Van : Programma Digitale Veiligheid en Cybercrime
Aan : Bestuurlijke werkgroep Digitale veiligheid en cybercrime
Datum : 10 maart 2025
Onderwerp : Jaarplan 2025
Status : Definief

MEMO

Introductie: Waarom dit jaarplan?
Het programma Digitale Veiligheid en Cybercrime heeft een looptijd van vier jaar en is gestart in april 2023. Dat betekent dat we begin 2025 halverwege de looptijd van het programma zijn. Om die reden zijn in september en oktober 2024 met alle leden van de bestuurlijke werkgroep Digitale Veiligheid en Cybercrime (tussen)evaluatiegesprekken gevoerd over (de voortgang van) het programma Digitale Veiligheid en Cybercrime. Het doel van de gesprekken is om inzicht te krijgen in wat goed gaat, maar ook waar we de resterende tijd van de veiligheidsstrategie op moeten versnellen om het beoogde resultaat te behalen.

Samenvattend (zie bijlage voor het volledige verslag van de reflectiegesprekken) kwamen de volgende evaluatiepunten naar voren:

- Actiestand wordt gewaardeerd, maar wordt het scherpe gesprek voldoende gevoerd?
- Informatiepositie van het lokale bestuur moet beter.
- Vakmanschap vergroten, ook bij professionals buiten het veiligheidsdomein
- Meer communiceren
- Urgentie voor het probleem bij bestuurders blijft (soms) achter
- Wat is de voortgang?

Deze evaluatie is meegenomen bij het formuleren van de acties die in 2025 uitgezet gaan worden. Deze acties worden omschreven in dit jaarplan voor 2025.

Wat is er aan de hand?

We weten dat digitale onveiligheid zich moeilijk laat vertalen in eenduidige cijfers. De reden hiervoor is tweeledig. Ten eerste, is er een hoog dark number omdat er onder slachtoffers veel schaamte is om aangifte te doen. Per delictsvorm zijn er grote verschillen in aangiftebereidheid. Uit de veiligheidsmonitor 2023 blijkt dat gemiddeld 16,9% van de slachtoffers aangifte doet bij de politie. 40% meldt het elders (bank, fraudehelpdesk, etc). Ten tweede, zijn de politiecijfers lastig uit de systemen te halen. Registraties moeten (nog) handmatig worden gelabeld voordat deze als (een vorm van) online criminaliteit uit het systeem komen.

Desalniettemin zijn de cijfers over 2024 alarmerend. Aan- en verkoopfraude maakte in 2024 de meeste slachtoffers in Midden-Nederland: ruim 5,500 mensen deden hiervan aangifte, goed voor ruim 1,3 miljoen euro. Beleggingsfraude is het delict dat het meeste schade veroorzaakte in onze eenheid: het schadebedrag is 5,6 miljoen euro bij 284 slachtoffers. Bankhelpdeskfraude volgt daarna als delict met de meeste schade: voor 4,3 miljoen euro bij ruim 1,100 slachtoffers. Met alleen het noemen van deze drie delictsvormen, is er al meer dan 10 miljoen schade bij ruim 6,800 slachtoffers. Bijgevoegd het volledige overzicht van 2024.

Over het geheel bekeken, blijkt uit de politiecijfers dat er in een afname was van -42% op cybercrime. Deze sterke daling is (deels) te verklaren door een wijziging in de maatschappelijke klassen van de politie. In het huidige beeld worden cybercrime en online fraude apart geregistreerd, terwijl dat daarvoor nog niet gebeurde. Daarom moet zeer terughoudend de vergelijking worden gemaakt met die van voorgaande jaren. Fraude (zowel online als offline) daarentegen is gestegen met +9%, waarvan de gedigitaliseerde criminaliteit met +12% is toegenomen.

Kroonstraat 25 - Postbus 8300 - 3503 RH - Utrecht - 06 148 73 690 - secretariaat@rvs-mn.nl - www.veiligheidscoalitie.nl

Wat willen we bereiken?

De ambitie is (in het DIN, zie bijlage) als volgt geformuleerd: in Midden-Nederland gaan we slachtoffer- en daderschap van gedigitaliseerde criminaliteit en cybercrime voorkomen en daders hiervan pakken. Hiertoe hebben we kundige(re) professionals nodig voor wie integraal samenwerken tussen gemeenten, politie en OM vanzelfsprekend is. Data wordt gebruikt om capaciteit gericht in te zetten. De potentiële slachtoffers en daders worden weerbaar tegen gedigitaliseerde criminaliteit en cybercrime.

Wat gaan we daarvoor doen?

