bij anderen neer te leggen. Ten slotte verwacht men dat het aanbod van zaken cyber- en/of gedigitaliseerde criminaliteit in de toekomst verder zal uitbreiden, waardoor meer capaciteit nodig is op het thema.

Bijhouden werking

Het bijhouden van kwantitatieve doelstellingen wordt als lastig omschreven, omdat de delicten onder diverse maatschappelijke klassen[15] vallen. Binnen de eenheid is besloten om een projectcode cyber te ontwikkelen en die aan elk cyberfeit te koppelen, zodat er zicht blijft op de zaken. Verder wordt er aangegeven dat de doelen omtrent kennis en kunde lastig meetbaar zijn. Wel is er een monitor binnen de eenheid waarin bepaalde ontwikkelingen op het gebied van cyber op kwalitatieve en kwantitatieve wijze worden gevolgd.

In district Tilburg wordt per cyberzaak die binnenkomt door een van de respondenten bijgehouden hoeveel zaken worden opgewerkt en uitgezet en hoeveel zaken opgelegd worden, omdat in de politiesystemen vaak niet terug te halen is wat er verder met een zaak gebeurd. In district Zeeland wordt op dit moment een evaluatie uitgevoerd door een projectgroep binnen de politie naar het aangifteproces van cyberzaken. Op basis van de geïdentificeerde tekortkomingen worden aanpassingen gedaan. Ten slotte is afgesproken om de districtelijke cyberteams als geheel project te evalueren, echter is er nog niet afgesproken hoe hier invulling aan zal worden gegeven.

Samenwerking

De districtelijke cybercrimeteams bestaan uit 7 tot 10 medewerkers. Afhankelijk van de expertise die aanvullend nodig is in een onderzoek wordt er overleg gepleegd met bijvoorbeeld collega's van TDO of van de financiële recherche. Daarnaast zijn er vanuit het Cyber HQ liaisons verbonden aan de districtelijke cybercrimeteams. Het Cyber HQ kan worden ingeschakeld voor

15 In de politiesystemen worden delicten in bepaalde maatschappelijke klassen (categorieën) ingedeeld.

kennis en expertise. Extern wordt regelmatig overlegd met het ECTF (electronic crime task force) en vermogenstraceerders van het OM. Zij leveren advies in de onderzoeken die door het districtelijke cybercrime team worden gedraaid. Ook is er een medewerker publiek-private samenwerking binnen de eenheid die indien nodig schakelt met andere externe partijen.

Afspraken

Er wordt geprobeerd om niet te veel op basis van formaliteiten en vaste afspraken te werken. Een formele afspraak is er omtrent de minimale capaciteit van 5FTE per districtelijk cybercrimeteam. Verder is er een vrije invulling voor de wijze waarop de 5FTE worden ingezet. De hele aanpak van cyber is binnen de eenheid gefocust op de dingen die werken, op de mensen die mee willen doen en het ondersteunen en faciliteren van de mensen die willen meedoen. De samenwerking in de vorm van districtelijke cybercrimeteams is voor onbepaalde tijd. Wel wordt het proces continue gemonitord en bijgestuurd waar nodig.

Kwaliteit samenwerking

De samenwerking met andere afdelingen binnen de eenheid wordt in eerste instantie als goed omschreven. Wanneer iemand zelf niet over bepaalde kennis beschikt, is er altijd ondersteuning binnen of buiten het team om informatie vandaan te halen. Wat soms lastig is in de samenwerking, is om bij doorzoekingen bijvoorbeeld extra personeel mee krijgen. Binnen de districtsrecherche of in andere eenheden is bijvoorbeeld bij doorzoekingen niet iedereen bereid om personeel af te staan. De samenwerking verloopt beter met afdelingen die al raakvlakken hebben met het thema cybercriminaliteit dan met afdelingen die de affiniteit niet hebben. Dit zou eventueel kunnen worden verbeterd door bijvoorbeeld tijdens briefings met de volledige districtsrecherche meer te vertellen over de onderzoeken die worden gedraaid, zodat wanneer er een verzoek komt, men weet welk onderzoek het betreft en meer verbondenheid voelt.

Implementatie praktijk

Op papier zijn de districtelijke cyberteams nu ingericht zoals bedoeld in de vorm van 5FTE. In de praktijk wordt er nog geschoven met personeel en is het lastig om te zoeken naar het juiste personeel dat voor langere tijd blijft. Dit komt onder andere doordat het thema cyber door sommigen als minder aantrekkelijk, moeilijk en ingewikkeld wordt gezien.

Implementatie schaal & intensiteit

Op dit moment wordt gekeken of het thema breder binnen de districtsrecherche kan worden geïntegreerd. Financieel economische criminaliteit raakt bijvoorbeeld cybercriminaliteit en andersom. Beide afdelingen draaien wel hun eigen opsporingsonderzoeken. Er wordt geïnventariseerd of de teams ook gemeenschappelijke onderzoeken uit kunnen voeren.

Met betrekking tot de intensiteit wordt aangegeven dat cyberzaken altijd groter getrokken kunnen worden en er altijd meer capaciteit besteed kan worden aan de recherches. Het is volgens de betrokkenen vooral van belang om slimmer en efficiënter te gaan werken, door de juiste ervaring en expertise op te doen. De informatiepositie is hierbij van groot belang. Daarnaast kunnen de districtelijke cyberteams maar een beperkt aantal onderzoeken draaien, waardoor goed onderbouwd dient te worden welke onderzoeken haalbaar zijn, kansrijk zijn en waarmee een groot effect wordt bereikt. In aanvulling hierop onderschrijft men het belang van landelijke organisatie, omdat anders een groot aantal districtsrecherches en basisteams op hun eigen manier problemen bekijken. Er wordt verwezen naar het project VIN-fraude in de eenheid Oost-Nederland als goed voorbeeld van een dergelijke aanpak. Geografie en de systeemwerkelijkheid binnen de politie worden als twee grote problemen omschreven.

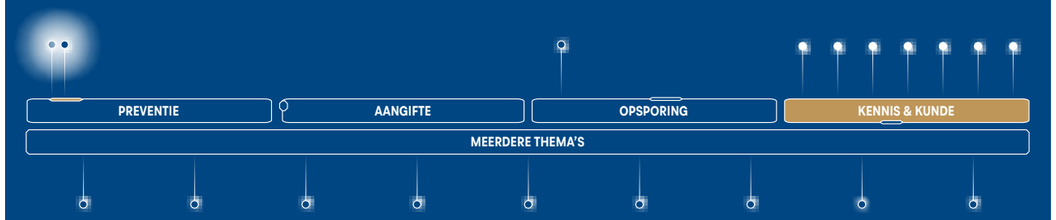
Toepasbaarheid andere eenheden

Het concept is makkelijk toe te passen in andere eenheden en vereist slechts het labelen van capaciteit en het creëren van randvoorwaarden in de vorm van kennis en middelen. In andere eenheden worden soortgelijke initiatieven genomen, maar capaciteit wordt niet zo zeer gelabeld. Hoe het verder wordt ingericht bij andere eenheden is niet bekend. Wel wordt aangegeven dat er enthousiast op het concept uit de eenheid Zeeland-West-Brabant wordt gereageerd en dat andere eenheden op bezoek komen om mee te kijken.

4.3 Kennis en kunde

Er zijn in totaal zeven initiatieven geïdentificeerd die zich uitsluitend richten op het versterken van de kennis en kunde van politiemedewerkers op het gebied van online criminaliteit: ‘Cybercrisisoefening met BT’, ‘Digitale vaardigheden Friesland’, IT-coaches district Twente’, Digitaal flexteam IJsselland’, ‘Cyber support team’, ‘Workshop cybercrime’ en ‘KOR3NWOLF’ (zie figuur 3). De initiatieven worden nu individueel besproken.

Figuur 3: initiatieven die zich richten op het versterken van kennis en kunde van politiemedewerkers



4.3.1 Cybercrisisoefening met BT

Eenheid Noord-Nederland

Introductie

Het initiatief ‘cybercrisisoefening met basisteam’ betreft een sessie waarin een basisteam samen met een andere partij (bv. een ziekenhuis) een fictieve casus doorloopt en scenario’s bespreekt om meer bewustwording te creëren binnen basisteams rondom het thema cybercrime.
Er is gesproken met twee politiemedewerkers uit de eenheid Noord-Nederland. De eerste respondent is operationeel specialist bij basisteam Groningen-Noord en heeft het thema cyber toegewezen gekregen om te zorgen voor een centraal aanspreekpunt voor ketenpartners in Groningen. De tweede respondent is accountmanager publiek private samenwerking (PPS) bij het regionale cybercrimeteam. In deze functie wordt verbinding gezocht met publieke en private partners buiten de politie op het gebied van cybercrime.

Aanleiding

Er worden verschillende aanleidingen genoemd voor het initiatief ‘cybercrisisoefening met BT’. Ten eerste constateerde de accountmanager PPS in gesprekken en overleggen met gemeenten dat er weinig partijen met de gemeenten samenwerkten op het gebied van preventie en crisismanagement van cybercrime. Tijdens de gesprekken is ook gekeken in hoeverre gemeenten voorbereid waren op een cybercrisis. Gemeenten keken vooral naar interne cybercrisissen in plaats van crisissen die extern (binnen het verzorgingsgebied) kunnen plaatsvinden. Vanuit de politie zijn toen (niet opsporingsgerichte) medewerkers aangewezen als gesprekspartners voor de stad Groningen op het gebied van cybercrime. Vervolgens is men ook binnen de politie verder na gaan denken over de rol van basisteams bij een cybercrisis in de regio en hoe het bewustzijn rondom dit onderwerp kan worden vergroot. De accountmanager PPS merkte namelijk dat basisteams alleen reageren bij meldingen, terwijl de politie ook zonder melding een rol heeft bij cyberincidenten. Bijvoorbeeld wanneer incidenten in het nieuws komen. Ondertussen was de veiligheidsregio Groningen begonnen met een grote cybercrisisoefening. Toen is het idee ontstaan om een soortgelijk initiatief te organiseren op basisteam niveau. Ten slotte zijn er ideeën opgehaald en is in drie sessies met samenwerkingspartners de cybercrisisoefening ontwikkeld.

Beschrijving project

Inhoud

Het initiatief ‘cybercrisisoefening met het basisteam’ is een sessie waarbij een cybercrisisoefening de aanleiding vormt om binnen basisteams het gesprek aan te gaan over cybercriminaliteit. Zo kan worden besproken wat nog meer het thema raakt en wat men binnen het basisteam kan doen.

Tijdens de sessie wordt begonnen met een presentatie over cybercriminaliteit door het lectoraat cybersafety van de Hogeschool Leeuwarden. Hierin wordt aan de hand van een aantal voorbeelden uitgelegd hoe de digitale wereld en fysieke wereld elkaar raken. Vervolgens is er een fictieve cybercrisisoefening, waarin een filmpje wordt afgespeeld van een nieuwsitem van RTV-Noord over een ransomware aanval op het lokale ziekenhuis waardoor een elektronisch patiëntendossier niet meer toegankelijk is. Het filmpje is opgenomen in de omgeving van het ziekenhuis, waar een verslaggever vertelt wat er speelt en medisch personeel aan het woord komt. Daarna wordt aan politiemedewerkers van het basisteam gevraag hoe men hierop zou reageren als dit op het nieuws zou komen. Hierover gaat men dan in gesprek en er wordt gekeken of de basisteams bekend zijn met partners in de wijk op het gebied van cyber en of zij daar verbinding mee hebben gelegd. Na dit gesprek komt het digitaal platform op bezoek om te vertellen wat zij voor het basisteam kunnen betekenen. Zij zijn het eerste aanspreekpunt voor een basisteam op het moment dat er kennis ontbreekt. Ten slotte wordt er vanuit het ziekenhuis uitleg gegeven over de behoeften van – en gevolgen voor – het ziekenhuis tijdens een cybercrisis en wordt de oproep gedaan om met elkaar contact op te nemen bij een cyberincident.

De eerste sessie duurde 1,5 à 2 uur en heeft online via Microsoft Teams plaatsgevonden. De eerste cybercrisisoefening bij een basisteam is in mei 2021 geweest, een tweede basisteam staat op de planning voor september 2021 en een sessie bij het derde basisteam is gepland eind 2021.

Doel
Het doel van de cybercrisisoefening is om bewustwording te laten plaatsvinden op het gebied van cybercrime onder basisteams. Het dient een laagdrempelige eerste kennismaking te zijn met het thema en informatie over de rol van het basisteam. Aan de hand van de sessie dient het gesprek binnen het basisteam aangegaan te worden over de rol, uitdagingen en keuzes omtrent het thema.

Doelgroep
De doelgroep van de sessie betreft de basisteams binnen de politie, specifiek de drie basisteams in de stad Groningen. Dit betreft in eerst instantie vooral de operationeel experts en operationeel coördinatoren van de basisteams. Ook wordt nagedacht over mogelijkheden om overige medewerkers van de basisteams mee te nemen in de sessie.

Niveau
De cybercrisisoefening vindt plaats op het niveau van basisteams. Er is gekozen voor basisteams omdat zij een belangrijke rol hebben in acute ondersteuning tijdens of na incident. De basisteams moeten op de hoogte zijn van incidenten en weten welke routes er zijn binnen en buiten de organisatie op het thema. Er werd geconstateerd dat kennis en kunde hieromtrent ontbrak en dat een cybercrisisoefening de discussie en bewustwording op het thema kon aanjagen.

Onderbouwing

Verwachte werking
Er wordt verwacht dat een fictieve cybercrisis (bijvoorbeeld bij een ziekenhuis) ook impact heeft op een basisteam en het werk op straat. Er is daarom gekozen om een groot incident als uitgangspunt te nemen en vervolgens de kleine rol van het basisteam in een dergelijke casus te belichten. Een andere verwachting is dat de sessie ervoor zorgt dat er een 'motor gaat draaien' binnen de basisteams rondom cybercrime. Het project is verder niet gebaseerd op wetenschappelijke of praktijkgerichte theorieën. Wel wordt tijdens de sessie kennis over het thema overgedragen door een onderzoeker van een Hogeschool.

Bijhouden werking
Een van de respondenten houdt zelf bij welke effecten de cybercrisisoefening heeft, door te kijken naar gebeurtenissen die plaatsvinden binnen de basisteams naar aanleiding van de sessie.

Doelen behaald?
Er wordt aangegeven dat het doel nog lang niet is bereikt, maar dat er wel concrete stappen zijn gemaakt. Een voorbeeld is dat wijkagenten voor de sessie aangeven dat cyber een 'blinde vlek' is waar ze geen kennis van hebben en dat na de sessie een van de wijkagenten naar aanleiding van een hack een gesprek heeft geïnitieerd met een IT-specialist van de Rijksuniversiteit en het digitaal platform van de politie. Een ander voorbeeld is dat tijdens de sessies bleek dat collega's niet meteen aan het digitaal platform dachten na een incident en tijdens de sessie benadrukt wordt dat dit een van de routes is. Verder is het basisteam naar aanleiding van de sessie op papier gaan zetten wat er binnen het basisteam gebeurd op het gebied van cybercrime en waar men naartoe wilt werken. Hierna gaat men cyber clusterdagen organiseren voor verschillende clusters binnen het basisteam.

Samenwerking

Er wordt voor het initiatief samengewerkt met verschillende interne en externe partners:
- Intern: basisteams, Digitaal platform
- Extern: partners uit de wijk, Hogeschool Leeuwarden, studenten van de Hanze Hogeschool

De basisteams zijn zoals eerder aangegeven de doelgroep van het initiatief. Verder is het digitaal platform betrokken om informatie te geven en verbinding te maken met de basisteams. Partners uit de wijk zijn bijvoorbeeld een ziekenhuis die een rol spelen tijdens de cybercrisisoefening. Vanuit de Hogeschool Leeuwarden wordt een presentatie verzorgd over cybercrime en studenten van de Hanze Hogeschool hebben voor de fictieve casus een filmpje gemaakt.

De samenwerking heeft eerst bestaan uit een aantal gesprekken waarin verwachtingen en ideeën rondom het project zijn besproken. Vervolgens zijn er concepten gemaakt en besproken voor de presentaties. Ook heeft men voorafgaand aan de sessie een keer fysiek bij elkaar gezeten om het hele programma te doorlopen.

Afspraken
Er zijn geen afspraken op papier vastgelegd. Het project is ontstaan vanuit enthousiasme. Verder is er geen duur vastgelegd met betrekking tot de samenwerking.

Kwaliteit samenwerking
Met betrekking tot de samenwerking wordt aangegeven dat de betrokkenen enthousiast zijn en graag willen samenwerken. Het kost dan ook weinig moeite om tijd vrij te maken bij de partners. Een verklaring voor de positieve samenwerking kan worden gevonden in het nut, de noodzaak en de ernst van de situatie die door alle samenwerkingspartners worden ingezien.

Verbeterpunten samenwerking
Uit de evaluatie van de eerste sessie bleek dat de voorbeelden in de sessie kleiner en meer lokaal kunnen zijn, omdat het anders te ver af kan staan van de belevingswereld van deelnemers.

Implementatie praktijk

Het project is vormgegeven zoals beoogd, gezien de effecten die de respondent ziet ontstaan binnen het basisteam na de cybercrisisoefening. Het initiatief is achteraf in een online bijeenkomst geëvalueerd met de partners die betrokken geweest zijn bij de uitvoering. Tijdens de evaluatie is aan iedereen gevraagd wat men ervan vond, wat goed ging en wat beter kan. Op basis van de sessie worden aanpassingen doorgevoerd. Zo zal bij een volgende sessie eerst gesproken worden met het basisteam en gevraagd in welke fase men nu zit op het thema en waar behoefte aan is. Aan de hand daarvan dan bepaalde accenten gelegd in de presentaties van de verschillende partners. De oefening wordt dus specifiek aangepast aan het basisteam waar de sessie wordt gegeven, omdat het ene basisteam verder in de materie zit dan het andere basisteam.

Er is tevredenheid over de eerder besproken effecten die respondent heeft gezien. Wat beter had gekund is de basisteams meer aan de voorkant van de sessies te betrekken, zodat het aanbod aansluit bij de behoeften en fase van het basisteam op het thema cyber.

Implementatie schaal & intensiteit
Voor het moment is gekozen om de sessies voor de drie basisteams in Groningen te houden. Voor eerste stap is dit voldoende volgens de respondent. De sessies duurt ongeveer twee uur en dit is voldoende om de aandacht van collega's er nog bij te houden. Wel wordt opgemerkt dat het belangrijk is om het onderwerp terug te laten komen. Zo wordt in het basisteam een stuk opgesteld over wat er speelt in het basisteam op het thema en neergelegd bij het managementteam.

Toekomstplan
Op het moment worden er nog twee sessies georganiseerd voor de overige basisteams in Groningen. Hierna ligt het verder open of de cybercrisisoefening nog een vervolg krijgt op andere of dezelfde plekken.

Toepasbaarheid andere eenheden
Een dergelijke cybercrisisoefening kan volgens de respondent goed worden toegepast binnen andere basisteams in andere districten en eenheden. Wel is het belangrijk om te bepalen hoever een basisteam als is met het inrichten van preventie en of er al stappen zijn ondernomen met gemeenten om samen te werken. Sommige basisteams zijn bijvoorbeeld al bekend met welke partners ze kunnen samenwerken in de wijk.

4.3.2 Digitale vaardigheden Friesland

Eenheid Noord-Nederland

Introductie

Dit project betreft een reeks aan initiatieven van het digitaal platform om de digitale vaardigheden van verschillende groepen politiemedewerkers binnen het district Friesland te verbeteren.

De respondent is als operationeel specialist B verbonden aan de districtsrecherche Friesland en is portefeuillehouder en leidinggevende binnen het digitaal platform. Het digitaal platform heeft een voornamelijk een forensische rol.

Aanleiding

De belangrijkste aanleiding voor de initiatieven is de opdracht die het digitaal platform heeft – naast het leveren van digitale ondersteuning tijdens opsporingsonderzoeken - om te werken aan de digitale vaardigheden van de politiemedewerkers binnen het district. Daarnaast heeft het digitale platform een beperkte capaciteit van zes personen, waardoor het belangrijk is om mensen mee te nemen in het onderwerp. De collega's dienen de meerwaarde in te zien van het uitleren van digitale vaardigheden. Ten slotte was er een intrinsieke motivatie binnen het digitaal platform om een goed product te ontwikkelen. In 2017 zijn de eerste initiatieven van start gegaan.

Beschrijving project

Inhoud
Het project digitale vaardigheden kan worden gezien als een reeks initiatieven om de digitale vaardigheden van politiemedewerkers in het district te verbeteren. Binnen het district is een grote diversiteit aan deskundigen – van diepte rechercheurs tot medewerkers die de aangiften opnemen – waardoor een uniforme aanpak niet mogelijk is. Er zijn daarom specifieke activiteiten voor specifieke doelgroepen georganiseerd. Een lijst is opgesteld met wat een bepaalde doelgroep zou moeten kunnen. Per doelgroep is vervolgens een bepaalde periode vastgesteld waarin een programma is aangeboden. De inhoud van het programma wordt gekoppeld aan wat de doelgroepen in de praktijk daadwerkelijk tegenkomen. Dit wordt geïnventariseerd vanuit het digitaal platform. Worden er bijvoorbeeld op een bepaald spoor herhaaldelijk vorderingen van onvoldoende kwaliteit ingestuurd, dan gaat men hierop in. Het project is vooral een tijdelijke oplossing, omdat in de reguliere opleidingen nog geen digitaal aanbod zit. De volgende activiteiten hebben plaatsgevonden:

1. Voor de doelgroep intake en service is een programma ontwikkeld dat bestaat uit klassikale les, presentaties, filmpjes en het laten zien van echt voorbeelden van aangiften met digitale aspecten. Dit programma heeft een aantal dagdelen plaatsgevonden voor zes basisteams uit Friesland die aangiften opnemen.
2. Medewerkers binnen de senior tactische opsporing zijn betrokken bij het beslissen of een zaak verder wordt opgepakt. Vanuit het OM was opgevallen dat veel zaken vroegtijdig beëindigd werden,

ondanks dat er opsporingsindicatie in de zaken zat. Tijdens het programma voor deze doelgroep worden voorbeelden van processen-verbaal gegeven die vroegtijdig zijn beëindigd. Er wordt dan gekeken welke argumentatie er onder de vroegtijdige beëindiging ligt en wat er anders had gekund, zodat medewerkers leren welke waarde bepaalde sporen kunnen hebben en hoe de kwaliteit van aangiften gecontroleerd kan worden.

3. Leidinggevenden binnen de basisteams (operationeel experts) zijn middels gesprekken en presentaties bewust gemaakt over de impact en ondermijnende werking die online criminaliteit kan hebben.
4. Voor de basispolitiezorg (BPZ) – ook wel de 'blauwe politie op straat' – is een escaperoom gebouwd omdat het een grote groep mensen betreft. In de escaperoom leren de medewerkers bijvoorbeeld welke risico's zij lopen wanneer zij worden afgeluisterd of gefilmd, hoe een telefoon op vliegtuigmodus kan worden gezet en dat er waardevolle informatie zit in computers van auto's en telefoons. De escaperoom is gebouwd in een trailer van 12 meter, waardoor de bus langs alle basisteams in Friesland kon rijden.
5. Op dit moment wordt voor rechercheurs een 'digitale trainingsstraat' ingericht. Twee stagiaires hebben voor het dit initiatief eerst in kaart gebracht waar rechercheurs tijdens hun dagelijkse werkzaamheden tegenaan lopen. In de digitale trainingsstraat leren de rechercheurs om digitaal te rechercheren, verbindingen te leggen en hoe en waar men een vordering kan uitzetten. De trainingsstraat is voor de districtsrecherches maar ook voor het deel van de basisteams dat zich richt op het oppakken van de VVC. De trainingsstraat wordt aangepast op basis van de actuele behoeften van politiemedewerkers.

Doel

Het doel van de reeks initiatieven is om de digitale vaardigheden van politiemedewerkers binnen het district Friesland te verbeteren. Dit hoofddoel kan worden onderverdeeld in verschillende subdoelen:

- Begripskennis creëren over definities en 'modus operandi' van bepaalde cyberdelicten
- Leren digitale sporen veiligstellen
- Aanhoudingen verrichten zonder dat digitale sporen verloren gaan
- Juridische kennis op het gebied van cybercriminaliteit bijbrengen

Doelgroep

De volgende doelgroepen worden aangemerkt binnen het district Friesland:

- Intake en servicemedewerkers
- Senior tactische opsporingsmedewerkers die de aangiftes veredelen
- Leidinggevenden (operationeel experts)
- Basispolitiezorg (BPZ)
- Recherches

Niveau

Het project heeft plaatsgevonden door de gehele eenheid, bij verschillende afdelingen en lagen van het district Friesland. Daarnaast is de escaperoom truck ook een keer ingezet op een landelijk evenement.

Onderbouwing

Verwachte werking

Er wordt aangegeven dat wetenschappelijk onderzoek laat zien dat kennis die vanuit een klaslokaal wordt aangeleerd voor ongeveer 10 procent beklijfd, het krijgen van coaching en feedback voor 20 procent en werken en leren op de werkplek voor 70 procent. Daarom kan er het beste in de praktijk ('learning on the job') verder worden geleerd en probeert men de deskundigheid zo dicht mogelijk bij het werk van de politiemedewerkers te brengen en het probleem vanuit de doelgroep te bekijken. De behoeften van de medewerkers worden in kaart gebracht en op basis daarvan worden middelen aangeboden.

Bijhouden werking

Er wordt aangegeven dat men zich niet bezig houdt met de werking van de initiatieven op kwantitatieve wijze. Vanuit het digitaal platform ziet en gelooft men dat het werkt.

Verdere onderbouwing

De respondent wil graag dat het wetenschappelijk klopt, maar het digitaal platform houdt zich hier zelf niet mee bezig. Wel sluit men graag aan bij initiatieven die het geheel van uitleren onderzoeken.

Samenwerking

Bij de verschillende afdelingen zijn interne en externe samenwerkingspartners betrokken:

- Intern (binnen de politie): specialisten van het digitaal platform, de stuurlijn (leidinggevenden)
- Extern (buiten de politie): OM, studenten NHL Stenden

De specialisten van het digitaal platform zijn betrokken bij de ontwikkeling van de initiatieven en het in kaart brengen van de behoeften binnen het district. Verder worden binnen de politie de leidinggevenden meegenomen in de verschillende initiatieven en zijn zij deels de doelgroep. Vanuit het OM is er een officier van justitie die bijvoorbeeld de trainingsstraat heeft geopend. Ook wil het OM met officieren van justitie door de trainingsstraat. Studenten van de NHL Stenden hogeschool hebben meegeholpen met het ontwikkelen van de escaperoom bus.

Afspraken

Er zijn afspraken dat het digitaal platform zich richt op de digitale vakbekwaamheid. Verder zijn er afspraken met de hogescholen dat er elke keer mensen kunnen worden aangenomen als stagiaires. Het project loopt in de huidige vorm tot december 2021, het project heeft dan 4 jaar geduurd.

Kwaliteit samenwerking

De samenwerking wordt in principe als goed omschreven. Zo zijn intake en service medewerkers dankbaar voor de trainingen en is er goed contact met de basisteams. Een aandachtspunt blijft dat sommige afdelingen erg op hun eigen taken zijn gefocust en afstand behouden tot digitale thema's.

Implementatie praktijk

Het project is verlopen zoals beoogd en de respondent is tevreden met het resultaat. Wat goed is verlopen, is dat er veel mensen enthousiast waren en zodoende reclame hebben gemaakt voor de initiatieven. Ook zorgt de spelvorm van sommige activiteiten dat het onderwerp laagdrempelig wordt aangeboden. Wat beter kan en moet vol-

gens de respondent is meer aandacht voor digitale kansen en vaardigheden binnen de basisopleiding van de politie. De taak van de respondent zou namelijk kleiner moeten zijn op dit gebied zodat de focus op specifieke fenomenen kan blijven in plaats van algemene vaardigheden.

Implementatie schaal & intensiteit
De initiatieven hebben door het gehele district plaatsgevonden. Het project is volgens de respondent niet op de juiste schaal geïmplementeerd, omdat het in andere districten nog niet is geïmplementeerd. De activiteiten zijn wel aangeboden aan andere districten, maar door tijdsgebrek in die districten is het daar nog niet van de grond gekomen. Dergelijke initiatieven zouden volgens de respondent door de gehele eenheid en het hele land genomen dienen te worden.

Met betrekking tot de intensiteit had men graag een opvolging willen geven aan de initiatieven bij een aantal doelgroepen, zodat gekeken kan worden wat het heeft opgeleverd. Hier was geen ruimte voor binnen het huidige project, maar het wordt aanbevolen om mensen terug te laten komen om te zien wat zij hebben geleerd.

Toekomstplan
Het project zal eind 2021 komen te vervallen in de huidige vorm. Vanaf dan zal er nog in tweejaarlijkse workshops (zogenaamde VAK-dagen) een programma worden aangeboden, maar er zal dan niet meer op de algehele vaardigheden worden gefocust. De respondent geeft aan dat er voldoende signalen zijn afgegeven aan de politieacademie en dat men het vanuit het district niet meer kan organiseren.