Bovenstaande ambitie is geoperationaliseerd in een vijftal operationele doelen. In dit document staat omschreven welke onderliggende acties in 2025 uitgevoerd gaan worden om te werken aan deze baten. Per baat wordt vervolgens aangegeven hoe er gemonitord gaat worden wat de resultaten zijn van de inspanningen die geleverd zijn/worden. Door te klikken op de actie komt u bij een verdere omschrijving van de actie.

Doel 1: Integraal sturen vindt plaats op basis van informatiebeeld.

Acties	:	Actie 1: Lokaal informatiebeeld aanleveren voor de lokale driehoeken. Actie 2: Toewerken naar een jaarlijks integraal strategisch informatiebeeld.
Monitoring/ Outputafspraak	:	Tweemaal per jaar lokaal informatiebeeld agenderen op basisteamdriehoek.

Doel 2: Slachtoffers hebben een hogere meldings- en aangiftebereidheid.

Acties	:	Actie 3: Lokaal en regionaal communiceren. Actie 4: Aangiftebereidheid verhogen.
Monitoring/ Outputafspraak	:	1. In 2027 is de aangifte- en meldingsbereidheid gestegen naar 20% ten opzichte van 2023 waarin dit 16,9% was. (Bron: Veiligheidsmonitor). 2. Ontwikkelen campagnemateriaal en beschikbaar stellen voor lokaal gebruik om de meldings- en aangiftebereidheid te vergroten.

Doel 3: Onze professionals zijn bewust en bekwaam t.a.v. DV&CC.

Acties	:	Actie 5: Actief de bestuurlijke aanpak tegen online criminaliteit inzetten in zaken die in Midden-Nederland gedraaid worden. Actie 6: Kennisuitwisseling organiseren en faciliteren. Actie 7: Uitvoeren en evalueren cyberoefendriehoek.
Monitoring/ Outputafspraak	:	Gemiddeld één kennisbijeenkomst per maand aan de hand van een leerlijn DVCC.

Doel 4: Effectiever (voorkomen en) aanpakken van daders.

Acties	:	Actie 5: Actief de bestuurlijke aanpak tegen online criminaliteit inzetten in zaken die in Midden-Nederland gedraaid worden. Actie 8: Verder versterken van de verbinding aanpak online criminaliteit met andere (veiligheids)thema's.
Monitoring/ Outputafspraak	:	1. In lijn met de landelijke veiligheidsagenda de minimale instroom van zowel cybercrime als gedigitaliseerde criminaliteit in 2025 met 10% verhogen t.o.v. de minimale instroomdoelstelling van 2024. 2. Minimaal één gecombineerde RIEC-casus per district. 3. Minimaal vijf bestuurlijke rapportages opgeleverd tegen personen die zich beziggehouden hebben met online criminaliteit of panden waarbinnen online criminaliteit heeft plaatsgevonden.

Doel 5: Onze inwoners weten beter hoe ze hun slachtofferkans kunnen verkleinen.

Acties	:	Actie 3: Lokaal en regionaal communiceren. Actie 9: Interventies uitrollen binnen (kleinere) gemeenten. Actie 10: Actiedag #echtnietvandaag organiseren. Actie 11: Huisbezoeken bij slachtoffers van online criminaliteit organiseren.
Monitoring/ Outputafspraak	:	In 2027 is het aantal slachtoffers in de regio gedaald naar 13% ten opzichte van 2023 waarin dit 15,6% was. (Bron: Veiligheidsmonitor).

Bijlage 1 Acties 2025

Actie 1: Lokaal informatiebeeld aanleveren voor de lokale driehoeken.	
Algemene info	Coördinatie: politie Status: lopend tot december 2025 In samenwerking met: bestuursondersteuning politie
Doel	Om te komen tot concrete (samenwerkings)afspraken op strategisch niveau, brengen we ieder kwartaal een informatieproduct online criminaliteit op de lokale driehoeken.
Output	- We organiseren een werksessie voor politie en gemeenten over het gebruik van het informatiebeeld dat aangeleverd gaat worden. - We beginnen in Q1 met een pilot in de driehoeken van de bestuurlijke werkgroepleden. Dit zal worden geëvalueerd door de bestuurlijke werkgroep, om vervolgens de lessons learned mee te nemen als we dit in de loop van 2025 breder uitzetten in de regio. - Aantal en soorten afspraken in basisteamdriehoeken worden bijgehouden, zodat we kunnen monitoren of het delen van de informatieproducten leidt tot het beoogde resultaat. Beoogd resultaat: eind 2025 heeft ieder basisteamdriehoek minimaal twee keer het informatiebeeld online criminaliteit besproken.

Actie 2: Toewerken naar een jaarlijks strategisch integraal informatieproduct online criminaliteit.	
Algemene info	Coördinatie: Bestuurlijke werkgroep DVCC Status: Op te starten Deze actie is onderdeel van 'project 2' Bureau RVS breed.
Doel	Om gerichter te kunnen sturen op lange termijn doelstellingen is een strategisch informatieproduct noodzakelijk. Daarom ontwikkelen we, samen met partners, een structureel informatieproduct welke jaarlijks uitkomt.
Output	- Inventariseren welke inhoud het strategisch informatieproduct online criminaliteit moet bevatten. - In kaart brengen welke partners er nodig zijn om de juiste informatie te leveren. - Afspraken maken mbt informatiedeling. Beoogd resultaat: eind 2025 zijn alle afspraken gemaakt en inhoud informatieproduct uitgedacht, zodat in 2026 het eerste integrale informatieproduct online criminaliteit opgeleverd kan worden.

Actie 3: Lokaal en regionaal communiceren.	
Algemene info	Coördinatie: bestuurlijke werkgroep DVCC Status: lopend tot december 2025
Doel	In 2025 wordt zowel lokaal, regionaal en binnen het netwerk online criminaliteit regelmatig onder de aandacht gebracht, met als doel het bewustzijn te vergroten en actie te stimuleren op verschillende niveaus.

Output	- Lokale integrale communicatie
	  ○ We organiseren een sessie voor communicatieadviseurs over digitale veiligheid (adhv tips Duwtje).
	  ○ Boodschappenhuis doorontwikkelen en implementeren
	  Beoogd resultaat: Elke gemeente plaatst minimaal één integrale communicatie-uiting over (de lokale kant van) online criminaliteit.
	- Regionale integrale communicatie. We gaan contact zoeken met regionale media om media-aandacht te vestigen op:
	  ○ Echtnietvandaag
	  ○ Cyberoefendriehoek

	○ Boodschap vanuit bestuurlijke werkgroep richting inwoners ○ Regionale campagne over PrioDigi (zie ook actie 3) Beoogd resultaat: Minimaal vier keer regionaal onder de aandacht brengen dat politie, OM en gemeenten samenwerken om (de impact van) slachtoffers- en daderschap te voorkomen en daders te pakken. - We houden ons netwerk actief betrokken door nieuwsbrieven / mailupdate: ○ 4 x mailupdate ○ 6 x externe nieuwsbrief Beoogd resultaat: Het netwerk regelmatig op de hoogte brengen van de stappen die gezet worden in de regio binnen het programma Digitale veiligheid en cybercrime.

Actie 4: Aangiftebereidheid verhogen.	
Algemene info	Coördinatie: bestuurlijke werkgroep DVCC Status: op te starten in april 2025 Wellicht in samenwerking met Burgernet
Doel	In 2025-2026 werken we aan het verhogen van de aangiftebereidheid voor online criminaliteit, omdat dit leidt tot een grotere pakkans en een betere informatiepositie van het lokale bestuur. In 2023 was de (gemiddelde) aangifte- en meldingsbereidheid voor online criminaliteit 16% (Veiligheidsmonitor). In de Veiligheidsmonitor 2027 willen we dat de aangifte- en meldingsbereidheid gestegen is naar 20%. Dit doen we door middel van (lokale en regionale) voorlichtings- en communicatiecampagnes.
Output	Output moet verder uitgewerkt worden zodra we aan de slag gaan met deze actie. Maar voor nu willen we ons richten op (globaal): - Regionale communicatiecampagne ontwikkelen waarin inwoners erop gewezen worden dat ze 112 kunnen bellen als ze slachtoffer zijn geworden van online criminaliteit (Prio Digi). - Communicatieadviseurs van gemeenten en politie informeren over het toepassen van strategieën om aangiftebereidheid te verghogen, zoals het benadrukken van het belang van aangifte en het erkennen van weerstand, zodat zij dit effectief kunnen verwerken in hun communicatie over online criminaliteit. - We signaleren verbeterpunten in het aangifteproces en geven adviezen om de gebruiksvriendelijkheid en toegankelijkheid ervan te vergroten.