Toepasbaarheid andere eenheden
Het project is volgens de respondent goed toepasbaar in andere districten en eenheden. Er is enthousiasme voor nodig en iemand die vanuit de andere eenheid het concept kopieert en afstemt op de desbetreffende eenheid. Van alles wat is gedaan binnen het project zijn hand-outs gemaakt die beschikbaar zijn gesteld voor de doelgroepen[16].

16 Via Agora, een intern politiesysteem dat wordt gebruikt om samen te werken en documenten te delen.

4.3.3 IT-coaches district Twente

Eenheid Oost-Nederland

Introductie

Het project IT-coaches binnen district Twente bestaat uit de aanstelling van twee IT-coaches die verschillende middelen inzetten om te voorzien in de leerbehoeften van politiemedewerkers binnen het district op het gebied van digitalisering. De respondent is werkzaam als operationeel specialist en houdt zich bezig met de vernieuwing en verbetering van politiewerk. Als aanjager voor het programma “cyber en leren” kijkt de respondent hoe men het district vaardiger kan maken en meer kennis kan geven op het gebied van cyber.

Aanleiding

In het district Twente heeft men een programma “cyber en leren”, in plaats van een portefeuille cybercrime zoals in andere districten. Men heeft hiervoor gekozen omdat men vooral een opdracht zag in het verbeteren van de kennis en vaardigheden rondom het thema.

Voor het programma cyber en leren is eind 2019 een strategie geschreven, waarin is opgenomen dat men een leerangst wil creëren bij collega’s. Een leerangst is een bewustwording bij iemand dat hij of zij iets moet gaan doen, maar nog niet weet hoe hij of zij dit moet gaan doen. Er worden verschillende middelen ingezet binnen het programma cyber en leren om de leerangst vervolgens op te lossen. Een van de middelen hiervan is de IT-coach.

Het idee voor de IT-coach ontstond enerzijds door informatie vanuit een lector digitalisering aan de NHL Stenden Hogeschool. De lector gaf aan dat leren in routine plaats moet vinden om effectief te zijn. Men wilde daarom graag ‘learning on the job’, waarbij collega’s coachende wijs verder komen op het gebied van digitalisering en cybercrime. Anderzijds ontstond het idee omdat politiemensen graag interactief willen leren in plaats van het leren uit boeken. Uiteindelijk is een plan voor IT-coaches voorgelegd aan – en goedgekeurd door – de eenheidsleiding. Begin 2020 is men gestart met de werving van IT-coaches.

Beschrijving project

Inhoud
Binnen het district Twente zijn twee IT-coaches aangesteld van buiten de organisatie. Een IT-coach is iemand die zowel IT-vaardig is (voldoende kennis heeft van de mogelijkheden en onmogelijkheden op digitaal gebied) als vaardigheden heeft om deze kennis over te brengen. De IT-coaches hebben tot nu toe vooral binnen het district gekeken waar de leerbehoefte zit, hoe de politieoperatie eruit ziet en waar in het dagelijks politiewerk kansen liggen om de digitale wereld in te vlechten in het politiewerk.

Op de leervraag dienen de coaches in te zetten met verschillende leermiddelen die zij zelf, samen met een team binnen de politie of met externe partners kunnen ontwikkelen. Mogelijke leermiddelen zijn een workshop, 1 op 1 begeleiding en online tools. Een voorbeeld van een project waar IT-coaches op dit moment mee bezig zijn is een bewustwordingspilot met een VR-bril. Hierin worden collega’s door een IT-coach in een VR-omgeving geplaatst en worden klassieke of digitale opsporingsmogelijkheden (sporen) gegeven die collega’s moeten leren herkennen. Een ander voorbeeld is

een bewustwordingsprikkel, waarin IT-coaches presentaties geven over dagelijkse rapportages van basisteams die de IT-coaches hebben verrijkt met digitale aspecten. Ook is er een workshop voor intake en service medewerkers over hoe men een aangifte volledig kan voorzien van digitale opsporingsmogelijkheden.

Doel
Het doel is om een leerbeweging op gang te brengen op het gebied van digitalisering. Het gaat men er vooral om collega's te bewegen naar dat zij het normaal gaan vinden om digitale aspecten te betrekken in hun werk. De leerbeweging is opgenomen in de strategie voor het programma cyber en leren.

Doelgroep
De doelgroep bestaat uit politiemensen in de vijf basisteams (binnen het district Twente) en politiemensen in de districtsrecherche. Het gaat dus om iedereen die iets doet in het dagelijkse politiewerk (intake en service, operationele coördinatie, collega's in 'blauwe' teams, recherche teams). In de toekomst wordt de afdeling informatieorganisatie wellicht ook een doelgroep. Men probeert namelijk te kijken of, in samenwerking met de informatieorganisatie, de kwaliteit van de aangiften digitale criminaliteit kunnen worden verhoogd voordat deze bij basisteams of de districtsrecherche terecht komen.

Niveau
Het project vindt plaats binnen district Twente, waar de vijf basisteams en districtsrecherche deel van uitmaken. Door het op district niveau aan te pakken beoogt men een groot bereik te creëren.

Onderbouwing

Verwachte werking
Men verwacht dat de IT-coaches bijdragen aan de geformuleerde doelen omdat zij een goed middel zijn om in de leerbehoefte te voorzien van de politiemedewerkers. Daarnaast blijkt uit de praktijk dat politiemensen graag op een actieve manier en werkend willen leren. Ook verwacht de respondent op basis van informatie van een lector digitalisering dat routinematig werken succesvol is. Ten slotte verwacht men dat door in het dagelijkse werk dingen herkenbaar terug te laten komen, de huidige routine een digitale routine gaat worden.

Bijhouden werking
Er wordt niet bijgehouden wat de IT-coach oplevert. Wel heeft men bijvoorbeeld een voor- en nameting ingebouwd bij de bewustwordingspilot met VR-bril. Zo vraagt men de eerste keer uit welke digitale sporen en kansen deelnemers zien, heeft men vervolgens een leergesprek hierover en wordt bij een vervolgsessie nog een keer gemeten welke sporen en kansen men ziet.

Doelen behaald?
Het is niet precies duidelijk of de beoogde doelen worden behaald. Wel merken IT-coaches dat zij door steeds meer collega's worden gevonden. Een deel van de collega's mailt iedere week de IT-coach om mee te kijken, een ander deel van de collega's vindt een IT-coach wel interessant en weer een ander deel denkt dat een IT-coach pas gebeld dient te worden als diegene iets digitaal wilt gaan doen.

Samenwerking

De volgende partners zijn betrokken bij de opzet en uitvoering van het project 'IT-coaches' in district Twente:
- Intern (binnen de politie): basisteams, districtsrecherche, regionale cybercrimeteam, TDO (team digitale opsporing)
- Extern (buiten de politie): Hogeschool Windesheim, NHL Stenden

De basisteams zijn betrokken omdat de doelgroep zich hier bevindt en enkelen van hen voor het programma "cyber en leren" identificeren wat de behoeftevragen in de basisteams zijn. Deze personen zijn voor de IT-coaches het eerste aanspreekpunt. Het cybercrimeteam en TDO hebben vanuit hun expertise contact met IT-coaches. Zij voorzien de IT-experts van politie-technische en tactische kennis. De samenwerking tussen IT-coaches en de inhoudelijke experts vindt ad-hoc plaats doordat men in chatgroepen zit waarin snel informatie kan worden uitgewisseld. Daarnaast komen de IT-coaches en inhoudelijke experts elke twee à drie weken bij elkaar om bij te praten over de ontwikkelingen.

Hogeschool Windersheim heeft het project eind 2020 voorzien van een onderwijskundige onderbouwing. Zij hebben aangegeven hoe de IT-coaches, op een onderwijskundig juiste manier, vorm kunnen geven aan hun coaching. Hiervoor is een onderzoek gedaan binnen een aantal basisteams en TDO om te kijken wat valkuilen zijn en hoe een coaching traject vorm kan worden gegeven. Er is een advies opgesteld waarin verschillende fasen zijn beschreven voor de coaches: eerst leerbehoeften ophalen, vervolgens een bewustwording workshop, daarna een kennisworkshop en ten slotte een terughaalmoment in de dagelijkse praktijk.

Afspraken
Er zijn geen formele afspreken gemaakt tussen de verschillende partners. Wel zijn er informele afspraken, bijvoorbeeld dat er geen expert meetings georganiseerd worden door IT-coaches zonder dat zij vooraf geschakeld hebben met TDO en het cybercrimeteam. Ook als nieuwe dingen worden geleerd aan collega's vindt vooraf met hen een check plaats. De IT-coaches hebben in principe een aanstelling voor 2 jaar gekregen. Er is geen duur of einddatum voor het project.

Kwaliteit samenwerking
De samenwerking wordt door de respondent omschreven als heel collegiaal. Zo worden de IT-coaches als gelijkwaardige partners gezien door collega's uit de basisteams, ondanks dat ze expertise hebben die de collega's zelf niet hebben. Ook met TDO en het cybercrimeteam hebben de IT-coaches een goede relatie. Een mogelijke verklaring voor de collegiale samenwerking die tevens wordt aangemerkt als succesfactor is dat men tijdens de selectie van IT-coaches ook heeft gelet op vaardigheden om contact te leggen.

Verbeterpunten samenwerking
Op moment van schrijven heeft men geen suggesties voor een verbetering van de samenwerking.

Implementatie praktijk

De uitvoering van het plan en de wijze waarop ontwikkelfasen elkaar opvolgen verloopt naar eigen zeggen zoals beoogd. Met IT-coaches zijn (twee-)wekelijkse contactmomenten om te kijken welke activiteiten lopen, wat men deze week gaat doen en wat men volgende weken gaat doen.

Wat goed gaat is dat IT-coaches zichzelf een positie hebben gegeven in de teams, waardoor er een goede basis is om het leren vorm te geven. Wat beter kan, is dat collega's graag nog hebben dat de coaches antwoorden op een presenteerblaadje geven. De wens is om te zorgen dat collega's niet 4/5 keer dezelfde zaken uitvragen maar dit na 2/3 keer zelf kunnen.

Implementatie schaal & intensiteit

Op districtsniveau is volgens de respondent de juiste schaal, omdat het niet te groot (het is overzichtelijk) en niet te klein is. Wanneer men zich op een enkel basisteam zou richten zouden het leereffect en de uiteindelijke beweging te klein zijn. Indien het meteen op een hele eenheid was uitgezet dan zijn er meerdere districten en worden de IT-coaches onvoldoende zichtbaar in het grotere geheel.

Met betrekking tot de intensiteit zijn er nu twee IT-coaches full time werkzaam. Er was 4 FTE beschikbaar, maar uiteindelijk bleven er twee geschikte kandidaten over.

Toekomstplan

Over 1,5 jaar zou men graag een meetmoment laten plaatsvinden waarin kan worden bekeken of het project op dat moment voldoende heeft bereikt, eventueel aangepast moet worden of dat er genoeg van de leerbeweging heeft plaatsgevonden. Factoren die hierop kunnen duiden zijn de zichtbaarheid van zaaks afhandeling en het dagelijkse kennisniveau in het politiewerk. Over specifieke KPI's (kritieke prestatie-indicatoren) is men in gesprek.

Toepasbaarheid andere eenheden

Het concept is volgens de respondent goed toepasbaar in andere districten en eenheden. Het is vooral belangrijk om op lokale schaal in een dergelijk thema te investeren om het uiteindelijk te kunnen laten groeien. Daarnaast is communicatie over de IT-coaches binnen het district van belang om het project goed te kunnen laten landen.

4.3.4 Digitaal Flexteam IJsselland

Eenheid Oost-Nederland

Introductie

Het project 'Digitaal Flexteam IJsselland' bestaat uit de oprichting van een team van politiemedewerkers die het district digitaal vaardiger dienen te maken door verschillende projecten en activiteiten uit te voeren. De respondent is werkzaam als coördinator van het Digitale Flexteam in district IJsselland. Het hele team is op dit moment een pilot, waardoor iedereen vanuit een ander team geplaatst wordt in het Digitale Flexteam.

Aanleiding

In 2012 heeft elke politie-eenheid een flexteam gekregen (15 FTE) dat vrij kon worden ingericht. Rond 2018 signaleerde de sectorleiding van district IJsselland dat het district achterbleef op het gebied van innovatie en digitalisering/cybercrime. Er is toen besloten om een digitaal flexteam op te richten voor een pilot van twee jaar. In oktober 2019 heeft de besluitvorming plaatsgevonden en in april 2020 is het digitaal flexteam opgestart. Er is ingezet op innovatie en digitalisering in de volledige breedte (cybercrime, social media, instructiefilms, grafisch werk etc.). Doordat mensen vanuit basisteams werden geleverd aan het digitale flexteam kon men daar voldoende draagvlak creëren om wat te veranderen op het gebied van innovatie en digitalisering. Belangrijke onderwerpen waar men zich op wilde gaan richten waren digitale criminaliteit en cybercriminaliteit, sociale media, dienstverlening (webcare) en ondersteuning van basisteams (basisteamrecherches). Het project is opgezet door de sectorleiding en plaatsvervangend sectorhoofd. Zij hebben de beslissing gemaakt dat het een innovatief team moest worden. Vervolgens heeft de respondent met enkele collega's verder vorm gegeven aan het team, de doelen, de strategie en de inhoud.

Beschrijving project

Inhoud

Het digitaal flexteam bestaat op dit moment uit 5,6 FTE, wat neerkomt op 11 medewerkers die voor 50 tot 75 procent van hun tijd beschikbaar zijn voor het flexteam. De medewerkers zijn wijkagenten, medewerkers van intake en service en personen die een achtergrond hebben in de recherche. Er zijn vier pijlers waar het digitaal flexteam zich op richt: (1) jeugd- en wijkagenten van basisteams, (2) opsporing, (3) Intake en Service en (4) sociale media en web care. Per pijler worden er verschillende projecten opgezet en activiteiten uitgevoerd. De respondent geeft aan dat er niet een hele duidelijke lijn in het project zit. Veel van de activiteiten komen op en men gaat er vervolgens mee aan de slag. Deze vrijheid heeft men bij aanvang van het project gekregen. Een van de eerste activiteiten is het bijspijkeren en faciliteren van intake en service medewerkers op het gebied van cybercrime.

Een voorbeeld van een project is het project digitaal bewust. Onder dit project vallen verschillende activiteiten, zoals dat collega's in de basisteams elke maand 3 prikkels krijgen rondom het thema (voorbeelden zijn het ophangen van een QR-code waarmee men in een virtuele doorzoeking terecht komt met digital devices, een quiz en het verspreiden van malafide QR-codes en mails. Men wil dit project afsluiten met

een evenement waarbij collega's met hun expertise workshops gaan geven op basis van de input die uit de prikkels wordt verkregen. De prikkels worden namelijk zoveel mogelijk meetbaar gemaakt, zodat men bijvoorbeeld weet hoeveel collega's op een malafide link reageren. Op deze manier kan aan collega's worden teruggegeven hoe ze zich gedragen. Het flexteam probeert politiemensen enerzijds te betrekken en anderzijds te triggeren met laagdrempelige, innovatieve ideeën.

Doel
Het hoofddoel van het digitaal flexteam IJsselland is het creëren van een digitaal vaardiger district.

Doelgroepen
De doelgroep betreft voornamelijk mensen binnen de politie organisatie. Specifiek de basisteamrecherches en basisteams zelf, maar ook andere teams (zoals TDO) die rondom de basisteams werken omdat men die teams probeert te verbinden met de basisteams.
Een andere doelgroep betreft mensen buiten de organisatie zoals ouderen of jongeren, waar men zich op richt met betrekking tot preventie. Aan ouderen wilde men bijvoorbeeld laagdrempelig via interviews en wijkkrantjes aangeven wat cybercriminaliteit is. Met betrekking tot preventie heeft het flexteam vooral een aanjaagfunctie: signaleren welke initiatieven er zijn (zoals HackShield) en dat proberen te laten landen bij de basisteams.

Niveau
Het digitaal flexteam IJsselland is opgezet op districtsniveau en richt zich voornamelijk op de verschillende basisteams binnen het district. Verder richt men zich vooral op gedigitaliseerde criminaliteit, cybercriminaliteit is meer de verantwoording van het regionale cybercrimeteam. Voor digitale bewustwording/awareness van collega's op straat is cybercrime wel belangrijk.

Onderbouwing

Verwachte werking
Er worden verschillende verwachtingen uitgesproken over waarom het flexteam zorgt voor een digitaal vaardiger district. Ten eerste verwacht men dat er draagvlak ontstaat binnen de basisteams voor het thema, omdat het flexteam bestaat uit mensen die zelf uit basisteams komen die naast de andere collega's staan. Daarnaast is er meer slagkracht omdat er in teamverband wordt gewerkt met meerdere mensen met verschillende expertises. Op deze manier is er niet maar een iemand die moet lobbyen voor het thema, zoals dat bijvoorbeeld het geval is bij een digitale wijkagent. Ten slotte probeert men zoveel mogelijk collega's te betrekken (zoals bij het project digitaal bewust), zodat er een participatiemaatschappij ontstaat binnen de politie.

Bijhouden werking
In het begin van het project zijn enquêtes onder medewerkers verspreid om de stand van zaken op dat moment vast te leggen. Verder zijn er verschillende kleine evaluatiemomenten ingebouwd. Bij de meeste activiteiten wordt namelijk uitgevraagd wat de gebruikservaringen zijn, of er dingen aangepast kunnen worden en of dingen beter kunnen. Een voorbeeld is een evaluatie van hulpmiddelen voor aangevers van cybercrime. Op het moment dat een aangever een hulpmiddel krijgt, wordt actief gevraagd in de laatste vragen wat iemand van het document vond en of de taal begrijpelijk was etc. Dit wordt actief gemonitord zodat men waar nodig aanpassingen kan doen. Voor eigen administratie wordt bijgehouden welke projecten men doet, hoe dat gedaan is en wat er is gedaan en of doelen zijn behaald. Intake en Service medewerkers zijn bijvoorbeeld in het district IJsselland opgeleid op het gebied van cyber waardoor men minder schroom heeft om een aangifte op te nemen en waardoor een aangever van een cyberdelict minder vaak benaderd hoeft te worden om uiteindelijk een volledige aangifte te krijgen. Nu levert de aangever alle informatie aan door het hulpmiddel en heeft de medewerker I&S een handleiding met werkinstructie. Ten slotte wordt er vanuit het Lectoraat Maatschappelijke Veiligheid van Saxion Hogeschool onderzoek gedaan naar het leereffect en knelpunten binnen het digitaal flexteam IJsselland.

Doelen behaald?
Het grootste gedeelte deel van de doelen wordt volgens de respondent behaald. Een voorbeeld waarbij doelen niet zijn behaald is dat in het district 'webcare' verplaatst is van de basisteams naar het Regionaal Service Centrum (RSC) [17], waardoor capaciteit ontstond bij basisteams die ingevuld zou moeten worden met een social media coördinator. Dit is uiteindelijk niet gebeurd. Redenen waardoor een doel vaak niet gehaal wordt hebben te maken met commitment vanuit de organisatie en de organisatiecultuur.

17 Het Regionaal Service Centrum is het voorportaal van de politie waar burgers contact kunnen opnemen met de politie, ook wel bekend als het landelijk servicenummer 0900-8844.

Samenwerking

Doordat de leden van het flexteam netwerken en verbinden worden er veel samenwerkingsverbanden aangegaan. Het aantal personen waarmee wordt samengewerkt is daarom 50 tot 70 mensen, waaronder wijk- en jeugdagenten, collega's van het regionale cybercrimeteam en collega's van de afdeling communicatie. De volgende partners worden aangemerkt:

- Intern (binnen de politie): intake en service (I&S), team digitale opsporing (TDO), regionale cybercrimeteam, expertisecentrum digitale opsporing (ECDO), project intensivering aanpak cybercrime (PIAC), district Twente en een portefeuillehouder GGP.
- Extern (buiten de politie): scholen, gemeentes, jongerenwerk.

De samenwerking met het district Twente bestaat uit het delen van kennis en actief samenwerken om een groter gebied te bestrijken en meer te kunnen bereiken.

Vanwege de covid epidimie is de samenwerking met externe partijen wat verwaterd. Men was met scholen bezig om voorlichting te geven aan leerlingen en docenten over bijvoorbeeld sexting en money muling. Verder probeert men met gemeenten in de vorm van bestuursrechtelijke aanpakken samen te werken, zoals een 'moneymule caese and desist' aanpak en een samenwerking met HackShield. Deze zijn echter nog niet van de grond gekomen.

Afspraken
Er zijn enkele afspraken intern gemaakt. Zo is met het regionale cybercrimeteam afgesproken dat alle communicatie richting het district via het digitaal flexteam moet gaan. Met district Twente zijn mondelinge afspraken gemaakt over de samenwerking. Verder

zijn er weinig formele afspraken gemaakt. De afspraken die zijn gemaakt zijn mondeling en op basis van vertrouwen.

Kwaliteit samenwerking
De kwaliteit van de samenwerking verschilt volgens de respondent bij de verschillende samenwerkingspartners. De samenwerking met partners die zich bezighouden op het gebied van cybercrime gaat goed, daar zit veel dynamiek en energie. Er is echter ook een conservatieve kant binnen de organisatie die (nog) niet inzien dat een groot deel van wat men binnen het digitaal flexteam doet hun werk van de toekomst gaat zijn. Binnen deze kant van de organisatie is veel weerstand. Een verklaring voor dit verschil ligt deels in de affiniteit die men heeft met een digitale component, politiewerk is bijvoorbeeld altijd fysiek geweest. Het is een uitdaging om deze mindset te veranderen.

Verbeterpunten samenwerking
Winst in de samenwerking kan worden behaald door meer resultaten te delen, mensen mee te nemen en mogelijkheden en risico's op het gebied van digitalisering te laten zien. Bijvoorbeeld in het geval van een huiszoeking de collega attenderen op de deurbel die filmopnames maakt en wat daar mee kan gebeuren. Daarnaast is het team een pilot en merkt men dat organisatie commitment het soms laat afweten waardoor niet de volledige kracht uit het team gehaald wordt. Respondent denkt dat dit voor de hele cyber ontwikkeling geldt.

Implementatie praktijk

Het project is deels vormgegeven zoals men dat heeft beoogd, omdat het project is ingestoken op basis van innovatie. Verder zijn er projecten die niet bij aanvang zijn bedacht maar wel zijn uitgevoerd en zijn er projecten bedacht maar niet uitgevoerd. Dit is volgens de respondent een logisch onderdeel van vernieuwing.

Het project wordt steeds geëvalueerd en op basis daarvan aangepast. Een voorbeeld is dat men als pijler eerst wijk- en jeugdagenten wilden bereiken, maar dat dit is aangepast naar de gehele basisteams. Een ander voorbeeld is op het gebied van opsporing, waar men uiteindelijk niet onderzoeken naar zich toe heeft getrokken, maar meer is gaan adviseren hoe het klassieke karakter van de opsporing ingezet kan worden in de opsporing naar gedigitaliseerde- en cybercriminaliteit.

Implementatie schaal & intensiteit
De respondent denkt dat het team op de juiste schaal is geïmplementeerd omdat betrokkenheid van collega's uit basisteams lastig is te bewerkstelligen op eenheidsniveau. Wel zou er bijvoorbeeld op eenheidsniveau samengewerkt kunnen worden wanneer meerdere districten op dezelfde manier accenthouders op het gebied van digitalisering hebben binnen basisteam. Die kunnen dan weer worden gekoppeld aan het regionale cybercrimeteam zodat er een netwerk ontstaat.

Met betrekking tot de intensiteit bestaat het team nu uit 5,6FT, wat volgens de respondent genoeg capaciteit is om te kunnen werken aan de doelstelling. Echter staat de capaciteit momenteel door verloop onder druk. Mensen die opgeleid zijn in het flexteam en goed functioneren worden namelijk overgeplaatst naar andere teams zoals THTC en technische toezicht teams. Een mogelijke reden hiervoor is dat het flexteam geen vaste contracten kan aanbieden.

Toekomstplan
In 2021 wordt de gehele pilot van het flexteam geëvalueerd vanuit de politieorganisatie, wellicht met hulp van een externe partij. Men heeft de ambitie om als team verder te gaan en samen te werken met andere districten en eenheden.

Toepasbaarheid andere eenheden
De respondent vindt het lastig te zeggen of een digitaal flexteam toepasbaar is in andere eenheden, omdat het uiteindelijk een capaciteitsvraag is. Het concept zelf is goed te kopiëren.

4.3.5 Cyber support team

Eenheid Amsterdam

Introductie

Het initiatief 'cyber support team' in de eenheid Amsterdam bestaat uit de oprichting van een team van medewerkers uit het regionale cybercrimeteam (TDO) dat politiemedewerkers in de districten ondersteuning biedt op het gebied van cybercrime. De respondent is coördinator cybercrime binnen de eenheid en houdt zich voornamelijk bezig met beleid en het verzorgen van opleidingen rondom het thema.

Aanleiding

Een belangrijke aanleiding voor de oprichting van het cyber support team zijn de jaarlijkse kwantitatieve doelstellingen voor de eenheid. Ieder jaar moet namelijk een bepaald aantal cybercrime verdachten (maatschappelijke klasse F90[18]) door de politie worden aangeleverd aan het OM[19]. In de eenheid Amsterdam heeft men besloten om deze verplichting deels te beleggen bij het regionale cybercrimeteam en deels bij de vier districten. Tegelijkertijd waren er onderzoeken die lieten zien dat het kennisniveau binnen de districten nog onvoldoende was om cybercrime zaken op te pakken. Verder werd geconstateerd dat er onder politiemedewerkers behoefte was aan 'learning on the job', waarbij door iemand wordt meegekeken wat bijvoorbeeld opsporingskansen zijn en hoeveel capaciteit een zaak gaat kosten. Voorheen werd voor ad-hoc vragen het telefoonnummer van het regionale cybercrimeteam gebeld (ook wel de 'cyberphone' genoemd). Uiteindelijk heeft de teamleider van het regionale cybercrimeteam ervoor gezorgd dat er een aantal politiemedewerkers vanuit Team Digitale Opsporing (TDO) zijn vrijgemaakt om de districten te ondersteunen bij het behalen van de kwantitatieve doelstellingen. Een vergelijkbaar initiatief draaide ook in de eenheid Rotterdam. Begin 2021 is het project 'cyber support team' formeel gestart in de eenheid Amsterdam. Bij de opzet van het initiatief zijn de teamleider van het regionale cybercrimeteam en de teamchef specialistisch opsporing betrokken geweest.

Beschrijving project

Inhoud

Het cyber support team bestaat uit politiemedewerkers van het regionale cybercrimeteam (TDO) die een dag per week politiemedewerkers uit de districten ondersteunen op het gebied van cybercrime. De leden van het cyber support team hebben ervaring op het gebied van cybercrime doordat zij een IT-achtergrond hebben of al geruime tijd meedraaien in cybercrime opsporingsonderzoeken. Enerzijds zijn de cyber support leden een aanspreekpunt voor de districten (per district is er een aanspreekput), anderzijds organiseren zij op eigen initiatief activiteiten binnen de districten. Voorbeelden van deze activiteiten zijn een vragenuur, het geven van presentaties en ondersteuning bij opsporingsonderzoeken. Per district wordt een eigen invulling gegeven aan de rol als cyber support teamlid, mede omdat ieder district zich in een ander fase bevindt. Zo is er een district dat bijvoorbeeld al de kwantitatieve doelstellingen heeft gehaald en mensen met kennis en expertise heeft, maar is er ook een district waar continue andere problematiek speelt waardoor cybercriminaliteit geen prioriteit krijgt.

Cyber support leden hebben de opdracht gekregen om ook fysiek de districten in te gaan en met zoveel mogelijk relevante collega's contact te leggen. Om de twee weken komt het cyber support team bij elkaar om bevindingen en werkwijzen te bespreken.

Doel

Uiteindelijk dient er een structuur te ontstaan binnen het district die voorbereid is op de criminaliteit van de toekomst: cybercrime en gedigitaliseerde criminaliteit. Verder is een van de doelstellingen om de cijfers van het aantal cybercrimeverdachten te halen. Echter is het ook van belang om ervoor te zorgen dat de districten in staat zijn om het onderwerp effectief op te pakken. Niet alleen op het gebied van opsporing, maar ook bijvoorbeeld kennis krijgen over mogelijke alternatieve interventies, zoals Hack_Right.

Doelgroep

Het cyber support team richt zich vooral op politiemedewerkers die werkzaam zijn in de opsporing. Het gaat dan om zowel de districtsrecherches als de basisteamrecherches). In het kader van preventie kunnen ook basisteamcollega's, wijk- en jeugdagenten, operationele collega's binnen de districten worden gezien als een doelgroep. Verder behoren ook medewerkers van de afdeling intake en service tot de doelgroep.

Onderbouwing

Verwachte werking

Er zijn verschillend verwachtingen waarom het cyber support team een effectief middel is. Ten eerste blijkt uit onderzoeken en praktijkervaring dat er onvoldoende kennis en kunde is binnen de districten op het gebied van cybercriminaliteit. In de praktijk ziet men bijvoorbeeld dat zaken niet worden opgepakt of dat er wordt gezegd dat er geen opsporingsindicatie aanwezig is. Daarnaast blijkt uit onderzoeken dat het belangrijk is om politiemedewerkers 'on the job expertise' aan te bieden. Ook verwacht men dat het fijn is om één persoon te hebben waar vragen aan kunnen worden gesteld, zodat niet gezocht hoeft te worden naar de juiste persoon in de complexe politieorganisatie. Ten slotte kregen het regionale cybercrimeteam en andere specialistische afdelingen al veel vragen vanuit de districten. Door het cyber support team wordt dit meer gestructureerd.

18 Dit betreft delicten computercriminaliteit en wordt gedefinieerd als 'alle vormen van bezitsaantasting, waarbij de computer het middel van plegen is'.

19 Voor de eenheid Amsterdam is in de Nationale Veiligheidsagenda 2019-2022 vastgelegd dat er 36 cybercrime verdachten aangeleverd dienen te worden bij het OM in 2021. Binnen de eenheid is besloten dat de districten gezamenlijk verantwoordelijk zijn voor 30 verdachten bij het OM en het regionale cyberteam voor 6 verdachten.

Bijhouden werking
Op dit moment wordt de werking van het team nog niet bijgehouden. Het lijkt de respondent goed om een evaluatiemoment te plannen na een bepaalde periode dat het team actief is.

Samenwerking

Het cyber support team bestaat uit 5 leden die werkzaam zijn bij het regionale cybercrimeteam. Verder zijn de teamleider van het regionale cybercrimeteam, een tactisch coördinator en de respondent betrokken bij de opzet en ondersteuning van het cyber support team. De cyber support teamleden werken uiteindelijk samen met een grote hoeveelheid politiemedewerkers die zich op een manier bezighouden met cybercriminaliteit. Dit betreft politiemedewerkers uit de district- en basisteams zoals teamchefs, internetrechercheurs en wijkagenten die het onderwerp adresseren etc.

De leden en ondersteuners van het cyber support team komen om de twee weken bij elkaar om te bespreken waar men tegenaan loopt. De samenwerking van de leden met de districten verschilt per lid. Wel is het de bedoeling dat de leden zo nu en dan fysiek aanwezig zijn binnen de districten.

Afspraken
Een belangrijke concrete afspraak is dat de cyber support leden een dag in de week beschikbaar dienen te zijn voor hun district. Verder hebben de leden vrijheid om invulling te geven aan de werkzaamheden. Het cyber support team is voorlopig opgericht voor een onbepaalde tijd.

Kwaliteit samenwerking
De samenwerking wordt vanuit het perspectief van de respondent als positief ervaren. De reacties op de komst van de leden waren verschillend: in een van de districten werd het lid van het cyber support team ontvangen met de boodschap dat het al goed liep en in een ander district was de behoefte zo groot dat het lid al meteen overvraagd werd. Over het algemeen is de behoefte volgens de respondent groot, omdat er een digitale transformatie plaatsvindt binnen de politieorganisatie. In de ‘frontlinie’ wordt de druk en verschuiving vooral gevoeld.

Implementatie praktijk

Het cyber support team is op dit moment vorm gegeven zoals beoogd. Wel wordt aangegeven dat het mooier was geweest wanneer de leden meer tijd zouden krijgen voor hun werkzaamheden. Er zijn nog geen structurele of grote aanpassingen geweest binnen het project.

Wat goed gaat is dat er veel vragen zijn vanuit de districten en dat er goed gereageerd wordt op de leden. Minder goed gaat het bewaken van de grenzen van de cyber support leden met betrekking tot de mate van hulp en ondersteuning die wordt geboden. Een voorbeeld is dat een van de leden bijna zelf opsporingsonderzoeken aan het draaien is, wat niet de bedoeling is. Wat ook minder goed gaat, is dat binnen de organisatie soms beperkingen zijn omtrent capaciteit en mensen specifiek vrijmaken voor cybercriminaliteit.

Implementatie schaal & intensiteit
De schaal en intensiteit kunnen volgens de respondent worden verbeterd. Er wordt namelijk gezien dat de behoefte groter is dan de leden van het cyber support team op dit moment kunnen aanbieden. De intensiteit zou dan ook omhoog kunnen door meer cyber support leden beschikbaar te stellen of door de huidige cyber support leden meer tijd te geven voor de werkzaamheden.

Toekomstplan
Het uiteindelijke plan is om een structuur neer te zetten binnen het district, waarbij in teamplannen duidelijk naar voren komt wat districten en basisteams willen en kunnen doen op het gebied van cybercriminaliteit en gedigitaliseerde criminaliteit. Deze vormen van criminaliteit moeten in de toekomst als vast onderdeel van het werk worden gezien en mensen dienen vast gelabeld te worden op de onderwerpen zodat de capaciteit niet voor andere zaken kan worden ingezet. Uiteindelijk hoopt de respondent dat de cyber support leden zichzelf overbodig maken en dat ze eventueel alleen aanspreekpunt blijven, maar dat de districten wel zelfredzaam zijn.

Toepasbaarheid andere eenheden
Het concept wordt omschreven als goed toepasbaar binnen andere eenheden en er wordt vermoed dat de behoefte in andere eenheden net zo groot is. Met betrekking tot de benodigde capaciteit voor een cyber support team wordt opgemerkt dat nog niet alle regionale cybercrimeteams op de volledige sterkte van 20FTE zitten. Het is dus de vraag of er mogelijkheden zijn om binnen het desbetreffende cybercrimeteam capaciteit vrij te maken. In Rotterdam is zoals eerder besproken al een soortgelijk team ingericht.

4.3.6 Workshop Cybercrime

Eenheid Amsterdam

Introductie

Tijdens het project 'workshop cybercrime' leren politiemedewerkers die werkzaam zijn binnen de eenheid Amsterdam aan de hand van een cybercrimecasus meer over cybercrime en digitale opsporingsmogelijkheden. De workshop duurt ongeveer een dag en is 15 tot 20 keer gedraaid tussen 2018 en 2020. De respondent is coördinator cybercrime, binnen de afdeling TDO (Team Digitale Opsporing), het regionale cybercrimeteam. Werkzaamheden zijn vooral op het gebied van beleid (de vertaalslag maken van de landelijke cybercrime strategieën naar de eenheid), maar ook het verzorgen van opleidingen.

Aanleiding

De voornaamste aanleiding is dat er in de districten nog veel politiecollega's zijn die onvoldoende kennis en kunde hebben van cybercrime om ermee aan de slag te kunnen. Dit merkte de respondent vanuit de praktijk door vragen die worden gesteld over cybercrime, maar ook wetenschappelijk onderzoek heeft dit kennistekort laten zien[20]. Ondanks dat er extern opleidingen worden ingekocht, is er volgens de respondent een grote behoefte aan praktijkervaring ('learning on the job'). Een groep collega's vanuit TDO was daarom op zoek naar een vernieuwende manier om andere collega's enthousiast te maken voor het thema cybercrime, onder de vlag van de Opsporingsacademie[21]. Er was geen geld beschikbaar voor een dergelijk initiatief, maar wel kennis en goedkeuring vanuit de leiding om er tijd aan te besteden. Het idee was om een 'serious gaming' concept in te zetten omdat men ziet dat dit goed werkt bij politie collega's vanwege de actieve en praktische manier van leren. In een leegstaand cellencomplex is de infrastructuur hiervoor neergezet met eigen middelen en apparatuur van collega's. Er is gekozen voor een casus over sextortion, omdat dit een delict is waarmee collega's de impact voelen. Het gaat in de casus om een Icloud hack, daarmee een vorm van cybercrime. Bij de opzet zijn TDO en de Opsporingsacademie betrokken geweest.

Beschrijving project

Inhoud

De workshop cybercrime is een kennismaking met cybercrime waarin mensen cybercrime kunnen herkennen en de eerste stappen kunnen maken in het opsporingsproces. Elementen die in de workshop zitten zijn bijvoorbeeld internet rechercheren, het opnemen van een goede aangifte en sporen veilig stellen. De workshop bestaat uit een trainingsdeel, een escape room en een presentatie. Tijdens het trainingsdeel wordt eerst voorkennis van deelnemers bevraagd en krijgt men een introductie over cybercrime. Voorkennis wordt bevraagd zodat organisatoren een beeld krijgen van de al aanwezige en ontbrekende kennis en zodat de inhoud van de workshop hier op kan worden afgestemd. De training bestaat uit drie onderdelen: aangifte, OSINT ('open source intelligence') en sporen veilig stellen.

- **Aangifte** – Men krijgt eerst een aangifte over sextortion met veel fouten erin zoals dit vaak in de praktijk voorkomt. Vervolgens komt er een fictief slachtoffer langs en moeten collega's een aanvullende aangifte opnemen. Het onderdeel wordt vervolgens klassikaal besproken.
- **OSINT** – Eerst wordt er klassikaal door een docent (internet rechercheur) informatie gegeven over OSINT. Vervolgens staan er laptops waarmee deelnemers online sporen opzoeken met betrekking tot de sextortion zaak. Ook dit wordt na afloop klassikaal besproken.
- **Sporen veilig stellen** – Dit onderdeel gaat over welke sporen er in 'devices' zoals een mobiele telefoon kunnen worden teruggevonden. Hierbij krijgt men eerst een introductie over UFED reader[22]. Vervolgens moeten deelnemers sporen zoeken in een zelfgemaakte database. Ten slotte is er weer een klassikale bespreking.

Na het trainingsdeel is er een escaperoom en een presentatie vanuit TDO. Tijdens de escaperoom komen alle leerelementen van de training terug en moeten deze worden toegepast om uit de escaperoom te komen. Een voorbeeld hiervan is dat er een puzzel is waarbij foutieve en goede IP-adressen moeten worden herkend om verder te komen. Tijdens de presentatie van TDO wordt uitgelegd welke specialismen en 'tools' men binnen TDO heeft en wat dat betekent voor de overige collega's.

Doel

Het doel van de cybercrimeworkshop is om 'collega's handvatten te geven om cybercrime onderzoeken op te pakken en hen bewuster te maken van digitale (on)mogelijkheden'.[23] Daarnaast zijn er een aantal leerdoelen geformuleerd[24], zoals zorgen dat politiemedewerkers in staat zijn om cybercrime te herkennen, dat politiemedewerkers de impact van cybercrime op slachtoffers begrijpen en in staat zijn om door middel van open bronnen relevante informatie te verzamelen voor een onderzoek.

Doelgroep

De doelgroep betreft alle politiemedewerkers binnen de eenheid Amsterdam. Bij de tot nu toe uitgevoerde workshops waren politiemedewerkers vanuit verschillende niveaus en functies. De Opsporingsacademie is normaal gesproken alleen bedoeld voor mensen uit de opsporing, maar deze specifieke workshop is breder uitgezet. In het nieuwe plan voor de workshop staat dat men de doelgroep wil opdelen in specifieke groepen: I&S (intake en service) en mensen in de richting opsporing. De reden hiervoor is dat I&S uiteindelijk geen onderzoek hoeft te doen en apparaten hoeft uit te lezen. Verder wil men in de toekomst politieme-

20 Zie bijvoorbeeld Leukfeldt et al. (2012) en Boekhoorn (2019).

21 De opsporingsacademie is een concept binnen de politie waarbij voor- en door collega's kennis en kunde wordt overgedragen. Het concept is begonnen in de Eenheid Noord-Holland en wordt nu landelijk uitgerold.

22 Een programma waarin uitgelezen informatie uit mobiele telefoons gestructureerd wordt gepresenteerd.

23 Het doel van de workshop cybercrime zoals omschreven in 'voorstel structurele escaperoom' (z.d.)

24 De leerdoelen zijn beschreven in een wervingsflyer van de Opsporingsacademie eenheid Amsterdam (Opzet Workshop Cybercrime Opsporingsacademie, z.d.).

dewerkers uit de basisteams betrekken in verband met veelvoorkomende delicten zoals vriend in nood fraude.

Onderbouwing

Verwachte werking

Men verwacht om verschillende redenen dat de eerder geformuleerde doelen worden bereikt:

- Er is veel onwetendheid op het gebied van cybercrime en lijkt voor veel politiemedewerkers een 'ver van de bed show'. Met de workshop wordt het thema dichterbij gebracht.
- De verwachting is dat politiemedewerkers enthousiast worden waardoor een beweging wordt gecreëerd van ambassadeurs op het digitale thema.
- Het is laagdrempelig, betreft slechts een dag en legt daardoor weinig druk op de capaciteit
- Men gelooft in het concept voor- en door collega's, waardoor contact (met bijvoorbeeld TDO) ook na de workshop makkelijk wordt gelegd.
- De kennis die wordt aangeboden, komt vanuit specialisten binnen de politieorganisatie.
- Er zitten didactische elementen in de workshop.
- 'Serious gaming' concepten sluiten goed aan bij de politie.

Daarnaast zijn er verschillende aannames die men heeft rondom het project. Zo veronderstelt men dat de kwaliteit van aangiftes onvoldoende is, dat OSINT kennis onvoldoende is, dat het voor collega's lastig is om cybercrime te herkennen en dat collega's het lastig vinden om zelf apparaten uit te lezen. De respondent vindt het lastig om te benoemen of er iets verder zou moeten worden onderbouwd aan het project.

Bijhouden werking

De mate waarin de doelen van het project worden behaald wordt niet stelselmatig bijgehouden. Wel zijn er standaard evaluatieformulieren vanuit de opsporingsacademie die collega's invullen na de workshop. Op deze manier zijn ervaringen en feedback van deelnemers verzameld en bekeken. Er is geen kennis getoetst in de evaluatieformulieren. De kennis probeert men te testen met behulp van de escaperoom, waarin men kennis uit de workshop dient te gebruiken om uit de escaperoom te komen.

Samenwerking

Bij het project is samengewerkt met verschillende mensen binnen de politie:

- Een vaste groep van 5 à 6 mensen vanuit de Opsporingsacademie
- Een flexibele schil van ongeveer 8 mensen die als docenten ingezet kunnen worden
- 2 cybervrijwilligers die enkele keren het OSINT deel van de workshop hebben gegeven

Vanuit de Opsporingsacademie heeft men de administratie verzorgd, uitnodigingen verstuurd, aanmeldingen beheerd en feedback verzameld. Tijdens een workshop is een groep van ongeveer 7 mensen betrokken: de cybercrime teamleider, een fictief slachtoffer, iemand van TDO, een OSINT specialist en iemand voor de begeleiding in de escaperoom. Er waren standaard presentaties die klaar lagen voor de verschillende onderdelen, maar docenten hadden de ruimte om hier verder een eigen draai aan te geven.

Afspraken

Vooraf is met de Opsporingsacademie afgesproken hoe vaak de workshop zou worden gegeven (4 à 5 keer in het voorjaar en 4 à 5 keer in het najaar) en hoeveel deelnemers er zouden meedoen (16 is het maximum). Met leidinggevenden van docenten is afgesproken dat er ruimte was om aan de workshop bij te dragen. Deze afspraken zijn mondeling vastgelegd, niet schriftelijk. Over de duur van de samenwerking zijn geen afspraken gemaakt.

Kwaliteit samenwerking

De samenwerking met de Opsporingsacademie wordt als goed en fijn omschreven vanuit het perspectief van de respondent. Het scheelde veel werk dat zij een deel van organisatie en administratie uit handen hebben genomen. Verder was men in de samenwerking met docenten afhankelijk van het enthousiasme en de wil van docenten om bij te dragen. De samenwerking met de docenten was goed omdat mensen enthousiast waren en het leuk vonden om de kennis over te brengen. Dat de samenwerking met docenten losser was maakte het bij ziekte lastig om iemand anders te vinden.

Verbeterpunten samenwerking

De samenwerking zou kunnen worden verbeterd door vooraf de verwachtingen duidelijk te maken aan docenten over hoe vaak en wanneer een workshop wordt gegeven en hoeveel tijd dit kost.

Implementatie praktijk

Het project is volgens de respondent geïmplementeerd op de manier waarop van te voren was beoogd. Vooraf is de keuze gemaakt om met een 'houtje-touwtje' oplossing te starten in plaats van de officiële weg te bewandelen voor toestemming en financiële middelen. Met minimale middelen heeft men een zo groot mogelijk bereik en impact proberen te creëren. Tussendoor is de workshop cybercrime geëvalueerd met de eerder besproken evaluatieformulieren. Aanpassingen hebben tussendoor plaatsgevonden. Een voorbeeld hiervan is een aanpassing in de escaperoom, omdat deze te lastig bleek te zijn. Men heeft toen een eigenaar van een escaperoom bedrijf gevraagd voor input. Andere aanpassingen zijn de tijd die docenten hebben besteed aan de instructies/ voorlichting.

Wat volgens de respondent goed is gegaan is dat er veel intrinsieke motivatie was bij mensen om zich aan te melden voor de workshop en dat mensen in een korte tijd kennis is meegegeven waar ze wat mee kunnen in de praktijk. Wat beter had gekund is de differentiatie in het niveau van de workshop, vanwege de niveauverschillen tussen deelnemers.

Implementatie schaal & intensiteit

Er waren nog veel mensen die wilden deelnemen aan de workshop, dus de respondent geeft aan dat hoe vaker de workshop wordt georganiseerd, hoe beter (zolang er animo is). Daarnaast is de workshop wellicht ook geschikt om met enkele aanpassingen aan te bieden aan collega's van het

Openbaar Ministerie of gemeenten. Verder zou de inhoud verspreid kunnen worden over twee dagen, omdat uit feedback bleek dat het voor sommige mensen teveel informatie was op een dag. Aan de andere kant kan dit volgens de respondent ervoor zorgen dat het teveel capaciteit kost om mee te doen.

Toekomstplan
Op dit moment is de locatie en de apparatuur die men had niet meer beschikbaar, waardoor de workshop stil ligt. Er is een nieuw plan geschreven voor de workshop dat is goedgekeurd door de eenheidsleiding en waarvoor geld beschikbaar is gesteld. De workshop heet in het plan de 'Cyber Cop Academy'. Op dit moment is men op zoek naar een geschikte locatie om het project opnieuw vorm te geven. De workshop is geen vervanging voor bestaande opleidingen, maar een manier om mensen te introduceren in het onderwerp cybercrime.

Toepasbaarheid andere eenheden
Het project is volgens de respondent goed toepasbaar binnen andere eenheden. Met betrekking tot materiaal, is voor het trainingsgedeelte alleen een trainingsruimte nodig. Voor de escaperoom is ook infrastructuur nodig, zoals laptops, muziekinstallaties en andere technische middelen. Niet in alle eenheden is nog een Opsporingsacademie, maar indien er mensen zijn die de administratie op zich willen nemen is dit goed mogelijk volgens de respondent.

4.3.7 KOR3NWOLF

Eenheid Limburg

Introductie

Het initiatief Kor3nwolf betreft een fictieve casus om de digitale kennis en vaardigheden van politiemedewerkers te verbeteren. De respondent is werkzaam als analist bij het regionale cybercrimeteam van de eenheid Limburg. Het regionale cybercrimeteam valt in de eenheid onder de Dienst Regionale Recherche (DRR).

Aanleiding

Het initiatief Kor3nwolf is ontstaan nadat de respondent de casus 'Pink Lady' heeft doorlopen tijdens een IBT-dag[25] in de eenheid Noord-Nederland. 'Pink Lady' is een 'real-life' casus waarbij een ziekenhuis wordt gehackt en deelnemers vervolgens observaties en aanhoudingen dienen te verrichten. Omdat de respondent zag dat collega's door een dergelijke casus loskwamen op het onderwerp cyber is de casus omgeschreven en aangepast voor de eenheid Limburg. Omdat de casus in Noord-Nederland een beperkte schaalbaarheid had (10 mensen per dag) heeft men de casus wel aangepast waardoor hij op grotere schaal is te doorlopen. Andere factoren die er uiteindelijk voor hebben gezorgd dat het initiatief in Limburg is ontstaan, zijn de capaciteit die is geleverd vanuit het cybercrimeteam en het IBT-centrum. Daarnaast werd het belang erkend binnen de eenheid waardoor er middelen beschikbaar werden gesteld. De Kor3nwolf casus in Limburg is opgezet in samenwerking met IBT, Team Digitale Opsporing (TDO) en het cybercrimeteam. Verder is aan collega's van het digitale platform gevraagd welke vragen men daar het meest binnen krijgt van collega's en over welke onderwerpen collega's het minst weten. Dit heeft men geprobeerd te verwerken in de casus. Augustus en september 2019 is de casus Kor3nwolf voor het eerst doorlopen in de eenheid Limburg.

Beschrijving project

Inhoud
Kor3nwolf is een fictieve casus die is gebouwd op een 'capture the flag (CTF)-platform'[26]. De casus is bedoeld om collega's binnen de politieorganisatie digitaal bewust te maken. Tijdens de casus komt er een melding binnen van een Limburgs bedrijf dat digitaal wordt afgeperst en bitcoins moet betalen. De CTF bestaat uit kleine opdrachten die men steeds vanachter een computer moet oplossen om verder te komen. Spelenderwijs worden de deelnemers in groepen door de casus heen geholpen. Zo moeten er bitcoin adressen worden opgezocht, dient men open bronnen onderzoek te verrichten en moet er een PV (proces verbaal) van verdenking bij worden gehouden. Andere onderwerpen waar men wat over leert zijn digitale sporen, inbeslagname van een telefoon en het indienen van vorderingen bij bijvoorbeeld tech-bedrijven. Er is ondersteuning voor deelnemers tijdens de casus in de vorm van begeleiders die

25 Een Integrale Beroepstraining (IBT) is een training voor politiemedewerkers om hun vaardigheden (zoals aanhoudings- en schietvaardigheden) te onderhouden. Iedere politie-eenheid heeft een eigen IBT centrum die dergelijke trainingen organiseert.

26 Een CTF platform is een omgeving waarin stapsgewijs (door deeltaken te volbrengen) kennis en vaardigheden kunnen worden opgedaan.

rondlopen, informatie op A4'tjes en hints die achter de CTF-challenges zitten. De casus duurt rond de 2 uur en is ongeveer 25 keer ingezet (tijdens IBT-dagen en incidenteel).

Doel
Het doel van de casus is om op een laagdrempelige manier politiemedewerkers bekend te maken met de digitale mogelijkheden binnen hun werk, ook wel omschreven als het wegenemen van 'koudwatervrees'. Verder is het doel om de collega's kennis te laten maken met het digitaal platform en het cybercrimeteam. De doelen zijn niet zozeer van te voren opgesteld, maar steeds mondeling aangegeven en toegelicht richting betrokkenen.

Doelgroep
De casus is geschreven voor politiemedewerkers die werkzaam zijn binnen de opsporing, zoals medewerkers in de opsporing van de basisteams, districtsrecherche en regionale recherche. Voor intake- en service medewerkers is de casus ook interessant volgens de respondent, echter moet de casus dan wel worden aangepast aan hun werkzaamheden. In totaal hebben ongeveer 250 tot 300 medewerkers de casus doorlopen tijdens de IBT-dagen. Verder is de casus nog ingezet tijdens teamdagen van verschillende afdelingen binnen de politie. Daarnaast is de casus recent gedraaid tijdens operatie Volt[27] voor mensen van buiten de politieorganisatie. Voor dit evenement is de casus op enkele punten aangepast en wat moeilijker gemaakt.

Niveau
De casus is gespeeld op het niveau van basisteams, districtsrecherches en regionale recherches binnen de eenheid Limburg.

Onderbouwing

Verwachte werking
Er wordt verwacht dat de casus bijdraagt aan het wegnemen van de 'koudwatervrees' rondom de digitale aspecten van het politiewerk, omdat de respondent ten eerste zelf heeft ervaren hoe de casus 'Pink Lady' werkte in Noord-Nederland. Daarnaast is de casus een 'gewone' casus met digitale tintjes waardoor deze dicht bij de belevingswereld staat van de deelnemers. Ten slotte wordt verwacht dat veel oefenen helpt om de digitale vaardigheden bij de deelnemers te versterken. De casus is verder niet gebaseerd op wetenschappelijke of praktijkgerichte theorieën, wel is bekend dat 'gamification' en 'CTF-challenges' goed werken.

Bijhouden werking
Voordat deelnemers de casus doorliepen hebben zij een enquête ingevuld. In de enquête zijn bijvoorbeeld vragen gesteld over de kenmerken van deelnemers (leeftijd, functie, etc.), bekendheid met het cybercrimeteam, de hoeveelheid cyber gerelateerde zaken waarmee deelnemers te maken hebben en of deelnemers vonden dat zij over voldoende kennis beschikten. Er heeft uiteindelijk geen vervolg meting plaatsgevonden nadat de deelnemers de casus hebben doorlopen.

27 Operatie Volt is een evenement van de politie en het Ministerie van Defensie waarin mensen van buiten de politie kennis maken met de werkzaamheden van de politie en Defensie op het gebied van IT.

Doelen behaald?
Men vindt het lastig om te bepalen of de doelen worden behaald. Wel zijn er meer aanmeldingen op de nieuwsbrief van het cybercrimeteam en heeft men het idee dat er vaker contact wordt opgenomen met het cybercrimeteam.

Samenwerking

Voor het ontwikkelen en uitvoeren van de casus is samengewerkt met verschillende afdelingen binnen de politie-eenheid Limburg. Zo heeft het IBT-centrum zorg gedragen voor de planning van de IBT-dagen, heeft TDO geholpen bij het formuleren van de hulpvraag en heeft het cybercrimeteam gefaciliteerd door ruimte te geven aan collega's binnen het cybercrimeteam om de casus te draaien. Ten slotte heeft het iLab (innovatie lab) van de politie Limburg) geholpen in de ondersteuning van het plan.

Afspraken
Er zijn afspraken gemaakt met het IBT-centrum over de momenten waarop de casus zou worden ingepland tijdens de IBT-dagen. Daarnaast zijn medewerkers enkele medewerkers (grotendeels) vrijgemaakt om de begeleiding tijdens de casus te verzorgen. Verder zijn er geen formele afspraken gemaakt. Met betrekking tot de duur is afgesproken dat er 10 dagen ingepland zouden worden waarop de casus zou worden doorlopen en verder is afgesproken om de casus bij interesse ook incidenteel in te zetten buiten IBT-dagen om.

Kwaliteit samenwerking
De kwaliteit van de samenwerking wordt als goed ervaren. Vanuit IBT is men op zoek naar inhoudelijke invulling van de IBT-dagen, waardoor het initiatief goed aansloot. Ook collega's binnen TDO, het cybercrimeteam en het digitaal platform waren enthousiast over het idee en konden ruimte maken. De samenwerking bestond uit af en toe bellen en afstemmen. Er zijn verder geen ideeën over hoe de samenwerking verbeterd zou kunnen worden.

Implementatie praktijk

Het initiatief is op dit moment vormgegeven zoals beoogd. Tijdens een pilot middag is de casus proef gedraaid zonder CTF systeem. Omdat deelnemers toen nog teveel hulp nodig hadden heeft men uiteindelijk een CTF platform gekoppeld aan de casus. Men merkte dat dit goed werkte omdat er zelfstandiger gewerkt kan worden en de opdracht zo in verschillende onderdelen werd opgeknipt.

Wat men goed vindt gaan rondom de casus is de samenwerking tussen de afdelingen die betrokken zijn bij de opzet en uitvoering van het initiatief en dat deelnemers elkaar spontaan dingen uit leggen tijdens de casus. Wat minder goed is gegaan is dat er ook collega's bij zaten die minder open stonden voor de casus en daardoor passief waren. Ook is uiteindelijk de vraag in hoeverre de kennis blijft hangen. Er is daarom nog informatie nagestuurd aan de deelnemers.

Implementatie schaal & intensiteit
Op dit moment zijn ongeveer 250 tot 300 van de 900 politiemedewerkers bereikt binnen de opsporing in de eenheid Limburg. Een nadeel van de implementatie via IBT-dagen is dat in principe alleen collega's worden bereikt die hieraan deelnemen (niet-wapen dragende collega's worden bijvoorbeeld niet bereikt). De casus is echter ook nog een aantal keer los gedraaid, voor

bijvoorbeeld collega's binnen de financiële opsporing. De duur van 2 uur per keer wordt als voldoende ervaren omdat de concentratie na 2 uur vaak op is bij de deelnemers.

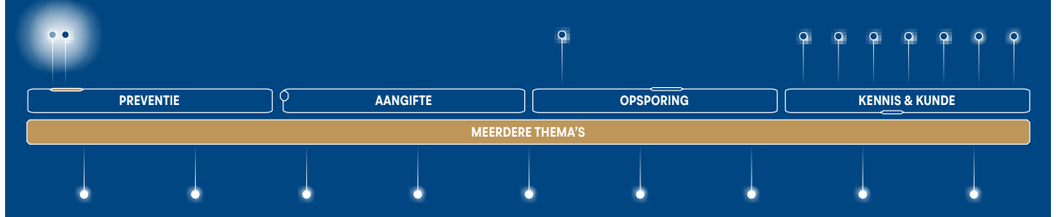
Toekomstplan
Er zijn ideeën om een nieuwe casus te schrijven, wat wel veel werk vereist omdat er een nieuwe gameplay moet worden bedacht. De huidige casus is makkelijk aan te passen en makkelijk te verspreiden, zoals bijvoorbeeld is gedaan voor operatie Volt. Kor3nwolf wordt op dit moment niet meer bij IBT aangeboden, maar er is een kans dat dit volgend jaar wel weer zal gebeuren. Er wordt wel opgemerkt dat inmiddels veel mensen binnen de eenheid de casus hebben doorlopen.

Toepasbaarheid andere eenheden
Een dergelijke casus is volgens de respondent goed toepasbaar binnen andere eenheden. De casus zou rechtstreeks over genomen kunnen worden, door bestanden over te dragen en uitleg te geven over de implementatie. Verder moet er wat capaciteit worden vrijgemaakt om de casus te begeleiden en is er een technisch onderlegde medewerker nodig om de CTF bijvoorbeeld op een server te zetten en die goed te beveiligen. Bij het rechtstreeks overnemen is het wel goed om te vermelden dat er enkele lokale aspecten in de casus zijn verwerkt (het getroffen bedrijf is bijvoorbeeld lokaal). Een van de andere politie-eenheden in Nederland en de Rijksrecherche (OM) wilden de casus ook graag overnemen, echter is het onduidelijk of zij de casus uiteindelijk hebben geïmplementeerd.

4.4 Meerdere fasen van het politiewerk

Er zijn in totaal negen initiatieven geïdentificeerd die zich op twee of meer fasen van het politiewerk tegelijkertijd richten: 'Project Vriend in Nood-fraude', 'Digitaal District', 'Cyberspecials', 'Cyberdriehoek', 'Aanpak geldezels', 'Cyber HQ', 'Digikamers', 'Digitaal weerbaar Breda' en 'Dagelijkse Cyberquery' (zie figuur 4). De initiatieven worden nu individueel besproken.

Figuur 4: initiatieven die zich op twee of meer fasen van het politiewerk tegelijkertijd richten



4.4.1 Project Vriend in Nood-fraude

Oost-Nederland

Introductie

Het project vriend in nood-Fraude (VIN-fraude) bestaat uit een (deels geautomatiseerd) centraal ingerichte werkwijze waarin aangiften van dit delict worden verrijkt met opsporingsindicatie, zodat basisteams de opsporingsonderzoeken verder kunnen afhandelen. De respondent is projectleider van het project 'vriend-in-noodfraude'.

Aanleiding

Er zijn verschillende aanleidingen aan te wijzen voor het ontstaan van het VIN-fraude project. Ten eerste heeft het cybercrimeteam in Oost-Nederland het thema vriend in nood-fraude[28] toegewezen gekregen. In 2020 werd een sterke toename van dit delict waargenomen. Daarnaast heeft het hoofd van de informatieorganisatie in Oost-Nederland een ICT-achtergrond. Toen het cybercrimeteam onder zijn verantwoordelijkheden viel zag deze persoon veel mogelijkheden om geautomatiseerd te gaan werken. Ten slotte wordt de beleving van politiemensen als aanleiding genoemd, omdat zij het lastig vinden om weinig te

28 Bij VIN-fraude stuurt een fraudeur berichten naar een slachtoffer waarin hij of zij zichzelf voordoet als een naaste of bekende, met het verzoek om geld over te maken. Slachtoffers maken dan geld over in de veronderstelling dat zij het naar een bekende overmaken.

kunnen doen tegen de hoge schadebedragen en grote aantallen onschuldige slachtoffers. Begin 2020 is ongeveer het startpunt geweest van het project.

Beschrijving project

Inhoud

Het project heeft ten eerste bestaan uit het inrichten van een online aangiftesysteem met een database. Hieruit kan met behulp van automatisering opsporingsindicatie worden gefilterd; een bankrekeningnummers en telefoonnummers.
Vervolgens heeft men een structuur gebouwd in de vorm van een samenwerking met banken waarin vorderingen op bankrekeningnummers in bulk kunnen plaatsvinden. In het project zijn grote hoeveelheden (tot 1100) rekeningnummers naar de bank verstuurd, waarna per rekening gedetailleerde informatie (zoals transacties, IP-login en de tenaamstelling) is teruggekregen. Dit gebeurde in grote bestanden en via een geautomatiseerde verbinding. De juridische basis hiervoor ligt in onderzoek naar georganiseerde structuren[29]. Het gaat dan over zwaardere feiten en een georganiseerd verband. Op basis van bankrekeningnummers en telefoonnummers kon men laten zien dat hier sprake van was omdat er soms tot wel 800 aangiftes waren waar enig verband tussen was. Met behulp van de grote hoeveelheden informatie vanuit banken heeft men 'kant-en-klare pakketjes'[30] kunnen verspreiden richting basisteams door heel het land.

Uiteindelijk heeft het OM geconcludeerd dat er niet voldoende bij de hogere lagen in de organisatie gekomen kan worden, omdat men vooral geldezels wist op te sporen. Daarom mogen er op deze basis geen vorderingen worden gedaan met deze grote hoeveelheid data en ligt het project op dit moment stil. Men is op zoek naar een nieuwe manier van werken om toch de gegevens binnen te krijgen. Eventueel toch met losse vorderingen, maar deze dan automatisch naar de bank versturen. Ook heeft men via telecomproviders gegevens willen opvragen in bulk hoeveelheden, maar omdat het volgen van een telefoon werd beschouwd als een zwaar middel om op te sporen konden slechts bulken van 100 telefoons worden verzameld.

Doel

Het project VIN-fraude heeft verschillende doelen. Een eerste doel is om de VIN-fraude strafrechtelijk aan te pakken. Ten tweede wil men met het project meer inzicht krijgen in het fenomeen en dit beter begrijpen. Een derde doel is het opwerpen van slimme barrières aan de voorkant waarmee VIN-fraude kan worden voorkomen. Ten slotte wil men structuren (zoals een geautomatiseerde samenwerking met banken) bouwen die herbruikbaar zijn. De doelen zijn niet schriftelijk vastgelegd, maar wel in e-mails heen en weer besproken.

29 Titel V uit het Wetboek van Strafvordering betreft 'bijzondere bevoegdheden tot opsporing voor het onderzoek naar het beramen of plegen van ernstige misdrijven in georganiseerd verband'.

30 Dit zijn zaken met bankrekeningnummers en tenaamstellingen van de geldezels die vanuit de eenheid worden verstuurd naar basisteams in het hele land.

Doelgroep

De doelgroep van het project bestaat enerzijds uit de politiemensen in de basisteams die de relatief eenvoudige VIN-fraude zaken zouden moeten oppakken. Ook wilde men graag dat de districtsrecherche zou aanhaken voor grotere onderzoeken. Anderzijds is een doelgroep de daders achter deze vorm van fraude, zoals de geldezels en ronselaars.

Niveau

Het project vindt op verschillende niveaus plaats. Lokaal gaan basisteams aan de slag met de aangeleverde zaken, op regionaal niveau is de eenheid initiatiefnemer van het project en op landelijk niveau worden de zaken verspreid onder de basisteams.

Onderbouwing

Verwachte werking

Er zijn verschillende verwachtingen waarom het project bijdraagt aan de eerder besproken doelen. Allereerst haalt men door het project informatie en gegevens binnen over VIN-fraude, waardoor er verbanden kunnen worden gezien en slim geselecteerd kan worden op de zaken die men aan wilt pakken. Zo blijkt uit de informatie bijvoorbeeld dat er een provinciestad is waar een ophoping van geldezels zit en dat er een bepaalde pinautomaat in het land is waar fraudeurs al 700.000 euro uit hebben gehaald.

Daarnaast verwacht men dat het project leidt tot een efficiëntere manier van werken. Enerzijds omdat er minder vorderingen gedaan hoeven te worden omdat dubbele vorderingen eruit worden gehaald. Dit kan het geval zijn als iemand uit stad X slachtoffers maakt op meerdere plekken en er vervolgens vorderingen worden gedaan door alle basisteams op hetzelfde telefoonnummer. Anderzijds worden vorderingen geautomatiseerd uitgevoerd, waardoor er een grote database ontstaat waar gegevens uit kunnen worden gehaald. Er zijn niet direct wetenschappelijke of praktijkgerichte theorieën die men gebruikt voor het project, wel wordt het fenomeen binnen de politie ontleed door crime-scripts van het delict te analyseren.

Bijhouden werking

Een deel van de resultaten van het project kan men kwalitatief beschrijven. Zo is bijvoorbeeld aan het licht gekomen dat er een landelijke aanpak mist, omdat het mechanisme van online fraude (grenzeloos) niet overeenkomt met het mechanisme van de nationale politie (de nationale politie is regionaal georiënteerd). Daarnaast probeert men bij te houden in hoeverre de geldezelpakketten die worden uitgezet daadwerkelijk worden opgepakt door de basisteams. Er is geprobeerd om in het BVH-systeem[31] van de politie een code aan de pakketjes te laten hangen of verdachten te identificeren, maar dit zijn geen sluitende mechanismen. Er wordt gezien dat sommige eenheden de pakketjes voortvarend oppakken en ook cijfermatig zaken terugkoppelen (de helft is opgepakt bijvoorbeeld).

Doelen behaald?

Op dit moment worden de doelen volgens de respondent deels behaald. De kennisdoestelling is aardig behaald omdat men nu

31 Basisvoorziening Handhaving (BVH) is het incidentregistratiesysteem van de Nederlandse politie. In het systeem kunnen politiemedewerkers incidenten registreren, aangiften opnemen en strafdossiers opstellen.

veel weet over VIN-fraude. De doelstelling van structuren hergebruiken is ook behaald, er is namelijk ervaring opgedaan met automatisering en bulken. Het strafrechtelijke doel wordt op dit moment maar deels gehaald, vanwege juridische- en capaciteitsbeperkingen binnen het OM en de politie. Capaciteitsbeperkingen zijn er omdat niet iedereen staat te trappelen om online fraude zaken op te pakken vanwege de lastige bewijsbaarheid. Daarnaast wordt op strafrechtelijk gebied vooral op het niveau van geldezels resultaat geboekt. Dit leidt tot juridische beperkingen om grotere hoeveelheden data te verkrijgen en analyseren, omdat een titel 5 onderzoek moet leiden tot inzichten in de criminele organisatie.

Samenwerking

Op het hoogtepunt waren er 8 personen fulltime vanuit de politie betrokken bij technische en juridische zaken: het schrijven van vorderingen, het verzamelen van data en het genereren van een 'front-end'. Daarnaast zijn er ook ongeveer 8 mensen meer zijdelings betrokken bij het project. Er wordt samengewerkt met interne en externe partners:

- Intern (binnen de politie): regionale cybercrimeteam, districten en basisteams
- Extern (buiten de politie): Openbaar Ministerie, banken, (telecomproviders)

Het regionale cybercrimeteam heeft twee mensen verantwoordelijk gemaakt om het project uit te rollen naar de districten en de districten hebben ook een coördinator. De recherches van de basisteams gaan vervolgens met de zaken aan de slag. Met het Openbaar Ministerie is veel afstemming geweest (ook op juridisch vlak) en zij leiden de onderzoeken. Vanuit de banken zijn vaak een of twee ontwikkelaars betrokken voor het opzetten van de geautomatiseerde systemen. De samenwerking met telecomproviders is eigenlijk nooit op gang gekomen.

Afspraken

Er zijn enkele ad-hoc afspraken gemaakt rondom het project. Met cybercrimeteams is bijvoorbeeld afgesproken dat zij ervoor zorgen dat geldezel-pakketten opgepakt worden, de voortgang daarvan monitoren en een status overzicht kunnen geven.
In de praktijk is dit lastig gebleken. Met banken zijn afspraken dat de gegevens die worden gevraagd worden geleverd via een bulk constructie en beveiligde verbindingen. Zij moeten dit aanleveren omdat het een wettelijk rechtmatige vordering is. De afspraken gaan vooral over de praktische inrichting van deze uitwisseling van informatie. Een van de banken wilde niet een ad-hoc manier van werken, waardoor met deze bank de samenwerking meer is geformaliseerd.

Er is geen duur aan de samenwerking gekoppeld. Men heeft de hoop en veronderstelling dat het beide partijen gaat helpen om minder mensen in te hoeven zetten op dergelijke vorderingen en daarom een duurzame samenwerking wordt.

Kwaliteit samenwerking

De samenwerking wordt met de meeste partners als goed omschreven. Binnen de politie snappen de verschillende organisatieonderdelen het probleem en is men meer dan bereid om daar een centrale rol in te spelen. De meeste banken zijn ook bereid tot samenwerking, al is men daar wel voorzicht met het verstrekken van gegevens omdat men bezorgd is om de privacy van klanten. Uiteindelijk is de samenwerking goed verlopen en heeft men ook veel gegevens gekregen. Met telecomproviders is geen direct contact geweest op operationeel niveau, omdat dit via een andere afdeling binnen de politie wordt uitgevraag middels juridische toestemming. Omdat het moeizaam gaat als iets juridisch niet lukt ervaart men dat als een minder prettige samenwerking. Vanuit het OM is de cyber officier van justitie gedreven om met het onderwerp aan de slag te gaan.

Verbeterpunten samenwerking

Organisaties zouden zich nog bewuster kunnen zijn van de veranderingen op het gebied van online criminaliteit. Vooral dat het opsporen van online fraude op eenheidsniveau lastig is, omdat het eenheid overstijgend is. Ook capaciteit is een probleem geweest tijdens het project, wat tot onbegrip leidt gezien de omvang van het probleem. Zo komt het bijvoorbeeld voor dat bij een winkeldiefstal van geringe aard een heel team wordt ingezet en bij online oplichting voor grote bedragen zaken niet opgepakt worden, vanwege onvoldoende opsporingsindicatie.

Implementatie praktijk

Het project is een sprong in het diepe geweest waarbij men is begonnen zonder te weten waar het eindigt. Het is deels geworden wat de respondent gedacht had, behalve dat men moest stoppen vanwege de juridische beperkingen. Er waren nog verschillende slimme ideeën om met de data verder te gaan, zoals het verzamelen van telefoons van geldezels en deze uitlezen om daarin verbanden te onderzoeken.

Project tussendoor geëvalueerd en aangepast?

De manier van werken waarin één cyberteam dergelijke zaken oppakt, is voorbij. Men moet nu op zoek naar een inbedding in de nationale politie die structureel van aard is. LMIO[32] is bijvoorbeeld om dezelfde reden opgericht, omdat niet te duiden was waar het thuis hoort.

Wat goed gaan in het project is dat de kwaliteit van de aangiften hoger is doordat aangevers gestructureerd stappen moeten doorlopen. Ook is er meer zicht op VIN-fraude en is het voor teams die kleine zaken moeten draaien overzichtelijk geworden door de kant en klare pakketjes met geldezels. Minder goed gaat het feit dat er niet vanuit alle basisteams opvolging en/

32 Het Landelijk Meldpunt Internetoplichting is een publiek-private samenwerking tussen de politie en andere organisaties (zoals het OM, banken en de Betaalvereniging) met als doel om online handelsfraude te bestrijden.

of terugkoppeling plaatsvindt en dat men tegen juridische beperkingen aanloopt om door te gaan met het verzamelen en analyseren van de grote hoeveelheid data.

Implementatie schaal & intensiteit
De respondent geeft aan dat het op landelijke schaal geïmplementeerd moet worden om eerder genoemde redenen. Doordat het kleinschalig is geweest heeft men wel veel dingen door kunnen zetten en niet alles hoeven formaliseren. Met de geografische oriëntatie van eenheden is niet alles op te lossen (kan niet op eenheidsniveau). Bv. Van 1300 gevallen in Oost-Nederland moeten er 800 naar een andere eenheid gestuurd worden, waardoor werkvoorbereiding op eenheidsniveau een stuk minder effectief en efficiënt is.

De bezetting van 8 full time mensen op het hoogtepunt is naar mening van de respondent veel te weinig. Met meer mensen had een betere structuur op gezet kunnen worden waarmee mensen 'dedicated' op sub-taken gezet konden worden.

Toepasbaarheid andere eenheden
Het project heeft op landelijk niveau vorm heeft gekregen (ondanks dat de werkwijze nog niet structureel is vormgegeven), waardoor andere eenheden niets hoeven te doen behalve het verspreiden van de kant en klare pakketjes. Bij deze vorm van online criminaliteit is het van belang om zaken centraal te organiseren vanuit een punt. Verder benadrukt de respondent dat het onderliggende probleem - dat er geen juiste organisatiestructuur is om dergelijke zaken op te pakken – belangrijk is. Er zou een landelijke werkvoorbereidingsclub moeten komen die alle vormen van online fraude binnenkrijgt en geautomatiseerd en slim kan achterhalen waar de zaak thuishoort.

4.4.2 Digitaal District

Eenheid Midden-Nederland

Introductie

Het Digitaal District wordt omschreven als de motor van de aanpak van cybercrime en gedigitaliseerde criminaliteit binnen de eenheid Midden-Nederland. In het Digitaal District is het regionale cybercrimeteam ondergebracht, wordt een team opgericht voor de aanpak van gedigitaliseerde criminaliteit en worden initiatieven genomen om districten en basisteams aan te jagen rondom het thema. De respondent is werkzaam als projectleider/teamleider van het regionale cybercrimeteam in de eenheid Midden-Nederland.

Aanleiding

De belangrijkste aanleiding voor de oprichting van het Digitaal District is een van de opdrachten die de respondent had als projectleider, namelijk om districten en basisteams meer 'cyber aware' te maken, het kennisniveau van cybercrime op te krikken en ervoor zorgen dat zij meer cybercrime onderzoeken gaan draaien. In de afgelopen jaren is deze opdracht lastig gebleken om een aantal redenen. Ten eerste is er al geruime tijd sprake van onderbezetting binnen de eenheid. Basisteams hebben moeite om roosters te vullen, waardoor geen tijd is voor een nieuw onderwerp zoals cybercrime. Daarnaast werd gemerkt dat wanneer er wel capaciteit beschikbaar was, de politiemedewerkers niet goed weten welk handelingsperspectief zij hebben. Een derde reden waarom er geen beweging zat op het gebied van cybercrime is omdat de impact van de delicten op het publiek wordt onderschat. Hierdoor gingen tijdens de case-screening, in de weging, fysieke delicten altijd voor digitale delicten. Ten slotte zijn basisteams geografisch gebonden (in de vorm van gebiedsgebonden politiezorg), terwijl cybercriminaliteit niet locatie gebonden is. Bij een zaak blijkt vaak dat ook in andere eenheden slachtoffers worden gemaakt, waardoor lokale teams zich minder verantwoordelijk voelen om de zaak op te pakken. Er was dus een andere aanpak nodig om meer beweging te krijgen rondom het thema binnen de districten en basisteams. Enerzijds was er capaciteit nodig (door het regionale cybercrimeteam verder op te tuigen en dit team onder te brengen in de organisatiestructuur) en anderzijds was er een motor nodig (een kenniscentrum) om de aanpak van cybercriminaliteit en digitale componenten in reguliere onderzoeken te bevorderen. Vanuit dit idee is het Digitaal District opgericht.

Beschrijving project

Inhoud
Het digitaal district bestaat uit het regionale cybercrimeteam en een aantal projectleden ter ondersteuning op het gebied van communicatie, opleidingen en bestuurlijke kwesties. Verder is een sectorhoofd verantwoordelijk voor het digitaal district. Enerzijds is het digitaal district een operationeel centrum waar onderzoeken gedraaid worden en anderzijds zit er een projectgroep om de beweging in de districten en basisteams aan te jagen. Hiervoor worden kennissessies georganiseerd, zijn inloop spreekuren gepland waar mensen met hun casus terecht kunnen en wordt een opleidingsaanbod gecreëerd rondom het thema. Ook worden een aantal recherchekundigen van de DRR (dienst regionale recherche),

bijvoorbeeld voor een tijdelijke aanstelling van twee jaar, geplaatst in het Digitaal District, zodat zij digitale kennis meenemen in de reguliere opsporing voordat zij terug worden geplaatst in de DRR.

Het Digitaal District wordt verder omschreven als een omgeving waar nieuwe initiatieven kunnen worden ontwikkeld. Zo wordt er op dit moment ook een aanpak voor gedigitaliseerde criminaliteit opgezet vanuit het Digitaal District. Een ander voorbeeld van een initiatief is en spreektafel met een van de districten. Vroeger werden aangiften gescreend bij het regionale cybercrimeteam en digitaal overgedragen naar een district of basisteam met een advies over te nemen acties. Omdat dit niet goed werkte, kijkt men nu periodiek en gezamenlijk naar kansrijke zaken om te bespreken hoe de zaken aangepakt kunnen worden en hoe werkzaamheden eventueel verdeeld kunnen worden tussen het Digitaal District en de districtsrecherche of basisteamrecherches.

Het verschil tussen het Digitaal District en regionale cybercrimeteams in andere eenheden zit vooral in de manier van werken. Zo is er een agile organisatiestructuur[33] opgezet en zijn er drie scrumteams[34] die zelfstandig onderzoeken en projecten draaien. Daarnaast heeft het Digitaal District een aanjaagfunctie om verandering te bewerkstelligen binnen de districten en basisteams rondom de aanpak van cybercrime en gedigitaliseerde criminaliteit. Formeel is het Digitaal District op 1 maart 2021 van start gegaan. Voor deze datum waren al enkele onderdelen geïmplementeerd.

Doel

Het doel van het digitaal district is om vernieuwing op het gebied van gedigitaliseerde criminaliteit en cybercrime aan te jagen. Enerzijds door zelf opsporingsonderzoeken uit te voeren en anderzijds door middels verschillende projecten andere onderdelen in de organisatie aan te sporen.

Doelgroep

De doelgroep van het digitaal district is de hele eenheid met alle verschillende lagen en functies. Zo zijn de ambassadeurs van de districten en basisteams een belangrijke doelgroep om het netwerk te creëren, worden medewerkers van intake en service betrokken om het aangifteproces te verbeteren en is ook het digitaal platform een belangrijke doelgroep.

Onderbouwing

Verwachte werking

Er wordt verwacht dat het digitaal district ervoor zorgt dat het onderwerp meer aandacht krijgt en dat er meer mensen mee aan de slag gaan. Met behulp van het digitaal district gaan mensen zich realiseren dat cyber steeds meer onderdeel is van de reguliere criminaliteit en dus onderdeel is van de aanpak. Er liggen geen wetenschappelijke theorieën ten grondslag aan het digitaal district. Wel zijn er een aantal pijlers landelijk binnen de politieorganisatie opgesteld op het gebied van cybercrime, zoals het investeren in verbeteren van het opnemen van aangiften en het verbeteren van de kennis en kunde van medewerkers. Deze pijlers zijn ook meegenomen in de pijlers van de aanpak van het digitaal district.

Bijhouden werking

Om bij te houden of de doelen van het digitaal district worden behaald is een consultancy bureau ingezet. Dit bureau heeft een nulmeting uitgevoerd en gaat binnenkort een vervolgmeting uitvoeren. Er zijn enkele doelen benoemd die worden gemeten. Zo zijn er harde criteria zoals aantallen zaken, maar ook zachtere criteria zoals preventie en verstoring. Hiervoor worden kwantitatieve cijfers geraadpleegd en kwalitatieve gesprekken gevoerd met politiemedewerkers.

Samenwerking

Het digitaal district bestaat uit ongeveer 50 medewerkers in de vorm van het voormalige regionale cybercrimeteam en een projectteam. Het projectteam bestaat uit een communicatiemedewerker, een opleidingscoördinator, een beleidsadviseur, iemand van een extern consultancy bureau en de respondent zelf. Het externe consultancy bureau is betrokken bij de vormgeving van het digitaal district en de eerder besproken evaluatie. Ten slotte wordt er ook samengewerkt met medewerkers uit de basisteams en districten. De samenwerking bestaat uit een aantal vaste momenten zoals de periodieke netwerkdagen, digitale donderdagen (spreekuren) en andere reguliere bijeenkomsten. Bij de digitale netwerkbijeenkomsten zijn ongeveer 150 mensen aanwezig.

Afspraken

Er liggen formele afspraken ten grondslag aan het Digitaal District die zijn vastgelegd in een projectplan. Dit projectplan is goedgekeurd door de eenheidsleiding. Het project ‘Digitaal District’ is voor een duur van 2 jaar vastgelegd, maar er wordt verwacht dat het district langer doorgaat.

Kwaliteit samenwerking

De respondent merkt dat het project positief ontvangen wordt, omdat mensen zich realiseren dat het een onderwerp is waar men wat mee moet. Ook wordt de aangeboden hulp gewaardeerd.

Implementatie praktijk

Het project is volgens de respondent volgens plan uitgevoerd op het moment van schrijven. Verder zijn er periodieke metingen om te kijken of het nog verloopt zoals gewenst. Op basis hiervan kunnen zaken eventueel aan worden gepast. Er zijn nog geen concrete voorbeelden van aanpassingen.

Wat op dit moment goed gaat binnen het project is dat er een plek is gecreëerd waarbij meer mogelijkheden zijn om initiatieven te starten op het thema cybercrime en digitalisering. De structurele onderbezetting binnen de eenheid zorgt voor een minder goed verloop van het project. Dit zorgt ervoor dat het lastig blijft om een nieuw thema te adresseren, omdat het werk al als lastig genoeg wordt ervaren. Dit wordt door alle lagen in de eenheid gemerkt. Zo is bijvoorbeeld de opsporing overbelast waardoor in de schaarste gezocht wordt naar redenen om geen cybercriminaliteit op te hoeven pakken.

33 Een agile organisatie bestaat uit teams in plaats van afdelingen die multidisciplinair, snel en zelfstandig kunnen werken en experimenteren.

34 Een scrumteam werkt op een flexibele manier toe naar bepaalde doelen, in korte sprints met een lengte van een aantal weken.

Implementatie schaal & intensiteit
De schaal waarop het project is geïmplementeerd wordt als goed ervaren. De respondent geeft aan dat het vooral de vraag is of er met de harde of zachte hand veranderingen op het thema worden gecreëerd. In dit initiatief is gekozen voor de zachte hand, door mensen te enthousiasmeren en te stimuleren. Een andere manier – met de 'harde hand' – zou zijn om een bepaald aantal FTE te labelen bij de basisteams en doelstellingen mee te geven rondom het thema. Binnen de eenheid is echter gekozen om op basis van intrinsieke motivatie verandering aan te brengen in plaats van afdwingen omdat dit passender is binnen de eenheid (o.a. schaarste zorgt ervoor dat er niet zomaar Fte's vrijgemaakt kunnen worden).

Of het digitaal district met de juiste intensiteit is geïmplementeerd is volgens de respondent moeilijk te zeggen omdat er nog weinig ervaringen zijn. Vooralsnog wordt wel gedacht dat de intensiteit goed is.

Toepasbaarheid andere eenheden
Het concept wordt gezien als goed toepasbaar binnen andere eenheden. Het is vooral belangrijk om een eenheidsleiding te hebben die het project ziet zitten. Verder zijn in andere eenheden al soortgelijke bewegingen ontstaan, bijvoorbeeld in de vorm van een Cyber HQ in Zeeland-West-Brabant.

4.4.3 Cyberspecials

Eenheid Amsterdam

Introductie

In dit project worden gespecialiseerde politie cybervrijwilligers - die in Amsterdam Cyber Specials worden genoemd – ingezet om ondersteuning te bieden binnen de eenheid op het thema cybercrime. Langzaam beginnen ook andere eenheden met het concept cybervrijwilliger. Er zijn inmiddels ongeveer 30 Cyber Specials in de eenheid Amsterdam. De respondent is aanjager voor de aanpak cybercrime (zowel cybercrime als gedigitaliseerde criminaliteit) en vanuit deze rol richt hij zich op de inzet van cybervrijwilligers.

Aanleiding

Een eerste aanleiding is dat er twee opdrachten waren vanuit beleidsvoering: 1. vanuit de landelijke cybercrime strategie (2016) uitvoering geven aan de 6 pijlers (verbeteren intake & service, versterken informatiepositie etc.) en 2. het concept cybervrijwilligers was ook in de strategie opgenomen omdat de politie meer gebruik moest maken van kennis van buiten de organisatie op dit gebied. Het concept politievrijwilligers bestaat al langer, maar vrijwilligers op specialismen zoals cybercrime waren nieuw.

De respondent had vervolgens de taak om werk te maken van publiek private samenwerking en de inzet van vrijwilligers. Respondent kwam in contact met Team Coördinatie Politievrijwilligers (TCP) en zij zijn samen het project verder vorm gaan gegeven. April 2019 is een oproep verspreid voor mensen met een achtergrond in IT die de politie wilden helpen als vrijwilliger in de aanpak van cybercrime. Vervolgens is er een informatieve avond georganiseerd voor 40 mensen, waarvan uiteindelijk 20 mensen hun gegevens hebben achtergelaten omdat ze geïnteresseerd waren. Wie het project oorspronkelijk heeft opgezet heeft weet de respondent niet precies. Wel is bekend dat een soortgelijk project al bestond in Engeland, waar cyber-specials zijn ingezet binnen de politie.

Beschrijving project

Inhoud
Het project bestaat uit het aanspreken en aanstellen van mensen buiten de politie organisatie als vrijwilliger. Vrijwilligers dienen te beschikken over een IT-achtergrond of affiniteit te hebben met cyber en de politie verder willen helpen. De achtergrond van de cybervrijwilligers is erg divers. Voorbeelden zijn een grafisch ontwerper, blockchain expert, ethical hacker, criminoloog, OSINT expert, cybersecurity consultant en jurist.

Het betreft een formele aanstelling in de vorm van een besluit waar mensen voor worden gescreend. De inzet van cybervrijwilligers varieert van minimaal 2 uur per week tot ongeveer 12 uur per week. Daarnaast bestaat het project uit het plaatsen van de cybervrijwilligers binnen de politie op zogenoemde landingsplaatsen binnen de politie organisatie. Hiervoor worden gesprekken georganiseerd tussen een kandidaat en een inlener (bijvoorbeeld een teamleider van het cybercrimeteam, een internetrechercheur van een district of een operationeel expert van een basisteam). Cybervrijwilligers hebben een landingsplaats, maar worden ook ingezet

voor projecten of ad-hoc klussen. Er wordt niet specifiek geworven, mensen melden zichzelf aan. Er is veel animo vanuit vrijwilligers om te helpen, de uitdaging is om het aanbod aan te kunnen en de mensen operationeel te maken.

De cybervrijwilligers hebben een brede rol en worden op alle paden van de cybercrime strategie ingezet, zoals het vergroten van kennis en kunde (les geven, doceren) en het vergroten van bewustwording. Tijdens het plaatsen houdt men de cybercrime strategie in het achterhoofd (ondersteunen aangifteproces, versterken informatiepositie).

In de eenheid Amsterdam worden de cybervrijwilligers 'cyberspecials' genoemd, in navolging van de benaming die in Engeland aan de vrijwilligers werd gegeven. Een reden hiervoor is dat het woord vrijwilliger binnen de politie veel foutieve beeldvorming opriep: de suggestie werd gewekt dat de vrijwilligers niet voldoende gekwalificeerd zouden zijn voor het onderwerp. De associaties die 'vrijwilliger' oproept werkte averechts voor de functie en dus is gezocht naar een betere benaming.

Doel
Het doel van het project is om door de inzet van cybervrijwilligers snellere voortuitgang te boeken in het versterken van de aanpak cybercrime en gedigitaliseerde criminaliteit. De doelen zijn opgenomen in de landelijke cybercrime strategie. Dit is een overkoepelend beleidsdoel waar men in Amsterdam invulling aan heeft gegeven. De cybervrijwilligers kunnen rondom alle vormen van cybercrime en gedigitaliseerde criminaliteit worden ingezet. Ze worden niet specifiek voor bepaalde delicten geworven of ingezet.

Niveau
Het is inmiddels een landelijk project, in de zin dat er binnen de politie een landelijke ambitie is om het op te zetten. Op verschillende plekken op verschillen momenten heeft het project vorm gekregen. Niet in elke eenheid groeit het even hard: in Amsterdam zijn er 30 cybervrijwilligers en in totaal zijn er landelijk 70 cybervrijwilligers. Niet iedere eenheid heeft iemand vrijgemaakt voor een aanjagersrol zoals de respondent die heeft. De respondent is in verschillende eenheden geweest om kennis te delen.

Onderbouwing

Verwachte werking
Er wordt ten eerste verwacht dat er veel kennis en kunde te halen is buiten de politie. Veel mensen zijn bereid om de politie te helpen, de politie moet zich er vervolgens voor open stellen en het inbedden om er op een goede manier gebruik van te maken. Daarnaast verwacht men dat de doelen worden behaald omdat de ervaringen van beroepscollega's vrijwel altijd positief zijn, ondanks dat er ook wel eens een cyberspecial is afgevallen. Verder zijn er steeds meer teams die aankloppen omdat ze een cybervrijwilliger willen aanstellen. Ten slotte wordt er door de respondent aangegeven dat wetenschappelijke onderzoeken laten zien dat het met de kennis en kunde binnen de politie op het gebied van cybercrime en digitalisering nog matig is gesteld.

De grootste uitdaging van het project is volgens de respondent het culturele aspect. Onderzoeken hebben laten zien dat de samenwerking tussen beroepskrachten enerzijds en vrijwillige specialisten anderzijds een uitdaging is en sociale lenigheid vereist van zowel de beroepskrachten als cybervrijwilliger. Het is een belangrijke uitdaging volgens de respondent om te kijken hoe de beroepsorganisatie zich verhoudt tot de groep specialisten, die minder uren aanwezig zijn en flexibel inzetbaar zijn.

Bijhouden werking
Er wordt op dit moment volgens de respondent door TNO onderzoek uitgevoerd uit naar de effectiviteit van de ondersteuning van intakemedewerkers door cybervrijwilligers. Daarnaast is volgens de respondent op dit onderwerp ook een kwalitatief onderzoek gericht op slachtoffers, intakemedewerkers en cyberspecials. Ook is er onderzoek gedaan waarbij cyberspecials en beroepskrachten geïnterviewd zijn om te kijken waar het goed gaat en waar het schuurt in de samenwerking. De respondent denkt dat er meer gebeurd maar heeft daar momenteel geen zicht op. Verder zou de respondent het interessant vinden om een goed onderzoek naar het rendement uit te voeren. Er zijn veel voorbeelden en reacties van collega's, maar dit betreft geen wetenschappelijk onderzoek.

Doelen behaald?
De respondent geeft aan dat het lastig is om te bepalen in welke mate de doelen zijn behaald. Er kan gekeken worden naar successen (intranet berichten waarbij zaken zijn opgelost met hulp van vrijwilligers), aantallen en tevredenheid onder politie medewerkers. Intern is er wel gewerkt met streef-aantallen, maar mensen worden niet aangenomen om hier perse aan te voldoen. De respondent heeft de indruk dat er draagvlak is binnen de organisatie. Verder zijn er evaluatiegesprekken achteraf vanuit TCP over wat goed ging en wat beter kan.

Of de cyberspecial een effectief instrument is om de kloof tussen externe expertise en de politie te dichten zou de toekomst uit moeten wijzen. In Engeland is het project volgens de respondent niet goed gelukt omdat er wrijving ontstond tussen beroepskrachten en specialisten. De beroepsorganisatie ging bepaalde besluiten nemen over de cyberspecials zonder hen daar bij te betrekken. Hier moet voor worden gewaakt: het zijn hoog opgeleide mensen die naar mening van de respondent zelf aan het roer moeten worden gezet op hun expertise.

Samenwerking

Er kunnen vijf belangrijke stakeholders worden aangemerkt binnen het project:
1. (Kandidaat) Cybervrijwilligers
2. Team Coördinatie Politievrijwilligers (TCP)
3. De inlener
4. De matchmaker, recruiter of coordinator
5. Landelijk programma

De rol van het TCP is het regelen van de aanstelling, het fungeren als aanspreekpunt en het regelen van de personele zorg. De inlener is afnemer van een cybervrijwilliger: het cybercrimeteam, Dienst Regionale Recherche (DRR), Districtsrecherche (DR), Basisteam (BT) of een project. De matchmaker, recruiter of coördinator onderzoekt hoe de kandidaat die door TCP wordt aangesteld verbonden kan worden met een inlener. Vanuit het landelijk programma is de opdracht gegeven om met cybervrijwilligers aan de slag te gaan.

Afspraken
Het is voor het project belangrijk om goede afspraken te maken, omdat het een soort uitzendconstructie is. Voordat een cyber-

vrijwilliger ergens begint is er een startgesprek en stelt TCP een document op met afspraken over bijvoorbeeld een aanspreekpunt, werkzaamheden en de inzet (werkuren). Ook met de inlener worden goede afspraken gemaakt en wordt geëvalueerd. Dit naar aanleiding van een mindere ervaring met een vrijwilliger, waarbij het voor de inlener niet duidelijk was waar men moest zijn om dit op te lossen. Men probeert duidelijker dan voorheen de afspraken in het begin vast te leggen op individueel niveau. Op een gegeven moment is een cybervrijwilliger klaar met een project, dan kan de inlener de cybervrijwilliger “teruggeven” aan TCP. Er is in principe geen duur vastgelegd, met de inlener is er vaak een openeind afspraak.

Kwaliteit samenwerking

Over het algemeen gaat de samenwerking met alle partijen erg goed volgens de respondent. Men moet het ook van de samenwerking hebben bij dit project. Het TCP is een cruciaal onderdeel om het te laten slagen. De samenwerking met de cybervrijwilligers verloopt op een enkele uitzondering na erg goed. Dit zou komen doordat de vrijwilligers het werk doen vanuit een intrinsieke motivatie en iedereen erg betrokken is. De samenwerking met de inleners is goed omdat er veel mooie initiatieven zijn ontstaan, maar soms ook spannend omdat niet alle potentiele inleners overtuigd kunnen worden om cybervrijwilligers aan te laten sluiten. Ook over de samenwerking met het landelijk programma is de respondent erg te spreken, omdat er veel mogelijkheden en ruimte was om het project te ontwikkelen en verder te brengen.

Verbeterpunten samenwerking

De samenwerking zou verbeterd kunnen worden door de vrijwilligers beter te betrekken bij de organisatie en ze beter voor te bereiden op de (cultuur binnen) de politie organisatie die vaak onbekend is voor de vrijwilligers. Ook kan de samenwerking worden verbeterd door meer verwachtingsmanagement richting de inlener over het feit dat de invulling van de functie (aantal uren, werkzaamheden etc.) per cybervrijwilliger kan verschillen. De combinatie tussen beperkt aanwezig zijn en wel een expert rol vervullen (soms ook op een hoge positie binnen de organisatie) kan weerstand opwekken onder collega’s binnen de politie organisatie.

Implementatie praktijk

Voor het grootste deel is het vormgegeven zoals beoogd, maar het project is nog niet klaar en er is nog veel werk te verzetten. Tussendoor wordt er geëvalueerd en aangepast op verschillende niveaus. Geëvalueerd wordt er landelijk door in verschillende kwartaalrapportages te rapporteren over het project cybervrijwilliger aan de programmadirecteur cybercrime en digitalisering. Daarnaast is er elke 2 weken een TCP - cyberspecial overleg waarbij de aanjager van het project met collega’s van TCP om de tafel zit en kijkt hoe het gaat. Eens in de paar maanden zitten de inlener, cyberspecial en TCP langer bij elkaar om de stand van zaken te bespreken. Daarnaast is er een tussentijdse evaluatie gewest waar veel leerpunten in zaten en loopt er momenteel onderzoek van TNO. De cyberspecials zelf stellen veel vragen en zijn kritisch, dat zijn continue evaluaties en leerpunten. Aanpassingen vinden continue plaats. Zo is er nu een startgesprek waarin afspraken vastgelegd worden, dat in het begin nog niet werd gedaan. Een andere belangrijke aanpassing is dat iemand nu pas wordt aangesteld op het moment dat er een mogelijke inlener is. Er is nu eerst een intake gesprek, vervolgens worden er lijntjes uitgegooid en is er een vervolggesprek met een mogelijke inlener.

Implementatie schaal & intensiteit

Binnen de eenheid Amsterdam vindt de respondent de schaal goed, omdat er een groot afzetgebied is voor de vrijwilligers. Een cybervrijwilliger kan namelijk aan zowel het cyberteam van DRR gekoppeld worden, maar ook op verschillende andere plekken. In andere eenheden werd in het begin vaak vooral de link met het cybercrimeteam gelegd (cyber in enge zin). Vanuit landelijk perspectief is het project volgens de respondent nog niet geïmplementeerd met de juiste schaal, omdat 80 procent van de vrijwilligers uit de eenheid Amsterdam komt.

De intensiteit is volgens de respondent goed. Op individueel niveau zou er nog meer uitgehaald kunnen worden. Sommige cybervrijwilligers zijn erg proactief en gaan snel, andere cybervrijwilligers is nog niet het volledige potentieel benut (omdat er toch nog niet een goede inlener voor is gevonden, of iets degelijks).

Toekomstplan

In de toekomst zou de respondent het project graag opschalen en beter organisatorisch inbedden. De respondent zou graag een landelijke poule cyberspecials creëren die goed verbonden is met de staande organisatie en ook de aandacht krijgt die het verdiend in de vorm van opleidingen, ontwikkelmogelijkheden etc. De grootste kunst is om het vraag en aanbod bij elkaar te brengen, daarom in de toekomst wellicht een online platform waar vragen vanuit de beroepskrachten kunnen worden gesteld aan cyberspecials, maar waar ook cyberspecials kunnen aangeven wat hun beschikbaarheid en expertise is.

Schaalbaarheid / toepasbaarheid andere eenheden

Verder opschalen is volgens de respondent goed mogelijk omdat elke eenheid een TCP heeft. Echter heeft niet elke eenheid een aanjager/matchmaker zoals de respondent. Op een gegeven moment is de matchmaker waarschijnlijk niet meer nodig indien het landelijk loopt en kan een inlener bijvoorbeeld online via een platform op zoek naar een vrijwilliger. Wanneer er veel cyberspecials zijn, wil men graag dat wanneer bijvoorbeeld in Groningen een ingewikkelde DDoS-aanval is, dat de specialist op dat gebied uiteindelijk daaraan gekoppeld kan worden.

Het project toepassen is in andere eenheden kan goed en hoeft niet exact op dezelfde manier georganiseerd te worden als in Amsterdam. Belangrijke succesfactoren zijn (1) het hebben van een ervaren en goed draaiend TCP en (2) voor de komende 4-5 jaar een vrijgemaakte coördinator om het binnen de eenheid of andere eenheden van de wal te krijgen. Verder verschillen eenheden in bijvoorbeeld geografie, dus moet het project aan sluiten bij de behoeften en bijzonderheden van de eenheid. In andere eenheden worden cybervrijwilligers wel al ingezet, maar in de eenheid Amsterdam loopt men voorop.

4.4.4 Cyberdriehoek

Eenheid Den Haag

Introductie

De cyberdriehoek bestaat uit structurele overleggen tussen de burgemeester van Katwijk (regionaal portefeuillehouder cybercrime), de politiechef van de eenheid Den Haag en de hoofdofficier van justitie van arrondissement Den Haag[35].De respondenten zijn werkzaam als accountmanager PPS (publiek private samenwerking) en teamleider van het regionale cybercrimeteam van de eenheid Den Haag. Vanuit het cybercrimeteam wordt input geleverd voor de cyberdriehoek.

Aanleiding

Er worden verschillende ontwikkelingen genoemd die mogelijk de aanleiding hebben gevormd voor de oprichting van een cyberdriehoek. Een daarvan betreft de verschillende cyber-incidenten die in gemeenten hebben plaatsgevonden. Hiermee samen hangt de afname van traditionele criminaliteit en toename van digitale criminaliteit. Verder is de politie informatie gaan aanleveren aan externe partners (zoals overheidsorganisaties en commerciele bedrijven) over digitale criminaliteit en is aangegeven dat dit een probleem is dat gezamenlijk opgelost dient te worden. Ten slotte veronderstelt men dat het onderzoek 'Burgemeesters in cyberspace'[36] over de taken en rollen met betrekking tot online openbare orde en veiligheid een aanleiding is geweest voor de cyberdriehoek. Redenen waarom het initiatief specifiek in Den Haag tot stand is gekomen zijn enerzijds dat men binnen de politie zich naast opsporing ook intensief bezighoudt met preventie en verstoren van criminaliteit en anderzijds omdat men vanuit Den Haag korte lijntjes heeft met het bestuurlijke en landelijke.

Beschrijving project

Inhoud

De samenwerking in dit project vindt plaats op het gebied van digitale veiligheid en criminaliteit, wat wordt onderverdeeld in cybercrime en gedigitaliseerde criminaliteit. Het is een overleg dat geen gezag heeft, maar wel kan stimuleren dat bepaalde zaken worden geagendeerd en dat er bewustwording wordt gecreëerd op het thema. De agenda wordt bepaald aan de hand van actiepunten uit het vorige overleg en door input vanuit beleidsondersteuners. Voorbeelden van agendapunten die eerder zijn besproken zijn: 'landelijke ontwikkelingen', 'smart cities' en 'informatievoorziening van de Vereniging van Nederlandse Gemeenten (VNG) over de informatie samenleving'. Vanuit het cybercrimeteam wordt input geleverd voor de cyberdriehoek en meegedacht over beleidsvorming.

35 Meer informatie over de eerste cyberdriehoek is te vinden op de website van het OM: https://www.om.nl/actueel/nieuws/2020/03/13/eerste-cyberdriehoek-van-nederland-komt-bij-elkaar

36 Bentema et al. (2018)

De cyberdriehoek staat los van de reguliere driehoek[37]. Burgemeesters die portefeuillehouder cybercrime zijn hebben daarnaast een rol in een landelijk overleg waar 25 burgemeesters vanuit het land overleggen over het thema cyber. Op dit moment hebben er twee cyberdriehoek overleggen plaatsgevonden en is een derde overleg gepland. Het eerste overleg was in maart 2020 en het derde gesprek staat gepland voor september 2021.

Doel

Het doel van de cyberdriehoek is om het lokale bestuur meer te betrekken bij de aanpak van cyber en daarbij zowel binnen als buiten de betrokken organisaties bewustwording te laten plaatsvinden.

Niveau

De cyberdriehoek vindt plaats op regionaal niveau, maar wel op het hoogste ambtelijke niveau waardoor er ook landelijk een link wordt gelegd.

Onderbouwing

Verwachte werking

Men verwacht dat de cyberdriehoek bijdraagt aan meer bewustwording omdat er vanuit twee kanten zaken in gang worden gezet. Enerzijds heeft het lokale invloed op de cyberdriehoek, doordat men vanuit lokaal of regionaal perspectief input kan leveren voor de cyberdriehoek. Anderzijds heeft de cyberdriehoek invloed op het landelijke niveau omdat de burgemeesters met cyber in hun portefeuille vervolgens zaken met elkaar bespreken in een landelijk overkoepelend overleg. Verder verwacht men dat het initiatief werkt omdat er steeds 'best' en 'worst practices' worden gedeeld met elkaar. Er is geen wetenschappelijk of basisdocument op basis waarvan de cyberdriehoek is ontstaan. Wel kijkt men naar publicaties van bijvoorbeeld Politie en Wetenschap over slachtofferschap van online criminaliteit om te zien wat er uit deze onderzoeken gehaald kan worden.

Bijhouden werking

Tijdens de cyberdriehoek maakt men afspraken die op lokaal niveau terug komen. Aan de hand van een actielijst wordt bijgehouden welke activiteiten er vanuit de cyberdriehoek overleggen plaatsvinden. Een van de punten is bijvoorbeeld het 'agenderen op een thematisch regionaal bestuur overleg'. De respondenten leveren hier dan bijvoorbeeld een bijdrage aan door een presentatie te geven aan een bepaalde doelgroep (zoals bijvoorbeeld uitvoerende ambtenaren of het college van burgemeester en wethouders).

Doelen behaald?

Men vindt het lastig te zeggen of de doelen worden behaald. Dat het onderwerp steeds meer op de agenda komt van het bestuur is voor de betrokkenen al een grote winst. Het is meer een bewustwording, waarbij niet perse SMART-doelen zijn geformuleerd.

37 De reguliere driehoek betreft het reguliere overleg tussen de burgemeester, officier van justitie en politie waarin men op gemeentelijk of bovenlokaal niveau overlegt over de taakuitvoering van de politie en afspraken maakt over de inzet van de politie (Politie, 2021): https://thesaurus.politieacademie.nl/Thesaurus/Term/1507

Samenwerking

Er zijn verschillende organisaties en afdelingen betrokken bij de cyberdriehoek:

- Intern (binnen de politie): de eenheidschef Den Haag, adviseur van de eenheidschef, regionaal cybercrimeteam
- Extern (buiten de politie): Regionaal Samenwerkingsverband Integrale Veiligheid (RSIV), gemeente Katwijk (burgemeester, afdeling Openbare Orde en Veiligheid, afdeling economische zaken), Openbaar Ministerie (hoofdofficier van justitie)

Het cybercrimeteam levert input aan de adviseur van de eenheidschef van de politie. Daarnaast sluiten de andere genoemde samenwerkingspartners veelal aan tijdens de cyberdriehoek.

Afspraken

Afspraken zijn gemaakt over het aantal keer dat de cyberdriehoek zou plaatsvinden. In het begin zou er twee keer paar jaar een cyberdriehoek zijn. Het is onduidelijk of dit meer of minder gaat worden. Andere afspraken worden vastgelegd in de notulen van het overleg. In hoeverre en waar verder nog zaken beleidsmatig zijn vastgelegd is onbekend. Verder is er geen einddatum vastgelegd, al is het idee om de cyberdriehoek structureel te beleggen. De duur van de cyberdriehoek laat zich vooral sturen door de onderwerpen die op de agenda staan en in de maatschappij spelen.

Kwaliteit samenwerking

De kwaliteit van de samenwerking is voor de respondenten lastig te beoordelen omdat zij zelf niet bij de cyberdriehoek aan tafel zitten. Wel is men blij met de ontwikkeling van het initiatief en werkt men steeds intensiever samen met collega's binnen de politie van beleidsadvisering en met collega's van het OM. Een mogelijke verklaring die wordt gegeven voor de steeds intensievere samenwerking is de grote hoeveelheid incidenten en maatschappelijke discussies.

Implementatie praktijk

De respondenten hebben geen invloed gehad op de vormgeving van de cyberdriehoek. Bij aanvang is wel met behulp van een 'position paper' bekeken hoe en wie er bij elkaar moesten zitten tijdens het overleg. De uitvoering komt overeen met deze 'position paper'.

Implementatie schaal & intensiteit

Ondanks dat de respondenten geen invloed hebben op de schaal en intensiteit, geeft men aan dat er wel vaker een cyberdriehoek plaats zou kunnen vinden gezien de ontwikkelingen op het gebied van digitale veiligheid.

Toepasbaarheid andere eenheden

Op dit moment vindt de cyberdriehoek alleen plaats in de eenheid Den Haag. Om het initiatief binnen een andere eenheid te implementeren is alleen nodig dat er tijd wordt vrijgemaakt in de agenda's van betrokkenen.

4.4.5 Aanpak geldezels

Eenheid Rotterdam

Introductie

Het project 'aanpak geldezels' bestaat uit een werkwijze binnen de eenheid Rotterdam waarbij men enerzijds opsporingsonderzoeken is gaan uitvoeren naar geldezels en anderzijds deze zaken op een gepaste wijze af wil handelen. De respondent is werkzaam als operationeel specialist B, ook wel 'chef-opsporing van een districtsrecherche' genoemd. Vanuit deze functie heeft de respondent het digitale platform onder zich.[38]

Aanleiding

Er zijn verschillende aanleidingen te benoemen voor het ontstaan van de specifieke aanpak van geldezels binnen de eenheid Rotterdam. De aanleidingen hebben met elkaar te maken en lopen door elkaar heen. Ten eerste is gedigitaliseerde criminaliteit de afgelopen jaren toegenomen. Binnen de gedigitaliseerde criminaliteitszaken ziet men vaak een financieel oogmerk, waarbij geldezels als belangrijke schakel fungeren in het uit cashen van geld. Ten tweede is het onder andere door de grenzeloosheid van de delicten vaak lastig om te bepalen wie de zaak op dient te pakken. Gedigitaliseerde criminaliteit zou voor het grootste deel opgepakt kunnen en moeten worden door de districtsrecherches en basisteams[39].Ten derde is uit onderzoeken van het LMIO (landelijk meldpunt internetoplichting) gebleken dat veel van de geldezels zich bevinden in de eenheid Rotterdam. Een laatste reden is dat er vanuit beleidsstukken en leidinggevenden een roep is om meer prioriteit te geven aan gedigitaliseerde criminaliteit. Uiteindelijk is er iemand binnen de eenheid Rotterdam met de portefeuille 'gedigitaliseerde criminaliteit en afpakken' die besloten heeft om een persoon (in de vorm van de respondent) volledig vrij te maken om de aanpak van geldezels vorm te geven binnen de eenheid. In september 2020 is de kick-off van het project geweest. De volgende organisaties zijn betrokken bij de opzet van het project: politie (districten, toeleveranciers LMIO en cybercrimeteam Oost-Nederland), Openbaar Ministerie (OM), Reclassering Nederland, Gemeente Rotterdam en Humanitas.

Beschrijving project

Inhoud

Het project bestaat uit grofweg drie onderdelen: (1) het aanstellen van aanspreekpunten binnen districtsrecherches en basisteams, (2) het oppakken van geldezel-zaken (3) de afhandeling van geldezel zaken. Eerst is de respondent begonnen om in iedere VVC (veel voorkomende criminaliteit) en in een districtsrecherche iemand aanspreekpunt en zaak-verantwoordelijk te maken voor geldezel-zaken. Inmiddels heeft de respondent een groep ter beschikking bestaande uit 3 à 4 mensen per district (6 districten in totaal). Vervolgens is de

38 Elke districtsrecherche heeft een digitaal platform. Een digitaal platform bestaat uit mensen met meer dan gemiddelde digitale kennis en vaardigheden en dient als extra ondersteuning voor politiemensen tijdens hun werkzaamheden (Stol, 2018).

39 Medewerkers van het basisteam die veel voorkomende criminaliteit (VVC) zaken oppakken.

respondent geldezel zaken gaan verspreiden onder dit netwerk. De geldezel zaken zijn aangeleverd vanuit enerzijds het LMIO (dit betrof een lijst met 400 openstaande geldezel zaken) en anderzijds de eenheid Oost-Nederland (dit betrof ruim 700 'Vriend in Nood-fraude' zaken). De districten en basisteams zijn vervolgens onderzoeken gaan draaien en in een nauwe samenwerking met ketenpartners de afhandeling van deze zaken vorm gaan geven met een afdoening op maat. Deze ketenpartners zijn het OM, Reclassering Rotterdam, Homerun Humanitas[40] en Expertise Team Financiën[41] van de Gemeente Rotterdam. De kern van het project is geldezels aanpakken in gezamenlijke actiedagen. Tijdens deze acties wordt de geldezel eerst verhoord door de politie, vervolgens vindt er een gesprek plaats met de reclassering of het ETF[42] waaruit een advies komt voor de Officier van Justitie, die op zijn of haar beurt een afdoening op maat geeft waarvan gedacht wordt dat de geldezel er het meest baat bij heeft. Er worden nog steeds (taak)straffen opgelegd aan de geldezels, maar ook vaak schadevergoeding of voorwaarden dat geldezels zich verplicht aansluiten bij hulpverleningsinstanties om een traject te gaan volgen. Het project is dus niet alleen 'strafrechtelijke tik', maar vooral ook met ketenpartners kijken wat voor de specifieke persoon een afdoening op maat is.

Doel
Het project heeft verschillende doelen:

1. Het aantal open geldezel zaken naar beneden brengen. Hiermee samen hangt het afgeven van een signaal richting aangevers dat de politie wat met de aangiften doet.
2. Preventie van geldezelschap doordat mensen horen dat zij kunnen worden opgepakt. Media wordt daarom meegenomen in het project, zodat duidelijk wordt dat politie en justitie zich met de problematiek bezighouden.
3. Maatwerk toepassen, zodat verdachten iets wordt aangeboden om uit de situatie te komen.
4. Een eenduidige manier van werken creëren binnen de eenheid om geldezel zaken op te pakken.

Doelgroep
Er is geen specifieke doelgroep waar dit project zich op richt, het ging om de geldezel in zijn algemeenheid. Later bleek tijdens de onderzoeken dat er meerdere doelgroepen onderscheiden kunnen worden, zoals naïeve jongeren, kwetsbare jongeren en ouderen met een uitzichtloze situatie. Voor de kwetsbaren/LVB-jongeren is volgens de respondent een heel specifieke aanpak nodig, door bijvoorbeeld Humanitas erbij te betrekken.

Niveau
Het project vindt plaats op eenheidsniveau, waar uiteindelijk districten en basisteams verantwoordelijk worden gemaakt voor het oppakken van de geldezel zaken.

Onderbouwing

Verwachte werking
Het project werkt volgens de respondent doordat men 'gewoon dingen is gaan doen', waardoor veel dingen zijn bereikt die anders niet in beeld waren gekomen. Verder wordt verwacht dat de doelen worden bereikt omdat de cijfers (het aantal zaken op de lijsten) al enorm gezakt zijn. De LMIO lijst bevatte in september 2020 ongeveer 400 verdachten en ten tijde van het onderzoek nog ongeveer 100 en de VIN-fraude lijst bevatte 700 VIN-fraude zaken en nu ongeveer 550. Het gaat dus om een tijdsbestek van een klein jaar. Een nuance die wordt gemaakt is dat sommige van de geldezels van de lijst verdwijnen wanneer zij een jaar 'schoon' blijven, maar dit zijn er volgens de respondent geen tientallen.
Daarnaast ziet de respondent dat de ketenpartners erg enthousiast zijn over de aanpak. Zo is de cyber-officier erg blij dat er eindelijk aandacht en prioriteit wordt gegeven aan de geldezels. Wel geeft de respondent aan dat de huidige aanpak veel capaciteit kost en niet altijd kan worden volgehouden. Het grote winstpunt is dat er nu mensen op de basisteams en binnen het OM zijn die feeling en ervaring hebben gekregen met geldezel-zaken. Zaken krijgen dan meer prioriteit en worden sneller opgepakt.

Bijhouden werking
Binnenkort wordt een overzicht opgesteld voor de partners (zie hieronder) met het aantal afgehandelde zaken. Men wil echter graag verder kijken dan enkel de cijfers. Politiemedewerkers binnen districten moeten het gevoel hebben dat de zaken ertoe doen. Daarnaast geven medewerkers van het ETF bijvoorbeeld aan dat zij door dit project de mensen aangeleverd krijgen die zij zoeken (namelijk met financiële problemen).

Verdere onderbouwing
De respondent geeft aan dat alles wat gedaan wordt rondom het project vooral vanuit de praktijk is ontstaan en dat het mooi zou zijn als dit nader wordt bekeken. Wat de respondent verder onderbouwd zou willen zien, is of er een rode draad zit in het ronselen van geldezels. Hier zouden interventies en preventie strategieën op afgesteld kunnen worden.

Samenwerking

Voor het project wordt samengewerkt met verschillende interne en externe partners:
- Intern (binnen de politie): district recherches en basisteams
- Extern (buiten de politie): Reclassering Nederland, Humanitas, team ETF van de gemeente Rotterdam, OM

Met name met het OM wordt intensief samengewerkt. Het OM is veel betrokken in de voorbereiding om te bepalen wie worden aangepakt, om de actiedag voor te bereiden en op de actiedag zelf de zaken af te handelen. De samenwerking bestaat uit veel overleggen met het OM (veel via mail, soms via Teams). In aanloop naar de actiedagen is er meer contact dan normaal. Met de VVC's heeft men contact via mail en Teams.

40 Homerun is onderdeel van Humanitas DMH (een zorgorganisatie) en biedt trajectbegeleiding op maat aan jongvolwassenen met een licht verstandelijke beperking (LVB) die problemen hebben met verschillende onderdelen van het leven.

41 Een team binnen de gemeente Rotterdam dat schuldhulpverlening biedt aan jongeren.

42 Het Expertise Team Financiën (ETF) is een afdeling van de gemeente Rotterdam waar experts werken die inwoners helpen met financiële problemen.

Er zijn geen vaste momenten waarop men afspreekt, maar dit gebeurd wanneer het nodig is.

Afspraken
Met het OM en politie is een protocol ontwikkeld waarin is vastgelegd hoe men het project vorm geeft. Dit is informeel vastgelegd en afgekaderd. Er is geen formeel vastgelegde duur gekoppeld aan de samenwerking. Vanuit het OM was het eerst voor een half jaar, maar dat is inmiddels opgerekt. Vanuit de politie was het een paar maanden, maar dat is inmiddels een jaar. Dit komt enerzijds omdat er geldezel zaken bijkwamen (vanuit de VIN-fraude lijst) en anderzijds omdat er ook veel ontwikkelingen waren binnen de politie op het gebied van gedigitaliseerde criminaliteit. Met dezelfde ketenpartners ontstonden diverse werkgroepjes en overlegvormen, waarin ook de verdere ontwikkeling op het gebied van gedigitaliseerde criminaliteit wordt besproken.

Kwaliteit samenwerking
De samenwerking gaat volgens de respondent erg goed. Een verklaring voor de goede samenwerking is dat de respondent een klik heeft met de personen en omdat men het belang inziet en iedereen dezelfde doelstelling heeft.

Implementatie praktijk

Toen het project begon had men wel een idee hoe het vorm gegeven zou moeten: eerst een fundering binnen de eenheid creëren door middel van aanspreekpunten. De respondent had niet voorzien dat het over de tijd zou uitgroeien tot de aanpak die het is geworden. Er zijn aanpassingen gedaan omdat men tegen dingen aanliep of zag dat ergens behoefte aan is. Zo zijn bijvoorbeeld later pas Humanitas en het ETF van de gemeente Rotterdam betrokken in de aanpak.

Implementatie schaal & intensiteit
Met betrekking tot de schaal van het project geeft men aan dat het voor nu zo kon worden gedaan, maar dat voor de toekomst wordt gekeken hoe de aanpak van gedigitaliseerde criminaliteit vormgegeven kan worden omdat het project veel capaciteit vraagt. De vraagstukken hoe dit geborgd kan worden in de organisatie liggen nu binnen de eenheid bij het OM en de driehoek.

Toekomstplan
Het is nog niet duidelijk hoe het project er in de toekomst uit zal zien. De respondent denkt zelf dat er per district een vaste kern moet zijn (zoals nu wordt gedaan) binnen de eenheid voor gedigitaliseerde criminaliteit om zaken te kunnen gaan draaien. Het moet uiteindelijk een automatisme worden wanneer iemand op een VVC zit en de 'workload' bespreekt met het OM, dat het ook over het aantal geldezels gaat. Het project moet worden geborgd door mensen verantwoordelijk te houden, prioriteit te behouden en opsporingsonderzoeken te blijven uitvoeren.

Toepasbaarheid andere eenheden
Of de aanpak van geldezels toepasbaar is in andere eenheden ligt volgens de respondent aan hoe groot de problematiek en noodzaak is binnen andere eenheden. Eenheden met een beperkt aantal geldezel zaken hebben wellicht minder behoefte aan een dergelijke grootschalige aanpak.

4.4.6 Cyber HQ

Eenheid Zeeland-West-Brabant

Introductie

Het project 'Cyber HQ (headquarters)' betreft de vorming van een multidisciplinair team - bestaande uit politiemedewerkers vanuit tactiek, specialisme en intel – op regionaal niveau dat zich richt op verschillende pijlers in de aanpak van cybercriminaliteit. Om dit te bewerkstelligen zijn het regionale cybercrimeteam en de Squad Cyber[43] van de DRIO (Dienst Regionale Informatie Organisatie) gefuseerd. De respondent is sinds april 2017 teamleider van het regionale cybercrimeteam en nu teamleider van het TDO (Team Digitale Opsporing) en het Cyber HQ.

Aanleiding

Het idee voor een Cyber HQ in de eenheid Zeeland-West-Brabant is ontstaan vanuit verschillende behoeften. Op een hoger niveau moest de gehele politieorganisatie toekomst bestendigd gemaakt worden op het digitale domein. Binnen de eenheid wilde men de organisatie in alle haarvaten (ook basisteams, districtsrecherches en andere afdelingen) meenemen op het gebied van digitale criminaliteit. Vervolgens kwamen drie portefeuillehouders (van digitalisering en cyber, intelligence en opsporing) tot de conclusie dat er twee zogenoemde 'vliegwielen' nodig waren binnen de eenheid: een voor ondersteuning en een voor opsporing. Deze vliegwielen moeten samen zorgen voor een versnelling van energie en kennis binnen het digitale domein. Om hier vorm aan te geven wilden de portefeuillehouders meer balans creëren tussen intelligence, tactiek en specialismes. Door deze drie onderdelen op het gebied van cybercriminaliteit fysiek bij elkaar te brengen in een team en de capaciteit van de drie onderdelen in balans te brengen is uiteindelijk het Cyber HQ ontstaan. Het Cyber HQ is eind 2019 opgezet, nadat een interne memo is opgesteld en uiteindelijk goedgekeurd door de eenheidsleiding.
De belangrijkste betrokkenen bij de opzet van het team zijn de drie eerder genoemde portefeuillehouders, de teamchef specialistische opsporing en de respondent.

Beschrijving project

Inhoud
Het Cyber HQ is een multidisciplinair team dat bestaat uit een fusie van het regionale cybercrimeteam (19,5FTE, waarvan de helft specialistische en de helft tactische politiemedewerkers) en de DRIO Squad Cyber binnen de eenheid. De twee teams zijn gefuseerd tot een team dat fysiek bij elkaar zit, met een nieuw huisvestingsplan, extra middelen, autorisaties en gezamenlijk werkproces. Hierbij is extra capaciteit toegevoegd in de vorm van intelligence medewerkers, zodat er meer balans ontstaat tussen intel, tactiek en specialisme.

Er worden drie hoofdpijlers onderscheiden in de aanpak van het Cyber HQ:

- **Operatie**: dit betreft het uitvoeren van operationele onderzoeken en interventies.
- **Crisis management**: op regionaal

43 De Dienst Regionale Informatie Organisatie bestaat uit verschillende onderdelen ('squads') die zich op specifieke thema's richten (zoals ondermijning, synthetische drugs en cybercrime).

niveau worden incidenten ondervonden rondom semi-vitale infrastructuur en incidenten die impact hebben op de maatschappelijke veiligheid (zoals een hack op de GGD). Vanuit het CyberHQ wordt gekeken welke rol gepakt kan worden rondom crisis situaties. Er wordt onder andere geïnventariseerd of piketdiensten kunnen worden gedraaid zodat er 24/7 bezetting is binnen het Cyber HQ. Dit onderdeel is ten tijde van het onderzoek nog in ontwikkeling (ook op nationaal niveau).

- **Specialisatie op thema phishing**[44]: enerzijds worden op dit thema opsporingsonderzoeken gedraaid, anderzijds wordt er een data gedreven bestrijdingsmethodiek ontwikkeld. Door op elke criminele bedrijfsstap van phishing intelligence op te bouwen probeert men specifieke interventies uit te voeren (vaak met partners en zo geautomatiseerd mogelijk). Een voorbeeld is een detectietool die is gebouwd met TNO, THTC en ECTF. De tool scant SSL-certificaten op zoek naar nieuwe domeinen. Vervolgens worden met behulp van 'machine learning' phishing-domeinen gevonden. Een rapportage hiervan wordt handmatig gecheckt, waarna de websites worden neergehaald. De processen en interventies worden steeds technisch (technisch te harmoniseren met bestaande systemen), organisatorisch (organisatorisch uitvoerbaar) en juridisch (in lijn met wetgeving) ingericht.

De fysieke fusie (in de vorm van huisvesting) heeft ten tijde van het onderzoek nog niet plaatsgevonden in verband met coronamaatregelen binnen de politie. In de tussentijd is het team al wel gevormd; er zijn gezamenlijke briefings, worden gezamenlijke keuzeprocessen doorlopen etc.

Doel

Het overkoepelende doel van het Cyber HQ is om de eenheid toekomstbestendig te maken, te intensiveren en energie te creëren op het gebied van digitale criminaliteit. De drie portefeuillehouders hebben ieder een eigen doelstelling gekoppeld aan het Cyber HQ[45]:

- **Portefeuillehouder digitalisering/ cyber**: (1) de aanpak van cybercrime op regionaal niveau zowel kwalitatief als kwantitatief verbeteren en (2) de energie vanuit het Cyber HQ gebruiken om ook binnen andere onderdelen van de eenheid digitalisering en cybercrime verder te helpen.
- **Portefeuillehouder Intelligence**: (1) De Squad Cyber binnen de DRIO vorm geven en in werking brengen, (2) samen met de digi specialisten en het cyberteam de werking en toegevoegde waarde van thematische intelligence vanuit het werk (operatie) ontwikkelen en (3) het gezamenlijk opbouwen van de nationale informatie coördinatie en intelligence gestuurde aanpak van het fenomeen phishing.
- **Portefeuillehouder opsporing**: (1) in werking brengen van de zogenaamde 'houtskoolschets[46]', als onderdeel van de vernieuwde opsporing en (2) ervaring opdoen.

Doelgroep

Er is niet direct een doelgroep te koppelen aan het project Cyber HQ. Wel zijn er verschillende organisatieonderdelen waar nauw mee wordt samengewerkt, zoals de vier districten. Vanuit het Cyber HQ zijn er bijvoorbeeld 'cyber intel liasons' (operationeel specialisten A) die gekoppeld zijn aan de districten zodat er actief verbinding wordt gezocht.

Niveau

Het Cyber HQ is een team op regionaal niveau, maar door overleggen zoals het LOCO en ROCO (Regionaal Operationeel CyberOverleg) ook op een landelijk- en districtsniveau ingebed. Het ROCO bestaat uit twee team coördinatoren van het CyberHQ, vier liaisons van het CyberHQ en vier coördinatoren van de districtelijke cyberteams.

Het team richt zich primair op fenomeenonderzoeken, vaak in de vorm van cybercrime in enge zin. Daarnaast probeert men ook randvoorwaarden te creëren (door kennis en kunde, de informatiepositie en intakeprocessen te verbeteren) waardoor gedigitaliseerde criminaliteit uiteindelijk ook effectief kan worden bestreden.

Onderbouwing

Verwachte werking

Er zijn verschillende verwachtingen en principes waardoor de eerder benoemde doelen zouden moeten worden behaald. Allereerst wordt aangegeven dat de verschillende expertises (tactiek, specialisme en intel) elkaar versterken doordat zij bij elkaar zijn gezet. Vanuit deze positie kan men van elkaar leren, kan op de juiste manier worden gecommuniceerd en kunnen binnen de eenheid en het land initiatieven worden genomen.

Daarnaast wordt verwezen naar het principe van de 'dynamische driehoek', waarin tactiek, intelligence en specialisme gezamenlijk en gelijkwaardig (voorheen was de tactische opsporing dominant, zij bepaalden zelf of specialisme/intelligence nodig was) naar een probleem kijken. Er dient continue gezocht te worden naar een juiste balans binnen de driehoeken door afhankelijk van het opsporingsonderzoek te bepalen waar het zwaartepunt ligt. Wordt er bijvoorbeeld een inbeslagname gedaan van veel goederen, dan zijn er twee weken veel digitale spullen die moeten worden uitgelezen waardoor het zwaartepunt bij digitaal specialisme ligt. Vervolgens moet tactiek en intelligence het interpreteren en uitzoeken, waardoor het zwaartepunt verschuift. Er dient continue gewisseld te worden, wat vereist dat flexibiliteit en wendbaarheid georganiseerd zijn binnen de afdeling.

Een derde principe dat naar voren komt is de 'houtskoolschets'. Dit betreft een werkwijze waarbij onder andere meer nagedacht moet worden hoe men aan de voorkant van een probleem kan komen. Hier

44 De eenheid Zeeland-West-Brabant is verantwoordelijk voor de aanpak van het thema phishing.

45 De individuele doelstellingen zijn geformuleerd in een interne memo over de 'samenwerking inrichting cyber HQ'.

46 De 'houtskoolschets van de opsporing' is een strategie die tot doel heeft om de kwaliteit van het politiewerk te verbeteren door de samenhang tussen de opsporing en de informatieorganisatie te vergroten. Onder andere handelen in het moment, criminaliteit voorkomen en het benutten van overvloed zijn pijlers in deze strategie. Teams moeten worden ingericht op gelijkwaardigheid, dynamisch zijn en in driehoekstructuren te werken. Zie https://vimeo.com/427649978 voor meer informatie over de houtskoolschets van de opsporing.

zijn verschillende randvoorwaarden voor nodig, waaronder een goede informatiepositie.

Bijhouden werking
De normatieve doelstellingen worden bijgehouden, bijvoorbeeld door resultaten uit interventies die worden gedaan bij te houden (hoeveel phishing websites zijn er neergehaald). Verder is er binnen de eenheid een monitor cybercrime, die zich deels ook focust op het kwalitatieve deel waarin men bijhoudt of de aanpak van cybercrime op regionaal niveau daadwerkelijk wordt verbeterd. Hiervoor houdt men bijvoorbeeld het aantal digi kamers en taak accenthouders bij en de activiteiten die zij weer verrichten.

Doelen behaald?
Een aantal van de doelen wordt volgens de respondent behaald. Zo is de informatiepositie op het gebied van phishing sterk verbeterd en lopen op dit thema omvangrijke publiek-private projecten, heeft men periodiek een intelligence beeld en wordt de houtskoolschets van de opsporing nu in werking gebracht. Verder wordt aangegeven dat men continue wil blijven doorontwikkelingen en op zoek wil gaan naar verbeteringen.

Samenwerking

In de samenwerking kan onderscheid worden gemaakt tussen samenwerking binnen het Cyber HQ en samenwerking met anderen in de politieorganisatie.

- Intern (binnen het cyber HQ): oude cybercrimeteam (bijna 20FTE), intelligence (7FTE en wordt nu uitgebouwd)
- Extern (buiten het cyber HQ): teamchef kolom specialistische opsporing, sectorhoofd Dienst Regionale Recherche, sectorhoofd van intelligence

De samenwerking binnen het cyber HQ bestaat uit een briefing die elke dag plaatsvindt, belangrijke overleggen etc. Buiten het cyber HQ wordt verantwoording afgelegd aan de teamchef kolom specialistische opsporing, het sectorhoofd DRR (Dienste Regionale Recherche) en het sectorhoofd van Intelligence. De samenwerking in de vorm van het Cyber HQ is voor onbepaalde tijd.

Afspraken
Er zijn zowel formele afspraken als informele afspraken gemaakt omtrent het Cyber HQ. Formele afspraken zijn er bijvoorbeeld met teamchefs over het personeelsgedeelte, autorisaties, P-zorg en R&O cyclussen. Daarnaast zijn er normatieve resultaatverplichtingen in de vorm van bijvoorbeeld GVA-afspraken en LOCO-afspraken. Voor de dagelijkse werking zijn vaak meer informele afspraken, zoals dat mensen gaan meedraaien in piketdiensten etc.

Kwaliteit samenwerking
De samenwerking wordt als positief omschreven, vooral over de balans die is ontstaan is de respondent erg tevreden. De balans in een team heeft namelijk uitwerking op hoe een team functioneert (de motivatie, sfeer) maar ook op de output die een team levert. Het team is complementair aan elkaar en door de balans worden continue ‘de goede dingen’ gedaan.

Implementatie praktijk

Het Cyber HQ is op dit moment grotendeels vormgegeven zoals beoogd. Het fundament staat namelijk (vliegwiel zijn, motorblok zijn en energie creëren) en ook de randvoorwaarden in de vorm van mensen en middelen zijn aanwezig. Alleen de fysieke huisvesting staat nog op de planning vanwege corona. Er wordt nu ook verder nagedacht over de manier waarop men goed kan communiceren met alle partners (een nieuwsbrief, website, etc.).

Er is tevredenheid over de commitment die er is vanuit de eenheidsleiding tot aan de teamchefs en de ruimte die wordt gelaten om het als een pilot te doen, waarin mag worden geleerd en geëxperimenteerd. Wat niet goed gaat vindt de respondent lastig te benoemen. Wellicht op detailniveau dat dingen minder goed lopen, zoals de samenwerking met de districten die nog naar een hoger niveau kan worden getrokken. Daarnaast kan de slagkracht omhoog door nog meer met elkaar af te stemmen wat men nodig heeft in een onderzoek om tot het gewenste resultaat te komen.

Implementatie schaal & intensiteit
Het CyberHQ is op dit moment ingericht conform de landelijke formatieve normering, aangevuld met extra intel capaciteit. Voor de huidige situatie en normatieve afspraken is de capaciteit volgens de respondent (net) toereikend. Echter, gezien de snelle digitalisering van de wereld en criminaliteit wordt verwacht dat een veranderende visie en extra capaciteit onontkoombaar zijn.

Toekomstplan
Er wordt aangegeven dat de politie niet verder dan 3 jaar vooruit moet kijken op dit thema, omdat er veel ontwikkelingen zijn en flexibiliteit vereist is. In de toekomst wordt wel verwacht dat het Cyber HQ een autoriteit wordt binnen de eenheid, op basis van de kennis en expertise dan is opgebouwd. Ook in het bredere digitale domein; volgens het concept van het cyberHQ met de drie pijlers wil men straks iedere vorm van criminaliteit in het digitale domein kunnen tackelen. Verder is het doel om te gaan kijken op welke wijze bestaande opsporingsprocessen kunnen worden verbeterd vanuit het Cyber HQ en TDO.

Toepasbaarheid andere eenheden
Het concept van het Cyber HQ is volgens de respondent gemakkelijk toe te passen binnen andere eenheden. Het gaat om commitment krijgen, capaciteit labelen en vervolgens het gewoon doen. In andere eenheden ontstaan inmiddels soortgelijke concepten, bijvoorbeeld door extra capaciteit in te zetten op intelligence. De vraag is dan of men echt bij elkaar in een team zit, of de continuïteit gewaarborgd kan worden en of er niet steeds een uitvraag gedaan moet worden naar andere afdelingen. Binnen het Cyber HQ is er een persoon die de leiding heeft en beslissingen maakt. Het vraagt dus wel om een ander inrichtingsproces.

4.4.7 Digikamers

Eenheid Zeeland-West-Brabant

Introductie

De digikamer is een fysieke ruimte waarin materialen beschikbaar zijn om binnen de eenheid digitaal politiewerk te realiseren en enthousiasmeren. De respondent is werkzaam binnen de staf van de politie-eenheid Zeeland-West-Brabant bij politieprofessie en ondersteunt portefeuillehouders, zoals de portefeuillehouder digitalisering en cyber. De respondent houdt zich bezig met de ontwikkeling van het politievak, zo ook hoe bijvoorbeeld de digitalisering van de maatschappij, veiligheid en criminaliteit omgezet kan worden in een passend politieproduct.

Aanleiding

De digikamers zijn ontstaan vanuit een bredere doelstelling waarbij de respondent en de portefeuillehouder digitalisering en cybercrime constateerden dat er een beweging ingezet moest worden in alle lagen van de organisatie (basisteam, district- en eenheidsniveau) om de digitalisering (van criminaliteit) aandacht te geven binnen de organisatie. Vanuit de gehele organisatie kreeg men namelijk signalen dat politiemedewerkers niet wisten wat ze moesten doen op het gebied van digitalisering.

Ondertussen gingen er op het niveau van basisteams enkele enthousiaste mensen aan de slag met het thema, al merkten zij dat er andere middelen nodig waren dan zij ter beschikking hadden op dat moment. Een specifieke groep van 3 collega's uit een basisteam heeft toen zelf vormgegeven aan de digitalisering, door vaak op een privé computer op een OSINT-matige manier (open bronnen raadplegen) te werk te gaan. Zo deed men bijvoorbeeld onderzoek via sociale media of op marktplaats. Door deze informatiepositie konden wijkagenten of opsporingsonderzoeken worden ondersteund. De respondent geeft aan dat de werkwijze op het randje was van wat wel en niet kon, omdat er nog geen protocollen waren voor dergelijke werkwijzen.

Vanuit de werkwijze van dit team is uiteindelijk begin 2020 de eerste digikamer pilot ontstaan voor het desbetreffende basisteam. Samen met het team is bedacht welke middelen, instrumenten en opleidingen er nodig waren. Er zijn toen OSINT-opleidingen, een UFED (computer om telefoons uit te lezen), grote schermen om te 'scrummen' en laptops geregeld vanuit de politieorganisatie die normaal voor specialisten binnen de Dienst Regionale Informatie Organisatie (DRIO) beschikbaar waren. Verder wilde men dat het er mooi uit zou zien zodat mensen nieuwsgierig worden om naar binnen te lopen. Er is toen een digitale opening geweest van de digikamer waarin heel het land mee kon kijken. Al snel werd het een beweging, waarbij andere basisteams ook een digikamer wilden. Op eenheidsniveau viel vervolgens het besluit dat men als pilot in elk district een digikamer zou inrichten. De digikamer is dus ontstaan ter ondersteuning van een beweging vanuit de realisatie dat er iets moest gebeuren met de digitale wereld en digitale criminaliteit. Hiervoor zijn volgens de respondent andere middelen en kwaliteiten nodig.

Beschrijving project

Inhoud

De digikamer is een instrument om bekwaamheid op digitaal politiewerk te realiseren binnen de politie-eenheid. Het is een fysieke locatie met verschillende middelen waar in principe vier medewerkers voor worden vrijgemaakt. De digikamer heeft verschillende functies:

- Het is een werkkamer voor de digitale wijkagent.
- Het is een werkplek waar telefoons uitgelezen kunnen worden (door de aanwezigheid van een UFED).
- Het is een plek waar OSINT-onderzoeken uitgevoerd kunnen worden.
- Er is een beeldtafel (groot scherm) waar geografische kaartlagen met data over elkaar gelegd kunnen worden.
- Er worden 'scrumsessies' gehouden waarin men elkaar aanvult vanuit de verschillende informatiebronnen (OSINT, beeldtafel etc.).
- De digikamer faciliteert de gewenste beweging. Het jaagt namelijk het proces van de digitalisering van het politiewerk aan door mensen enthousiast te maken en te prikkelen om hiermee aan de slag te gaan. Collega's lopen bijvoorbeeld langs en gaan vragen stellen.

De digikamers zijn verder breed inzetbaar. Zo vindt de eerste veredeling van ingewikkelde cyberzaken plaats bij het basisteam en worden de digikamers steeds meer gebruikt voor live sessies over veiligheid en digitale criminaliteit voor burgers. Inmiddels heeft elk district binnen de eenheid een basisteam waar een digikamer is ingericht. Basisteams worden pas voorzien van een digikamer op het moment dat er enthousiasme en energie wordt geproefd en er minimaal vier medewerkers worden vrijgemaakt voor de digikamer.

Doel

Het belangrijkste doel van de digikamers is om de digitalisering breed binnen de politieorganisatie vorm te geven. Dit doel is vastgelegd in beleidsdocumenten.

Doelgroep

De digikamers zijn in eerste instantie bedoeld voor medewerkers binnen de basisteams van de politie. Inmiddels is men ook in gesprek over soortgelijke mogelijkheden voor districtsrecherches.

Niveau

Digikamers zijn ingericht op het niveau van basisteams en richten zich op meerdere onderdelen van het politiewerk: van communicatie tot preventie en opsporingsonderzoeken.

Onderbouwing

Verwachte werking

Er worden verschillende factoren benoemd die ervoor kunnen zorgen dat de digikamers bij dragen aan de beoogde doelen. Zo worden er middels de digikamer middelen en opleidingen beschikbaar gesteld aan medewerkers in de basisteams die op dit moment niet voorhanden zijn en nodig zijn om vorm te geven aan digitalisering. Daarnaast wil men graag inspelen op positieve energie die er al is onder medewerkers. Het idee is om deze energie te vergroten en succes te laten ontstaan zodat het een onderwerp wordt waar steeds meer mensen bij willen zijn. In aanvulling hierop probeert men passie en werk te verbinden, door mensen die 'boven het maaiveld' uitsteken op het gebied van digitalisering te faciliteren. Ten slotte staat het principe 'changing by design' centraal bij het project, waarbij men verandering bij mensen wil creëren

door hun omgeving te veranderen in plaats van het schrijven van stukken en organiseren van vergaderingen of werkgroepen. Het project is verder vooral gebaseerd op ‘gezond boerenverstand’, aangevuld met kennis van specialisten vanuit de opsporing.

Bijhouden werking
Bij de aanvang van het project is besloten om niet zozeer naar cijfers te gaan kijken, maar vooral te kijken of er een beweging ontstaat. Uiteindelijk moet die beweging dan weer resulteren in minder slachtoffers en meer verdachten. Er is wel een monitor opgezet door een collega vanuit de afdeling ‘control’, die de eerdergenoemde beweging binnen de eenheid monitort. Vanuit de monitor houdt men zowel harde cijfers bij (aangiften, opgeloste zaken etc.) als activiteiten en deelprojecten rondom de beweging (persberichten, leermomenten, aantal opleidingen, aantal digikamers etc.). Door de activiteiten en harde cijfers te combineren probeert men inzicht te krijgen in de effecten. Het gaat dan niet om ‘keiharde’ effecten, maar het verkrijgen van een beter beeld.

Doelen behaald?
Op dit moment ziet men enerzijds dat er op verschillende plekken meer incidenten - zowel aangiften als ambtshalve vervolging[47] - plaatsvinden. Dit wordt verklaard door de extra inspanningen van de basisteams die ervoor zorgen dat er meer zaken aan het licht komen. Anderzijds wordt gezien dat het aantal opgeloste zaken toeneemt.

47 Een besluit tot vervolging en opsporing door de officier van justitie en politie zonder dat er aangifte wordt gedaan.

Samenwerking

Bij de opzet van de digikamer zijn vele afdelingen en onderdelen van de politieorganisatie betrokken geweest, zoals het PDC (politie dienstencentrum), HRO (human resource ontwikkelen en opleiden), HRM (human resource management), financiën, IV (informatievoorziening), de DRIO (dienst regionale informatieorganisatie), het landelijk cybercrimeteam en de korpsleiding. Voor het project wordt samengewerkt met een grote hoeveelheid personen binnen de politieorganisatie. Een vast team van 8 personen vanuit ondersteuning bestaat uit collega’s van de afdelingen communicatie, control, bedrijfsvoering, HRO, thema jeugd, bestuur ondersteuning en sociale media. Dit team praat over alle ontwikkelingen rondom de eerdergenoemde beweging van digitalisering en cybercrime. Een keer in de twee weken bespreekt men alle deelprojecten (waaronder de digikamers). Verder zijn er facilitaire ondersteuners (voor het aansluiten van computers, verven van muren etc.) en zijn portefeuillehouders betrokken. Er is in de samenwerking met alle collega’s veel telefonisch contact of contact via e-mail.

Afspraken
De samenwerking binnen het ondersteuningsteam is niet gebaseerd op formele afspraken. Op het moment dat een project zich aandient kijkt men met elkaar waar het grootste accent zit van kwaliteiten die nodig zijn. De desbetreffende collega is dan vaak de trekker van het project, maar verder worden verschillende taken verdeeld over de verschillende afdelingen.

Kwaliteit samenwerking
De samenwerking wordt als ‘super’ omschreven. Men probeert te werken als een ecosysteem, waarbij iedereen elkaar aanvult, ongevraagd adviseert en anderen in positie worden gebracht. Er is geen sprake van een hiërarchie, het is het aanvullen van kwaliteiten om een volgende stap te maken. De respondent vindt dit prettig werken. Een verklaring voor de goede samenwerking ligt in de manier van werken, maar is ook afhankelijk van de waardering die men krijgt dat men goed bezig is. Voorbeelden hiervan zijn verzoeken om digikamers, complimenten, aangewezen worden als voorbeeld etc.

Implementatie praktijk

Op dit moment is het project vormgegeven zoals men dat heeft beoogd. Tussendoor vinden continue aanpassingen plaats omdat de digitale wereld ook steeds veranderd. Een voorbeeld is dat er nu camera’s worden aangeschaft, omdat collega’s steeds meer digitaal met de burger willen communiceren om digitaal slachtofferschap te voorkomen. Wanneer men tegen iets aan loopt, wordt dit onmiddellijk besproken. Het is een voortdurend proces en zit niet in beton gegoten. Wat wel vast staat is het concept: een plek creëren op een basisteam om energie los te maken, de juiste materialen beschikbaar stellen en een plek creëren die anderen aantrekt om in te stappen op digitalisering van het politiewerk.

Wat men goed vindt gaan is de beweging die er ontstaat op het thema en de energie die er wordt losgemaakt. Minder goed is dat de bevlogenheid die men constateerde bij het eerste team nog niet bij alle andere basisteams wordt gezien omdat al snel de ‘klassieke agenda’ weer voorrang krijgt.

Implementatie schaal & intensiteit
Op dit moment wordt de schaal waarop het project is geïmplementeerd als prima ervaren. Voor de nabije toekomst voorziet de respondent dat elk basisteam een dergelijke ruimte moet hebben en dat er niet 4 maar 40 mensen moeten zijn binnen de basisteams die handig zijn op het thema. Op dit moment zijn 4 mensen fulltime gealloceerd aan de digikamer, wat als te weinig wordt ervaren gezien de digitale ontwikkelingen en cijfers van online criminaliteit.

Toekomstplan
Op dit moment is er in elk district een digikamer. In de plannen van het komend jaar staat dat ook andere basisteams binnen de districten kunnen aangeven dat zij een digikamer willen hebben. Ook is men in gesprek met soortgelijke mogelijkheden voor districtsrecherches. Verder wordt er aangegeven dat de digikamer er in de toekomst heel anders uit kan zien met andere modellen, technieken en opleidingen omdat de ontwikkelingen op het thema erg snel gaan volgens de respondent.

Toepasbaarheid andere eenheden
Het concept is volgens de respondent toe te passen in andere eenheden, omdat de taakstelling en verantwoordelijkheid van elk basisteam binnen de nationale politie soortgelijk is. Op dit moment worden of zijn ook in andere eenheden vergelijkbare concepten als de digikamer opgezet. Het concept en de doestelling is overal hetzelfde. Binnenkort wordt een voorstel opgesteld om de digikamers als standaard op te gaan nemen in de inrichting van basisteams.

4.4.8 Digitaal weerbaar Breda

Eenheid Zeeland-West-Brabant

Aanleiding

Het project digitaal weerbaar Breda is ontstaan naar aanleiding van gesprekken tussen verschillende personen[48]die interesse hebben in digitale veiligheid. Tijdens deze gesprekken werd geconstateerd dat cybersecurity vaak in kolommen (verticaal) is georganiseerd, waarbij iedere organisatie zijn eigen cybersecurity regelt. Voorbeelden zijn banken, bakkers en slagers die ieder voor zich hun cybersecurity vormgeven. Tijdens het gesprek is de wens geuit om ervoor te zorgen dat er meer horizontaal gedacht wordt over cybersecurity, waar verschillende organisaties met elkaar in contact komen en samenwerken. Dit heeft uiteindelijk geresulteerd in een pilotproject op lokaal niveau in de gemeente Breda met vitale partnerorganisaties, genaamd 'digitaal weerbaar Breda'. Betrokken organisaties zijn onder andere de politie, de gemeente, een ziekenhuis, een waterbedrijf, een energieleverancier, een telecomprovider en een ICT-bedrijf. De basis voor het project is een intentieverklaring van de verschillende organisaties om dit project vorm te geven.

Beschrijving project

Het project kan worden gezien als een ecosysteem, waarin verschillende vitale partnerorganisaties met elkaar samenwerken op het gebied van cyberveiligheid. Het uiteindelijke doel van digitaal weerbaar Breda is 'door informatie met elkaar te delen elkaar tevens in positie te brengen om de digitale weerbaarheid te vergroten'. De samenwerking wordt omschreven als een ecosysteem, waarin geen hiërarchie is of een organisatie die centraal staat maar waar organisaties vanuit vertrouwen met elkaar kennis en informatie delen en van elkaar leren.
Er zijn tot nu toe 3 bijeenkomsten geweest waarin de organisaties bij elkaar zijn gekomen. Een concreet voorbeeld van wat er uit de bijeenkomsten komt is dat een van de organisaties bijvoorbeeld recent een incident response plan heeft ontwikkeld. Andere organisaties hebben aangegeven dit niet te hebben, wat heeft geresulteerd in een nieuwe bijeenkomst waarin de desbetreffende organisatie het plan zal presenteren aan de andere organisaties om hiervan te leren. Een ander voorbeeld is dat de gemeente Breda heeft verzocht om als groep na te gaan denken over de cyberveiligheid rondom de gemeenteraadsverkiezingen van volgend jaar. Verder deelt men vanuit de politie bijvoorbeeld informatie over werkwijzen van criminelen, zodat de verschillende organisaties hierop kunnen inspelen.

Digitaal weerbaar Breda vindt op lokaal niveau plaats, maar doordat verschillende organisaties met regionale of soms landelijke vertegenwoordigers aansluiten is er ook sprake van een bredere betrokkenheid. Vanuit de politie is men op eenheidsniveau betrokken bij het project, doordat de respondent bij de bijeenkomsten aansluit. Het project is gestart medio 2020 en de intentieverklaring tussen de organisaties is voor de duur van in ieder geval een jaar. De respondent hoopt dat vanaf dat moment de samenwerking zo vanzelfsprekend is dat iedereen door wilt.

Onderbouwing project

Er wordt verwacht dat digitaal weerbaar Breda bijdraagt aan de digitale weerbaarheid omdat er zowel vanuit extern onderzoek[49] als ervaringen binnen de politie wordt gezien dat er op horizontaal niveau moet worden samengewerkt om cyberveiligheid te creëren. De respondent geeft aan dat zowel (lokale) systemen als organisaties met elkaar verbonden zijn en van elkaar afhankelijk zijn op het gebied van cyberveiligheid[50]. Zo ziet men in opsporingsonderzoeken hoe criminelen gebruik maken van kwetsbaarheden in kleinere of minder goed beveiligde organisaties of apparaten om vervolgens toegang te krijgen tot systemen of gegevens van andere organisaties of apparaten. Verder verwacht de respondent dat de betrokken organisaties vanuit energie[51] en vertrouwen kennis met elkaar gaan delen zodat de organisaties van elkaar kunnen leren. Er wordt niet expliciet bijgehouden in welke mate er bepaalde doelen worden bereikt. Wel is er verslaglegging van de bijeenkomsten en worden actiepunten bijgehouden.

Samenwerking

De volgende organisaties zijn betrokken bij het project digitaal weerbaar Breda:
- Amphia Ziekenhuis
- Brabant Water
- Essent
- Landelijke telecomprovider
- ICT-bedrijf
- Gemeente Breda
- Politie

Op het moment van schrijven zijn er drie bijeenkomsten geweest. Steeds vaker haken personen aan die vanuit een IT-functie werkzaam zijn bij de verschillende organisaties, zodat er ook op technisch niveau over de beveiliging van systemen kan worden gesproken. Er zijn naast de intentieverklaring geen concrete afspraken gemaakt met organisaties.

Kwaliteit samenwerking

Met betrekking tot de kwaliteit van de samenwerking geeft de respondent aan dat organisaties over het algemeen erg gesloten zijn over cyberincidenten en cyberveiligheid richting externe organisaties. Langzaam maar zeker ziet de respondent dat men hier tijdens de bijeenkomsten meer open over is. Zo geven organisaties aan geen incident response plan te hebben. Dit komt volgens de respondent door de vertrouwde omgeving die wordt gecreëerd waarin politie en gemeente bijvoorbeeld eerst hun ervaringen hebben gedeeld, waardoor andere organisaties volgen.

Verbeterpunten samenwerking

De samenwerking zou kunnen worden verbeterd door de frequentie van de overleggen te verhogen, zodat de relatie tussen de partners sneller gaat groeien. Daarnaast wordt er nagedacht om een 'vrij inloopmo-

48 Waaronder de respondent vanuit de politie en iemand vanuit een ICT-bedrijf.

49 De respondent verwijst naar een rapport dat is opgesteld voor de gemeente Amsterdam door Connected worlds over vitale digitale infrastructuur (zie https://connectedworlds.nl/vitale-digitale-infrastructuur-gemeente-amsterdam/).

50 Met betrekking tot de onderlinge afhankelijkheid van organisaties op het gebied van cyberveiligheid wordt ook wel gesproken over cyber-ketenweerbaarheid (Bekkers et al., 2021).

51 Met energie bedoelt de respondent dat men vanuit passie samen digitale weerbaarheid wil vergroten.

ment' te organiseren tussen vakgenoten, zodat 'operationele' ervaringen en actuele cyberdreigingen met elkaar kunnen worden besproken.

Implementatie

De samenwerking vindt plaats op basis van de eerder genoemde intentieverklaring. Tussendoor wordt de vorm van het project aangepast op basis van het verloop van de bijeenkomsten. Een voorbeeld van iets wat men wil gaan aanpassen is om vaker bij elkaar te komen. De aanleiding hiervoor is dat er tussen de bijeenkomsten door veel gebeurd en incidenten plaatsvinden, waardoor het wenselijk is om hier vaker met elkaar over te spreken.

Wat goed gaat met betrekking tot het initiatief volgens de respondent is dat er nu een overleg is en dat mensen steeds meer vertrouwen voelen om interne ervaringen met het ecosysteem te delen. Wat nog minder goed gaat is dat het contact tussen de partners zich nog beperkt tot de vaste overlegmomenten. De tussentijdse contactmomenten moeten nog groeien.

Implementatie schaal & intensiteit

Het project is volgens de respondent voor nu op de juiste schaal geïmplementeerd, door het lokaal te organiseren. Uiteindelijk moeten de lokale bijeenkomsten ertoe leiden dat er ook op regionaal/landelijk niveau gesproken wordt over cyberveiligheid tussen de verschillende vitale partnerorganisaties. De intensiteit mag voor de respondent worden verhoogd zoals eerder besproken, door vaker bij elkaar te komen.

Toekomstplan

Er is geen concreet toekomstplan voor het project. De respondent hoopt dat op basis van de bijeenkomsten er uiteindelijk afspraken worden gemaakt en zaken als certificering en keurmerken ontstaan zoals die ook in het fysieke veiligheidsdomein bestaan. Daarnaast wordt verwacht dat door de regelmatige bijeenkomsten de samenwerking uiteindelijk onmisbaar en vanzelfsprekend wordt. Het project is volgens de respondent goed toepasbaar in andere gemeenten. Er is vooral energie en vertrouwen nodig vanuit betrokken partnerorganisaties om een dergelijk project vorm te geven.

4.4.9 Dagelijkse cyberquery

Eenheid Limburg

Introductie

Het initiatief 'dagelijkse cyberquery' betreft het duiden en scoren van aangiften cybercrime door medewerkers van de Dienst Regionale Informatie Organisatie (DRIO), zodat basisteams concrete aanwijzingen krijgen over aangiften die opgepakt dienen te worden. De aangiften die de DRIO scoort en duidt zijn aangiften die uit de cybercrime query naar voren komen.
De respondent is werkzaam als analist bij de Dienst Regionale Informatie Organisatie (DRIO) en het regionale cybercrimeteam, dat valt onder de Dienst Regionale Recherche (DRR).

Aanleiding

Er zijn een aantal aanleidingen die het initiatief tot stand hebben gebracht. Ten eerste hebben de DRIO en het cybercrimeteam de taak om de kennispositie van basisteams te verbeteren op het gebied van cybercriminaliteit. Daarnaast wilde men graag de 'koudwatervrees' wegnemen onder politiemedewerkers om met zaken cybercriminaliteit aan de slag te aan en daarbij richting geven aan welke zaken effectief kunnen worden opgepakt. Verder is het idee voor een dagelijkse veredeling gebaseerd op een initiatief uit de eenheid Oost-Nederland. Hier werden zowel aangiften cybercrime als gedigitaliseerde criminaliteit op soortgelijke wijze veredeld. Eind 2019 is de eerste pilot in de eenheid Limburg opgestart.

Beschrijving project

Inhoud

Het initiatief betreft een dagelijkse veredeling van aangiften cybercriminaliteit door de DRIO en het regionale cybercrimeteam. Aangiften die door de landelijke cybercrime query worden gefilterd worden door medewerkers gescoord en geduid. Dit betekent dat opsporingsindicatie wordt bekeken en er op basis van de opsporingsmogelijkheden en impact een groene, oranje of rode kleur wordt gekoppeld aan een aangifte. Een groene kleur betekent dat basisteams wordt geadviseerd om de aangifte geen prioriteit te geven, een oranje kleur betekent dat er interessante opsporingsindicatie aanwezig is, en een rode kleur betekent dat de zaak met prioriteit moet worden opgepakt gezien de heterdaad mogelijkheden. De case-screener heeft wel de mogelijkheid om af te wijken van het advies van de DRIO. Aan de aangifte wordt een extra klasse toegevoegd (G71) zodat er een extra document ontstaat waar de veredeling in kan worden opgenomen die toegankelijk is voor alle collega's (ook binnen het BOSZ-systeem). Uiteindelijk wordt elke dag een overzicht gestuurd met de veredelde aangiften naar een grote lijst met politiemedewerkers (zie doelgroep). Op het moment van schrijven zijn er vier medewerkers binnen de DRIO en het cybercrimeteam die zich bezighouden met de dagelijkse veredeling van zaken cybercriminaliteit. Dit kost een medewerker ongeveer 1,5 uur per dag.

Doel
Er zijn verschillende doelen gekoppeld aan het initiatief. Ten eerste wil men de kennispositie verbeteren op het gebied van cybercriminaliteit, door kennis mee te geven over de 'modus operandi' en mogelijke digitale sporen voor de opsporing. Daarnaast moet het initiatief zorgen voor uniformiteit in de verwerking van aangiften cybercriminaliteit. Ten slotte dienen de basisteams in stelling gebracht te worden om cybercrime zaken op te pakken.

Doelgroep
De doelgroep van de dagelijkse veredeling op basis van de cyberquery betreft in eerste instantie case-screeners (medewerkers senior tactische opsporing) en leidinggevenden van basisteams (operationeel specialisten). Daarnaast krijgen de medewerkers van het cybercrimeteam, iemand van het OM en de DR's (districtsrecherches) ook het overzicht dagelijks toegestuurd om de veredelde aangiften in te zien.

Niveau
Het project vindt plaats op eenheidsniveau en de dagelijkse cyberquery wordt gebundeld per basisteam. Het type cybercriminaliteit waarvoor dit werkproces is ingericht betreft cybercriminaliteit in enge zin. Deze keuze is enerzijds gemaakt vanwege de expertise vanuit het regionale cybercrimeteam op technische delicten, anderzijds zou het includeren van gedigitaliseerde criminaliteit een te groot aantal aangiften opleveren om te veredelen.

Onderbouwing

Verwachte werking
Er wordt verwacht dat er door de dagelijkse cyberquery uniformiteit wordt gecreëerd in het verwerken en oppakken van aangiften cybercrime. Daarnaast zorgt de veredeling en het scoren van de aangiften ervoor dat medewerkers uit de basisteams in stelling worden gebracht om deze zaken op te pakken en dat zij weten waar zij vragen kunnen stellen. Ook staat de manier van werken dicht bij de belevingswereld van de collega's in de basisteams. Tot slot wordt verwacht dat de werkwijze goed werkt omdat deze in Oost-Nederland ook als goed en prettig is ervaren. De best practices zoals de G71 klasse komen uit Oost-Nederland. Het initiatief is gebaseerd op praktijkervaring en 'learning on the job'.

Bijhouden werking
Recentelijk zijn de cijfers met betrekking tot de afhandeling van de zaken die zijn gescoord en geduid binnen één district verzameld. Ook voor andere districten wordt dit nu verzameld. Het bleek dat 'oranje' zaken beduidend vaker werden opgepakt dan 'groene' zaken en dat er veel minder 'oranje' zaken waren dan 'groene' zaken. Dit vindt de respondent een goed teken, omdat men liever vol investeert op een kleiner aantal zaken met kansen, dan dat overal een beetje op wordt geïnvesteerd. Verder heeft er een evaluatie plaatsgevonden door iedereen op de lijst van de cyberquery te bellen voor feedback over de werkwijze. Voorbeelden van aanpassingen die op basis van de evaluatie zijn gedaan is dat de G71 toevoeging nu ook te zien is in het BOSZ-systeem en een verbetering van de uitleg van de delicten. Ook is de vormgeving verbeterd door per basisteam en per district de aangiften automatisch onder elkaar weer te geven. Of de doelen uiteindelijk zijn behaald is lastig te zeggen volgens de respondent. Wel helpt het initiatief medewerkers om de duiding en score van aangiften beter op het netvlies te krijgen.

Samenwerking

Er zijn verschillende medewerkers en afdelingen betrokken bij het initiatief. Vanuit de DRIO en het cybercrimeteam zijn vier collega's betrokken bij de dagelijkse veredeling van de aangiften. Daarnaast zijn er verschillende afdelingen die de veredeling te zien krijgen en meelezen. Dit zijn de DR's, BT's, het cybercrimeteam en het digitaal platform. Extern leest ook het OM leest mee met de cyber query. Het OM gaat op basis van deze ervaringen een richtlijn schrijven om aan te geven welke zaken daadwerkelijk opgepakt kunnen en moeten worden.

Afspraken
Er zijn enkele informele afspraken rondom het initiatief, zoals dat de DRIO probeert om voor 12 uur de lijst te versturen binnen de eenheid. Verder wordt het project wat formeler ingezet sinds er ook wordt gekeken in hoeverre aangiften worden opgevolgd volgens het advies. Er is geen eindduur bepaald voor het project. Wel is het einddoel om de dagelijkse query uiteindelijk overbodig te maken, wanneer collega's zelf ook zien en snappen wat men met de aangifte kan en welke aangiften het beste opgepakt kunnen worden. De komende twee à drie jaar zal dit volgens de respondent echter nog niet het geval zijn.

Kwaliteit samenwerking
De (geringe) samenwerking die er is met de basisteams verloopt gemakkelijk door de wijze waarop de aangiften veredeld aangeleverd worden. Wanneer er vragen zijn wordt er meteen geschakeld met de DRIO en het cybercrimeteam.

Implementatie praktijk

Gedurende de implementatie van het initiatief zijn er enkele aanpassingen gedaan. Zo werd de veredeling eerst in losse word-documenten gedaan en doet men dit nu in hetzelfde programma waar de aangiften ook gescoord worden (groen, oranje of rood). Hierdoor wordt er efficiënter gewerkt. Ook is het aantal medewerkers dat mee kan helpen met de veredeling vanuit de DRIO verhoogd van twee naar vier medewerkers.

Wat goed gaat binnen het project is dat er door de veredeling heel concreet aan basisteams wordt aangegeven welke opsporingskenmerken er zijn en met welk autorisatieverzoek en welke vragen zij bijvoorbeeld naar een bank moeten. Wat beter kan is de sturing vanuit de leiding op het project en ruimte maken om de werkwijze weer te evalueren.

Implementatie schaal & intensiteit
Het initiatief had eventueel in het begin op kleinere schaal kunnen worden geïmplementeerd volgens de respondent, door bijvoorbeeld met één district te beginnen. Op deze wijze kan er namelijk beter worden geëvalueerd met collega's. Indien de schaal zou worden vergroot door ook aangiften voor districtsrecherches te veredelen dan zouden zaken meer geclusterd moeten worden, omdat de districtsrecherche zich meer richt op fenomeenonderzoeken. Dit zou teveel capaciteit vragen.

De intensiteit is op dit moment hoog in de vorm van een keer per dag, maar wel noodzakelijk. Op het moment dat er minder vaak veredeld wordt is er kans dat de termijn van drie dagen waarin aangiften moeten worden gescreend niet wordt gehaald.

Toepasbaarheid andere eenheden
Het concept is volgens de respondent goed toepasbaar binnen andere eenheden. Om het concept te implementeren is capaciteit nodig die geborgd is, zodat er continuïteit is in de werkvoorbereiding. Verder is zoals eerdere genoemd enige snelheid vereist in verband met de benodigde case screening.

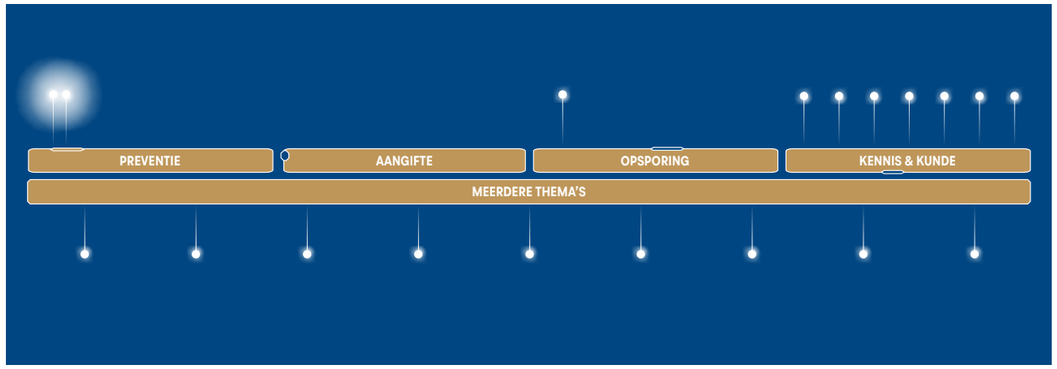
5. Conclusies en discussie

In dit hoofdstuk geven we antwoord op de twee onderzoeksvragen die in dit rapport centraal staan: (1) 'Welke initiatieven zijn er bij de regionale en lokale afhandeling van online criminaliteit?' en (2) 'Wat zijn de kenmerken van deze initiatieven?'. Hiertoe worden de bevindingen van de individuele parels in hoofdstuk 4 samengenomen. In de paragrafen 5.1 en 5.2 bespreken we de antwoorden op de hoofdvragen. De discussie volgt in paragraaf 5.3 en bestaat uit een reflectie op de gevonden resultaten en enkele aanbevelingen.

Voordat we de conclusies presenteren willen we enkele beperkingen van dit onderzoek bespreken zodat de lezer de conclusies kan lezen in het licht van die beperkingen. Een eerste beperking is de werving en selectie van initiatieven. Ondanks de uitvragen naar dergelijke projecten – bij het PIAC, teamleiders van regionale cybercrimeteams en respondenten – is het goed mogelijk dat niet alle initiatieven bij de onderzoekers terecht zijn gekomen. Mogelijke verklaringen hiervoor zijn dat de benaderde personen niet op de hoogte zijn van alle initiatieven binnen de eenheid of dat personen geen tijd of behoefte hadden om initiatieven te melden. Daarnaast kan er een vertekening plaats hebben gevonden in de initiatieven die bij de onderzoekers zijn gemeld, doordat het grootste deel door teamleiders van regionale cybercrimeteams is gemeld. Ondanks dat deze personen ook zicht kunnen hebben op initiatieven op district- of basisteamniveau, kan het zijn dat kleinere parels niet bij de onderzoekers terecht zijn gekomen.

Een tweede beperking betreft de mogelijkheid dat er sociaal wenselijke antwoorden zijn gegeven door respondenten. Voor respondenten zou er namelijk een belang kunnen zijn om een beter beeld te schetsen van het initiatief dan daadwerkelijk het geval is, omdat veel van de initiatieven pilotprojecten zijn waarvan nog onduidelijk is of het initiatief zal blijven voortbestaan. Ondanks dat er tijdens de interviews kritisch is doorgevraagd en actief is gevraagd naar zaken die minder goed verlopen, kunnen sommige resultaten positiever voor zijn gesteld dan zij in de werkelijkheid zijn. Overigens doet dat niets af aan de inzichten die deze regionale en lokale initiatieven ons geven: het zijn duidelijk signalen van problemen waar de praktijk tegen aan loopt.

Ten slotte is er omtrent elk initiatief in de regel maar een persoon geïnterviewd. Door een gebrek aan validatie van de antwoorden is de betrouwbaarheid van sommige bevindingen van het onderzoek mogelijk lager. Dit probleem is deels ondervangen door beschikbare beleidsdocumenten te raadplegen ter validatie.



5.1 De initiatieven

Tijdens dit onderzoek zijn binnen de politie-eenheden 37 initiatieven geïdentificeerd op het gebied van online criminaliteit. Van deze initiatieven voldeden er 19 aan de inclusiecriteria van het onderzoek (zie hiervoor paragraaf 1.2). In tabel 1 is een overzicht weergegeven van de 19 initiatieven, verdeeld over de eenheden en de fases van het politiewerk waarop de parel betrekking heeft. De figuur hierboven laat in een schematisch overzicht zien op welk gedeelte van het politiewerk de initiatieven zich richten.

Wanneer wordt gekeken naar de inhoud van de initiatieven, dan blijkt dat er verschillende activiteiten worden uitgevoerd om de beoogde doelen te bereiken. Ten eerste zijn er de initiatieven die zich richten op preventie. De initiatieven proberen criminaliteit te voorkomen door middel van een externe samenwerking en de inzet van een escaperoom-bus. Zo wordt er in Limburg samengewerkt met de Risk Factory zodat burgers scenario's doorlopen op het gebied van online veiligheid en probeert het initiatief Bl@ckmail sextortion te voorkomen met behulp van een mobiele escaperoom waarin het gesprek wordt aangegaan met jongeren. Ten tweede is er een initiatief dat zich uitsluitend richt op de opsporing van online criminaliteit. De oprichting van districtelijke cybercrimeteams binnen de districtsrecherche moet daaraan bijdragen. Ten derde proberen de kennis en kunde initiatieven kennis bij te brengen bij politiemedewerkers door middel van escaperooms, fictieve casussen, CTF-challenges, workshops, klassikale lessen en de inzet van een digitale trainingsstraat. De kennis die wordt overgedragen betreft alle onderdelen van het politieproces: het opnemen van aangiften, case screening, digitale opsporingsmogelijkheden, virtuele doorzoekingen, open bronnen onderzoek en het indienen van vorderingen bij bedrijven. Tot slot zijn er initiatieven die zich direct richten op meerdere fasen van het politiewerk tegelijkertijd. Deze initiatieven proberen hierop in te spelen door bijvoorbeeld speciale teams op te richten die zelf operationeel actief zijn of ondersteuning bieden aan operationele teams. De oprichting en wijze waarop de teams zijn vormgegeven laten zien dat er binnen de verschillende eenheden behoefte is aan (samenwerking tussen) verschillende expertises. Ook wordt er van buiten de politieorganisatie expertise ingevoegd door bijvoorbeeld de inzet van cybervrijwilligers en IT-coaches. Andere initiatieven die zich op meerdere fasen richten proberen door externe samenwerking bij te dragen aan geformuleerde doelen. Zo zijn er in Zeeland-West-Brabant in een 'cyberdriehoek' structurele overleggen en zijn er overleggen tussen vitale partnerorganisaties in Breda om informatie en kennis met elkaar te delen.

Tot slot blijkt dat bijna alle initiatieven (n=14) worden uitgevoerd op eenheidsniveau, wat betekent dat men met het initiatief de gehele eenheid beoogt te bereiken. De initiatieven richten zich veelal op basisteams (n=7), maar ook op districtsrecherches (n=5) of op meerdere niveaus tegelijkertijd (n=4).

5.2 Kenmerken van de initiatieven

Aanleidingen

Om zicht te krijgen op de behoeften binnen de politie-eenheden wat betreft de aanpak van online criminaliteit, is gekeken naar de aanleiding voor het opzetten van de initiatieven. De meest genoemde beweegredenen zijn enerzijds opdrachten vanuit politiebeleid (n=10) en anderzijds de behoefte aan meer kennis en kunde van politiemedewerkers (n=10). Opdrachten vanuit politiebeleid bestaan uit strategische doelstellingen die zijn vastgelegd in beleidsstukken. Voorbeelden zijn kwantitatieve doelstellingen omtrent het aantal cybercrime verdachten en afspraken dat eenheden zich op een bepaald fenomeen richten. De initiatieven zijn daarmee een instrument om aan bestaande doelstellingen of strategieën binnen de politie bij te dragen. De andere veelgenoemde aanleiding is dat het in de praktijk blijkt dat de kennis en kunde van politiemedewerkers rondom het thema online criminaliteit en digitalisering onvoldoende is en dat het initiatief als doel heeft deze kennis en kunde te vergroten. Overige factoren die mede leiden tot de opzet van een initiatief zijn de toename van online criminaliteit, de behoefte aan 'learning on the job' onder politiemedewerkers en soortgelijke initiatieven in andere politie-eenheden.

Doelen en typen online criminaliteit

Er worden verschillende doelstellingen gekoppeld aan de projecten, waarvan sommige projecten ook meerdere doelen tegelijk proberen te bewerkstelligen. De doelen clusteren zich voornamelijk rondom drie thema's: (1) bewustwording verhogen en de kennis en vaardigheden vergroten van politiemedewerkers, (2) meer opsporingsonderzoeken kunnen uitvoeren en (3) de preventie van online criminaliteit verbeteren. Naast de drie genoemde doelstellingen is ook een uniforme werkwijze rondom de bestrijding van (specifieke vormen van) online criminaliteit een doel van enkele projecten. Hiermee hangen doelen samen als het vormgeven van digitalisering en het toekomstbestendig maken van de politieorganisatie. Andere doelen zijn kennis opdoen, maatwerk creëren in de afdoening en het lokale bestuur meer betrekken bij de aanpak van online criminaliteit.

Enkele projecten richten zich op specifieke vormen van online criminaliteit (n=4). Zo zijn er projecten op het gebied van sextortion, VIN-fraude en geldezels. Een verklaring voor deze specifieke focus op online criminaliteitsvormen kan worden gevonden in de verantwoordelijkheid van

politie-eenheden voor specifieke fenomenen vanuit het Voorstel Intensivering Aanpak Cyber (Politie, 2018b). Verder richten verschillende projecten zich op cybercrime (n=6) en is er één project dat zich alleen op gedigitaliseerde criminaliteit richt. Andere projecten richten zich op zowel cybercrime als gedigitaliseerde criminaliteit (n=4) of meer indirect op (een vorm van) online criminaliteit (n=3). Indirecte projecten betreffen vooral de projecten waar politiemedewerkers kennis en vaardigheden wordt bijgebracht. Daarbij richt men zich vooral op digitale opsporingsvaardigheden, wat betekent dat de kennis ook voor traditionele criminaliteitsvormen kan worden gebruikt.

Inhoudelijke activiteiten van geïdentificeerde projecten

Inhoudelijk gaat het bij vijf initiatieven om een training die gegeven wordt aan politie personeel. Voorbeelden zijn een workshop, een escaperoom en een cybercrisisoefening. In zes andere initiatieven gaat het om een interne verandering van de organisatiestructuur. Zo zijn er flex-teams en multidisciplinaire teams opgezet en aanspreekpunten aangewezen. In drie andere gevallen gaat het om een samenwerking met externe partijen, zoals de Risk Factory of in het geval van de cyber driehoek overleggen. Tot slot zijn er drie initiatieven die niet in deze categorieën onder te verdelen zijn, zoals het opstellen van een aangiftesysteem.

Samenwerking met stakeholders

Rondom de geïdentificeerde projecten vindt veel samenwerking plaats, met zowel interne als externe partners. Interne samenwerking vindt plaats met afdelingen, teams en personen met verschillende expertisen uit verschillende lagen van de politieorganisatie. Zo wordt er samengewerkt met basisteams, districtsrecherches en regionale cybercrimeteams, maar spelen ook communicatie afdelingen, intake en service en de opsporingsacademie een rol. Het blijkt dat de meeste projecten (12 van de 19) ook samenwerken met externe organisaties. Naast de bekende strafrechtketenpartners zoals het OM en reclassering wordt er samengewerkt met commerciële organisaties, non-profit organisaties en kennisinstellingen. De samenwerking met interne en externe partners is vaak niet formeel vastgelegd, maar bestaat uit informele afspraken. Soms in de vorm van mondelinge afspraken en soms via afspraken per e-mail. Bij enkele initiatieven is er wel een formele samenwerking met bijbehorende afspraken De duur van de samenwerking is bij meer dan de helft van de initiatieven niet vastgelegd of is volgens respondenten voor onbepaalde tijd.

Bevorderende en belemmerende factoren

Respondenten geven bij de helft van de initiatieven aan dat betrokkenen enthousiast, gemotiveerd en energiek zijn. Het gaat dan om enthousiasme onder mensen die (zowel intern als extern) een rol vervullen bij de uitvoering van het initiatief, maar ook om enthousiaste deelnemers van bijvoorbeeld trainingen en workshops. Er lijkt een verband met het hebben van een gezamenlijke doelstelling (n=4). Dit leidt weer tot (een proactieve) samenwerking met partners (n=4). Een andere factor die wordt genoemd is het commitment vanuit de politieorganisatie en de ruimte die projectleiders krijgen om te experimenteren en te leren (n=3). Ook wordt volgens de respondenten de hulp die door de initiatieven wordt geboden – bijvoorbeeld in de vorm van IT-coaches of leden van het cyber support team – goed ontvangen door politiemedewerkers (n=3). Ten slotte worden verschillende positieve effecten gehoord in relatie tot de initiatieven. Zo is volgens respondenten bij het VIN-fraude project de kwaliteit van de aangifte hoger geworden en is er meer kennis over het fenomeen, is er door het Digitaal District een plek gecreëerd waardoor meer initiatieven mogelijk zijn en leggen deelnemers tijdens de KOR3NWOLF casus elkaar spontaan dingen uit.

Belemmerende factoren zijn er ook. Wat betreft een minder goed verloop van de initiatieven valt op dat dit voor verschillende projecten de andere kant van dezelfde munt lijkt te zijn. Er zijn namelijk ook juist afdelingen of personen binnen de politieorganisatie die minder ontvankelijk en conservatiever zijn in relatie tot digitalisering en online criminaliteit (n=5). Zo wordt opgemerkt door respondenten dat enkele afdelingen nog afstand behouden tot digitale thema's en dat sommige medewerkers tijdens trainingen een minder open houding hebben ten aanzien van het thema en daardoor passiever zijn. In relatie tot deze bevinding wordt opgemerkt dat de 'klassieke agenda' (m.a.w. traditionele criminaliteit) uiteindelijk vaak voorrang krijgt op de problematiek rondom online criminaliteit (n=2). Andere belemmeringen zijn dat, ondanks dat men bij enkele initiatieven tevreden is over het commitment vanuit de politieorganisatie, er ook respondenten zijn die aangeven dat er te weinig capaciteit beschikbaar is om het project naar volledigheid uit te kunnen voeren (n=4). Als laatste blijkt dat er soms bij trainingen een betere afstemming nodig is op het niveau van medewerkers (n=2) en dat er behoefte is aan beter verwachtingsmanagement richting betrokken politiemedewerkers rondom de initiatieven (n=2).

Het behalen van doelstellingen

Een groot deel van de initiatieven (n=14) blijkt een vorm van evaluatie te hebben ingebouwd. Het gaat dan vooral om evaluaties die de politie zelf uitvoert. Zo worden er evaluatiegesprekken gevoerd en evaluatieformulieren uitgedeeld aan deelnemers en betrokkenen, zodat feedback wordt verkregen en aanpassingen mogelijk zijn. In de eenheid Zeeland-West-Brabant wordt verwezen naar een monitor cybercrime, die op kwalitatieve en kwantitatieve wijze bijhoudt welke resultaten er binnen de eenheid worden geboekt op het gebied van online criminaliteit (ook in relatie tot de initiatieven).

Er kunnen enkele kritische kanttekeningen worden geplaats bij de wijze waarop de initiatieven worden geëvalueerd. Zo wordt vaak maar een deel van het initiatief geëvalueerd, krijgen sommige nulmetingen geen vervolg en betreffen de evaluaties doorgaans geen (wetenschappelijke) effect-evaluaties. Een aantal initiatieven (n=4) heeft een evaluatie laten uitvoeren door een externe organisatie. Voorbeelden van deze organisaties zijn onderzoeksinstellingen, een consultancy bureau en een universiteit. Ten slotte blijkt dat een deel van de initiatieven (n=6) niet (stelselmatig) bijhoudt of de doelstellingen worden behaald. Verklaringen die hiervoor worden gegeven zijn bijvoorbeeld dat er geen capaciteit voor is of dat men in de opstartfase zit van het project.

Of de doelen daadwerkelijk worden behaald is voor het grootste deel van de initiatieven onduidelijk of onbekend (n=13). Wel worden er verschillende praktijksignalen benoemd die een indicatie geven dat doelen (gedeeltelijk) worden behaald. Zo worden er voorbeelden gegeven dat medewerkers meer contact zoeken met andere afdelingen om vragen te stellen of kennis op te halen en zijn er cijfers dat (meer) opsporingsonderzoeken worden afgerond.

Toepasbaarheid en verspreiding in andere eenheden

Bijna alle parels in het onderzoek zijn uitgevoerd op eenheidsniveau, met uitzondering van enkele projecten die in een specifiek district of basisteam hebben plaatsgevonden. Aangezien de politieorganisatiestructuur grotendeels vergelijkbaar is in de verschillende politie-eenheden, zouden veel van de initiatieven in principe ook in andere politie-eenheden kunnen worden toegepast. Een enkel initiatief is niet toepasbaar in alle politie-eenheden. Zo kan de samenwerking met de Risk Factory zoals in Limburg alleen plaatsvinden in eenheden waar de Risk Factory bestaat.

Voor de praktische toepasbaarheid van de initiatieven is het voornamelijk van belang dat er capaciteit wordt vrijgemaakt. Vooral voor de organisatorische projecten, waarbij speciale teams worden opgericht, is (gelabelde) capaciteit nodig. Dit vereist ook goedkeuring van personen die beleid maken en beslissen over personele inzet. “Kennis en kunde projecten” vereisen doorgaans minder capaciteit, maar ook hier zijn medewerkers nodig voor de coördinatie en kennisoverdracht. Naast capaciteit zijn ook (technische) middelen nodig voor enkele projecten. Wel zouden casussen en trainingsmaterialen in de meeste gevallen kunnen worden overgedragen vanuit de politie-eenheden waar het initiatief al draait. Naast de afhankelijkheid van capaciteit, middelen en goedkeuring van beleidsbepalers is ook de attitude van politiemedewerkers van belang voor de implementatie in andere eenheden. Dit blijkt uit de eerder genoemde signalen dat sommige afdelingen of politiemedewerkers minder open staan of weerstand vertonen in relatie tot online criminaliteit en de digitale aspecten van het hedendaagse politiewerk.

Tot slot blijkt dat bij het overgrote deel van de huidige initiatieven onbekend is of de doelen worden behaald. Ondanks dat er positieve geluiden en soms duidelijke signalen zijn dat de initiatieven tot verbetering leiden in het politieproces is het van belang dat er meer zicht komt op de werkzaamheid van de initiatieven. Goede voorbeelden zijn de inzet van externe organisaties voor evaluatieonderzoek en het verrichten van voor- en nametingen bij trainingen. Aantoonbare werkzaamheid van de initiatieven is belangrijk om de initiatieven verder uit te kunnen rollen naar andere eenheden, zeker ook om de benodigde capaciteit, middelen en commitment onder politiemedewerkers te verkrijgen.

5.3 Discussie

Initiatieven richten zich vooral op kennis en vaardigheden van politiemedewerkers

Ten eerste valt het op dat er relatief veel initiatieven geïdentificeerd zijn die zich richten op bewustwording en ontwikkeling van vaardigheden en kennis bij politiemedewerkers. In principe zijn deze initiatieven natuurlijk een goede ontwikkeling. Uit dit onderzoek blijkt immers dat er behoefte is vanuit politiemedewerkers aan deze kennis voor de uitoefening van het werk. Daarnaast pleit eerder onderzoek voor kennisverbetering met betrekking tot verschillende onderdelen van het politiewerk in de aanpak van online criminaliteit (Leukfeldt et al., 2012; Huisman et al., 2016; Boekhoorn, 2019; Jansen et al., 2020) en zijn dergelijke doelstellingen ook opgenomen in strategische en beleidsmatige doelstellingen van de politieorganisatie. Maar blijkbaar is de behoefte aan meer kennis en kunde in de praktijk nog steeds erg groot. Tijdens de discussiebijeenkomst met experts, concluderen de experts dat het gebrek – en de behoefte - aan kennis en kunde op het gebied van online criminaliteit al geruime tijd aanwezig is in de politieorganisatie. De politieorganisatie is hierin volgens de deelnemers echter niet alleen. Ook andere opsporingsdiensten zoals de Koninklijke Marechaussee ervaren een gebrek aan kennis en kunde op het gebied van digitalisering. Gezien de snelle ontwikkelingen op het gebied van online criminaliteit verdient het volgens experts dan ook de aanbeveling om verder te investeren op kennis en kunde omtrent online criminaliteit en vooral ook om deze kennis up-to-date te houden door continue bijscholing.

Gezien de grote behoefte aan kennis en trainingen in verschillende afdelingen, lagen en eenheden van de politieorganisatie en eerdere rapporten waarin deze conclusie is getrokken, verdient het dan ook de aanbeveling om de kennisverbetering landelijk te organiseren. De Politieacademie zou hierin een rol kunnen spelen, door basiskennis over online criminaliteit en digitalisering niet alleen in specialistische opleidingen aan te bieden, maar ook in basisopleidingen.

Een tweede aspect dat opvalt is dat initiatieven zich ook richten op verbeteringen binnen het proces van opsporing. Voorbeelden zijn de ‘aanpak geldezels’ en het ‘project VIN-fraude’. Deze initiatieven zijn echter niet geheel nieuw. Het LMIO bestaat bijvoorbeeld al enkele jaren en ook het ECTF heeft een soortgelijke functie. Wel is duidelijk dat de impact van digitalisering op criminaliteit groot is. De politie krijgt steeds meer te maken met nieuwe vormen van gedigitaliseerde criminaliteit waarbij aangiftes uit het hele land komen. Het verdient dan ook de aanbeveling om de aanpak of werkvoorbereiding van dit soort nieuwe fenomenen landelijk aan te sturen, zodat kennis op een centraal punt kan worden ontsloten en lokale opsporingsteams beter in stelling kunnen worden gebracht om de zaken op te pakken. Waar mogelijk door samenwerking met externe partners, aangezien burgers vaak melding doen bij deze organisaties (Van de Weijer et al., 2019) en zij over een goede informatiepositie beschikken. Uiteraard is dan ook beleid nodig met betrekking tot het daadwerkelijk oppakken van zaken die centraal voorbereid zijn en vervolgens in diverse eenheden worden uitgezet.

Verandering in de opsporing

Met de toename van online criminaliteit – en dus ook het dagelijkse werkaanbod van politiemedewerkers – kunnen de in dit onderzoek geïdentificeerde initiatieven in de context van een bredere transitie worden geplaatst. Eerder onderzoek naar verandering binnen de politieorganisatie laat zien dat de politie in haar structuur en cultuur normaliter vaak ‘opmerkelijk resistent’ is tegen dergelijke veranderingen (Landman et al., 2020). De bevindingen van onderha-

vig onderzoek hieromtrent zijn tweeledig. Enerzijds wordt door initiatiefnemers opgemerkt dat er vaak enthousiast wordt gereageerd op de initiatieven door deelnemers (vaak politiemedewerkers) en betrokkenen bij de uitvoering (politiemedewerkers of externe organisaties). Ook leidinggevenden geven ruimte om aan de slag te gaan met de initiatieven. Anderzijds wordt echter ook gezien dat er verschillende onderdelen en medewerkers weerstand vertonen ten opzichte van (projecten op het gebied van) online criminaliteit en digitalisering.

In het recente onderzoek van Landman et al. (2020) wordt benadrukt dat het van belang is om weerstand tegen verandering onder politiemedewerkers te begrijpen in de context van de politieorganisatie. Factoren omtrent deze context zijn bijvoorbeeld de 'blauwe identiteit', de werking van het strafrechtsysteem en de organisatiestructuur binnen de politie. De invloed van innovatieve projecten en trainingen kan worden geremd of teniet gedaan worden door het bredere institutionele en organisatorische systeem waarin politiemedewerkers werken. Verandering dient volgens de auteurs dan ook plaats te vinden middels een strategie van twee sporen: enerzijds door lokale leeromgevingen te organiseren en anderzijds door aanpassingen te verrichten in het systeem en de organisatie. De digikamers in Zeeland-West-Brabant illustreert goed de werking van deze strategie: begonnen in een basisteam, uitgegroeid tot een organisatorische verandering binnen de eenheid en tegelijkertijd ook een omgeving die op lokaal niveau weer innovatieve projecten stimuleert. Ook het CyberHQ en Digitaal District zijn voorbeelden waarbij aanpassingen in de organisatiestructuur kunnen leiden tot een omgeving waar meer (verandering) mogelijk is. In deze teams ontstaat namelijk ruimte voor innovatieve projecten die hun uitwerking hebben op de rest van de eenheid.

In het kader van verdere implementatie van de geïdentificeerde projecten geven experts tijdens de discussiebijeenkomst aan dat er niet zozeer hooggespannen verwachtingen hoeven te zijn over een landelijke implementatie van projecten. Lokale of regionale behoeften en projecten hoeven namelijk niet per definitie voor de hele politie te gelden, aangezien er geen garantie is dat op andere plekken hetzelfde enthousiasme of dezelfde resultaten worden behaald rondom een project. De winst van dergelijke initiatieven zou er volgens experts vooral in moeten zitten dat men op lokaal of regionaal niveau bezig is met digitalisering en online criminaliteit. Lokale en regionale initiatieven dienen dan ook vooral een functie te hebben in de verspreiding van kennis en verdere enthousiasmering op het thema. Het huidige rapport kan in die zin functioneren als inspiratie voor andere eenheden en verdere verspreiding stimuleren.

Weinig bekend over de werking van initiatieven

Dit rapport laat zien dat er weinig bekend is over de werking van de initiatieven. Er zijn weliswaar positieve geluiden en voorbeelden, maar concrete effectevaluaties blijven grotendeels uit. Dit is enerzijds begrijpelijk, aangezien de politieorganisatie andere doelstellingen en prioriteiten heeft die met een beperkte capaciteit moeten worden aangevlogen. Anderzijds zorgt de beperkte capaciteit er ook voor dat de middelen op een effectieve wijze ingezet dienen te worden. Het verdient dan ook de aanbeveling om meetbare doelen te formuleren en vervolgens effectevaluaties of mimimaal plan- en procesevaluaties uit te voeren. Sommige doelstellingen kan de politie wellicht eenvoudig zelf toetsen, andere doelstellingen kunnen worden onderzocht door andere organisaties zoals sommige van de initiatieven al doen. Experts benadrukken tijdens de discussiebijeenkomst dat het meten van effecten vooral dicht bij de politie dient te staan, door kleine en laagdrempelige effecten te meten. Voorbeelden zijn een kennismeting (voor- en nameting), het bijhouden van activiteiten of het bijhouden van het aantal zaken dat wordt opgepakt op het gebied van (een vorm van) online criminaliteit. Een andere aanbeveling vanuit de experts is om initiatiefnemers te ondersteunen bij de evaluatie van hun project. Dit kan onder andere door het opstellen van een handleiding waarin uitleg staat over hoe projecten op een juiste wijze kunnen worden geëvalueerd.

Literatuurlijst

- Beerthuizen, M. G. C. J., Sipma, T., & van der Laan, A. M. (2020). *Aard en omvang van dader-en slachtofferschap van cyber-en gedigitaliseerde criminaliteit in Nederland.* Den Haag: WODC.
- Boekhoorn, P. (2019). De aanpak van cybercrime door regionale eenheden van de politie. Van intake van cybercrime naar opsporing en vervolging. *Politiekunde 102.* Den Haag: Politie & Wetenschap.
- Boes, S., & Leukfeldt, E. R. (2017). Fighting cybercrime: A joint effort. In *Cyber-Physical Security* (pp. 185-203). Springer, Cham.
- CCV (2019). *Digitale wijkagent troef in strijd cybercrime.* Geraadpleegd van https://hetccv.nl/onderwerpen/cybercrime/praktijkvoorbeelden/digitale-wijkagent-troef-in-strijd-cybercrime/
- Centraal Bureau voor de Statistiek (2020). Veiligheidsmonitor 2019. Den Haag: CBS.
- Jansen, J., Van Valkengoed, T., Veenstra, S. & Stol, W. (2020). *Level-up! Kennis voor politiewerk in een digitale samenleving.* NHL Hogeschool, Lectoraat Cybersafety.
- Leukfeldt, E.R. (2016). *Cybercriminal Networks : Origin , Growth and Criminal Capabilities.* Den Haag: Eleven International Publishers.
- Leukfeldt, Kentgens, Prins & Stol (2015). *Alledaags politiewerk in een gedigitaliseerde wereld. Handreiking voor de intake van delicten met een digitale component.* Leeuwarden: NHL Hogeschool, Lectoraat Cybersafety.
- Leukfeldt, R., Veenstra, S., Domenie & M., Stol, W. (2012). *De strafrechtketen in een gedigitaliseerde samenleving. Een onderzoek naar de strafrechtelijke afhandeling van cybercrime.* Den Haag: Sdu Uitgevers.
- McGuire, M., & Dowling, S. (2013a). *Chapter 1: Cyber-dependent crimes.* London: Home Office UK.
- McGuire, M., & Dowling, S. (2013b). *Chapter 2: Cyber-enabled crimes.* London: Home Office UK.
- Nu.nl. (2017) Politie krijgt tien nieuwe teams om cybercriminaliteit te bestrijden. Geraadpleegd van https://www.nu.nl/binnenland/4380363/politie-krijgt-tien-nieuwe-teams-cybercriminaliteit-bestrijden.html
- Politie (2017). *Jaarverantwoording politie. Jaarverantwoording 2017.* Geraadpleegd van https://www.rijksoverheid.nl/documenten/jaarverslagen/2018/05/16/nationale-politie-2017
- Politie (2018a). J*aarverantwoording Midden in de samenleving. Jaarverantwoording 2018.* Geraadpleegd van https://www.rijksoverheid.nl/documenten/jaarverslagen/2019/05/15/nationale-politie-2018
- Politie (2018b). *Voorstel intensivering aanpak cybercrime RA-gelden en Miljoenennota* [politie intern].
- Politie (2021). *150 arrestaties en inbeslagname van € 26 miljoen euro bij politieactie tegen drugsverkoop op het dark web.* Geraadpleegd van https://www.politie.nl/nieuws/2021/oktober/26/11-150-arrestaties-en-inbeslagname-van-%E2%82%AC-26-miljoen-euro-bij-politieactie-tegen-drugsverkoop-op-het-darkweb.html
- Politie. (z.d.). *Cybercrime*. Geraadpleegd van https://www.politie.nl/themas/cybercrime.html
- Politie. (z.d.). *Over de politie. Organisatie: één politie, elf eenheden.* Geraadpleegd van https://www.politie.nl/over-de-politie/een-politie-elf-eenheden.html
- Roks, R. A., Leukfeldt, E. R., & Densley, J. A. (2020). The digitized opportunity structure of street offending. *British Journal of Criminology*, 61(4), 926-945.
- Struiksma, N., de Vey Mestdagh, C. N. J. V., & Winter, H. B. (2012). *De organisatie van de opsporing van cybercrime door de Nederlands politie.* Apeldoorn: Politie & Wetenschap.
- Van Bree, R., Nijeboer, R., Klerkx, G., Witteveen, L. & Monsma, E. *Cybercrime strategie 2020. Voor een veiliger Nederland, ook in het digitale domein.* Geraadpleegd van https://www.regioburgemeesters.nl/save430/

Bijlage 1:
Alfabetisch overzicht van geïncludeerde initiatieven

Naam initiatief	Eenheid
Aanpak geldezels	Rotterdam
Bl@ckmail	Amsterdam
Cyber HQ	Zeeland-West-Brabant
Cyber support team	Amsterdam
Cybercrisisoefening met BT	Noord-Nederland
Cyberdriehoek	Den Haag
Cyberspecials	Amsterdam
Dagelijkse Cyberquery	Limburg
Digikamers	Zeeland-West-Brabant
Digitaal District	Midden-Nederland
Digitaal flexteam IJsselland	Oost-Nederland
Digitaal weerbaar Breda	Zeeland-West-Brabant
Digitale vaardigheden Friesland	Noord-Nederland
Districtelijke cybercrimeteams	Zeeland-West-Brabant
IT-coaches district Twente	Oost-Nederland
KOR3NWOLF	Limburg
Project Vriend in Nood-fraude	Oost-Nederland
Samenwerking Risk Factory	Limburg
Workshop cybercrime	Amsterdam

Bijlage 2:
Interviewprotocol

Algemeen

- Wat is uw naam en leeftijd?
- Noteer: geslacht
- Bij welke organisatie bent u werkzaam? (niveau, eenheid, afdeling)
- Wat is, in uw organisatie, uw functie en met welke werkzaamheden houdt u zich bezig?
- Op welke wijze bent u betrokken bij project X?

Beschrijving project X

- Wat is project X?
- Wat zijn de doelen van project X? (preventie, verstoring, opsporing)
  - Zijn deze doelen schriftelijk vastgelegd?
- Wat is de doelgroep van project X? Richt het project zich op specifieke vormen van online criminaliteit? Zo ja, welke?
  - Is deze doelgroep schriftelijk vastgelegd?
  - Worden er in de toekomst wellicht nog ander doelgroepen/vormen van online criminaliteit voor project X toegevoegd?
- Op welk niveau vindt het project plaats? (welke eenheid, regionaal of lokaal)
- Hoe en waarom is project X ontstaan?
  - Wie heeft project X bedacht en ontwikkeld?
  - Wanneer is het ontwikkeld en sinds wanneer wordt het nu in de praktijk uitgevoerd?
- Welke organisaties en/of andere afdelingen zijn betrokken (geweest) bij het opzetten van project X?

Onderbouwing project X

- Waarom verwachten jullie dat project X werkt, dat project X zijn doelen bereikt?
- Wordt er bijgehouden of en in welke mate project X de beoogde doelen bereikt? Zo ja, op welke wijze en door wie? Zo nee, waarom niet?
- Worden de beoogde doelen behaald?
- Is project X gefundeerd op bestaande, wetenschappelijke of praktijkgerichte theorieën? Zo ja, welke?
- Is project X verder nog gefundeerd op eventuele professionele aannames? Zo ja, welke en hoe zijn deze tot stand gekomen?
- Wat zou er naar uw eigen mening verder onderbouwd kunnen worden aan project X?

Samenwerking

- Hoeveel mensen zijn betrokken bij project X? Wie zijn dat? (intern of extern)
- Wat is de reden dat deze samenwerkingspartners betrokken zijn?
- Hoe ziet de samenwerking met de verschillende partners eruit?
- Welke afspraken zijn met de samenwerkingspartners gemaakt?
  - Zijn al deze afspraken schriftelijk vastgelegd?
- Wat is de duur van de samenwerking tussen de samenwerkingspartners?
  - Is dit schriftelijk vastgelegd?
- Hoe ervaart u de kwaliteit van de samenwerking tussen de samenwerkingspartners?
  - Wat verklaart volgens u de kwaliteit van deze samenwerking?
- Wat zou er volgens uzelf aan de samenwerking tussen de samenwerkingspartners verbeterd kunnen worden?

Implementatie project/project in de praktijk

- Is project X nu vormgegeven zoals beoogd?
- In hoeverre wordt project X tussendoor geëvalueerd en aangepast? Wat geeft daartoe eventueel de aanleiding?
- Wat gaat goed en wat minder goed?
- Is het project geïmplementeerd op de juiste schaal? Moet dit groter of kleiner?
- Is het project geïmplementeerd met de juiste intensiteit? Moet dit groter of kleiner?
- Wat is het geplande en gewenste toekomstsplan voor project X?
  - In hoeverre is het project volgens u toepasbaar binnen andere eenheden?

Afsluiting

- Zijn er beleidsdocumenten beschikbaar omtrent project X?
- Wilt u verder nog iets toevoegen?

Bijlage 3:
Expertbijeenkomst

De expertbijeenkomst heeft plaatsgevonden met de volgende deelnemers (en de onderzoekers):

- Mariëlle Den Hengst, Senior onderzoeker bij het Nederlands Studiecentrum voor Criminaliteit en Rechtshandhaving.
- Wouter Landman, Onderzoeker en Adviseur bij Bureau Landman.
- Richard Nijeboer, Senior Liaison Cybercrime en Digitaal Opsporen bij Politie Nederland.
- Wouter Stol, Lector Cybersafety bij NHL Stenden Hogeschool en de Politieacademie.
- Guus van Kessel, Brigade Recherche bij de Koninklijke Marechaussee.
- Adriaan Rottenberg, Programmamedewerker Politie & Wetenschap bij Politie Nederland.