Actie 5: Actief de bestuurlijke aanpak tegen online criminaliteit inzetten in zaken die in Midden-Nederland gedraaid worden.	
Algemene info	Coördinatie: politie Status: Lopend tot december 2025
Doel	Door bestuurlijke bevoegdheden in te zetten willen we online criminaliteit sneller en efficiënter aanpakken en verdere schade voorkomen.
Output	- Bewustwording vergroten bij politie bij cybercrimeteam en gedigitaliseerde criminaliteit tbv bestuurlijke maatregelen. - Presentatie geven aan bestuurlijke werkgroep over (on)mogelijkheden van bestuurlijke aanpak op online criminaliteit. Beoogd resultaat: minimaal vijf bestuurlijke rapportages schrijven tegen personen die zich beziggehouden hebben met online criminaliteit of panden waarbinnen online criminaliteit heeft plaatsgevonden.

Actie 6: Kennisuitwisseling organiseren en faciliteren.

Algemene info	Coördinatie: bestuurlijke werkgroep DVCC Status: doorlopend
Doel	In 2025 willen we de vakmanschap van collega's in de regio's verder vergroten, ook bij professionals buiten het veiligheidsdomein. Dit doen we door minimaal één bijeenkomst te organiseren.
Output	- Leerlijn online criminaliteit 2025 ontwikkelen en uitvoeren. - Gemiddeld 1 kennisbijeenkomst per maand organiseren. Onderstaande bijeenkomsten zijn al ingepland en/of worden georganiseerd: • Werksessie Informatiegestuurd werken (januari) • Netwerkbijeenkomst Veiligheidscoalitie (april) • Bijeenkomst Online jeugdcriminaliteit (maart) • Summer School (4-6 bijeenkomsten) (juli-augustus) Beoogd resultaat: Toegenomen kennis en vaardigheid van professionals in het herkennen en aanpakken van online criminaliteit, wat leidt tot een verbeterde samenwerking tussen partners en een snellere en effectievere respons. CISO-netwerk Midden-Nederland: - Een netwerk van betrokken CISO's die elkaar weten te vinden indien nodig. - Faciliteren van kennisdeling tussen CISO's in de regio. Beoogd resultaat: Twee fysieke regionale netwerkbijeenkomsten over een (voor de CISO's) relevant thema ter vergroting van de expertise.

Actie 7: Uitvoeren en evalueren cyberoefendriehoek. ⮌	
Algemene info	Coördinatie: bestuurlijke werkgroep DVCC Status: lopend tot april 2025
Doel	Regionaal voorbereiden op cybercrisis en opleveren evaluatie cyberoefendriehoek met daarin concrete handvatten voor het verder voorbereiden van de de driehoeken en het verbeteren van de samenwerking.
Output	- In samenwerking met werkgroep organiseren we de oefening. Beoogd resultaat: op 5 maart 2025 zal in het Van der Valk hotel in Amersfoort de oefening gehouden worden. 12 basisteamdriehoeken doen mee aan de oefening. Beoogd resultaat: Verslag met daarin suggesties voor verdere voorbereiding van de regio op een digitale verstoring.

Actie 8: Verder versterken van de verbinding aanpak online criminaliteit met andere (veiligheids)thema's. ⮌	
Algemene info	Coördinatie: bestuurlijke werkgroep GOC/RIEC en bestuurlijke werkgroep DVCC Status: doorlopend
Doel	Het verbeteren van de samenwerking tussen de betrokken organisaties op het gebied van online criminaliteit, ondermijning en online jeugdcriminaliteit door onderstaande initiatieven te organiseren in 2025, met als doel de effectiviteit en efficiëntie van de gezamenlijke aanpak te vergroten."
Output	Ondermijning: - Politiecollega's van het Cybercrimeteam en Team Digitale Criminaliteit in contact brengen met netwerk ondermijning. - Samenwerking met belastingdienst verkennen om online criminaliteit tegen te gaan. - Signalenkaart ontwikkelen voor ondermijnende digitale criminaliteit. Beoogd resultaat: Minimaal één RIEC-casus op online criminaliteit per district te draaien.

	Online jeugdcriminaliteit: - Leerlijn online jeugdcriminaliteit uitwerken voor 2025 en vertalen in kennisbijeenkomsten 2025. De eerste sessie hierover staat gepland in maart en gaat over samenwerken bij online jeugdcriminaliteit, handreiking 'online jeugdcriminaliteit' wordt gepresenteerd. - Onderzoek Fast Money opleveren aug 2025. - Verbinding leggen met het Zorg- en Veiligheidshuizen in Midden-Nederland op dit thema. Beoogd resultaat: naar aanleiding van gepresenteerde handreiking bij ten minste vijf gemeenten een sessie begeleiden met jeugdprofessionals over (het signaleren van) de problematiek in hun gemeente.

Actie 9: Interventies uitrollen binnen (kleinere) gemeenten.	
Algemene info	Coördinatie: bestuurlijke werkgroep DVCC Status: Doorlopend
Doel	Het versterken van de digitale weerbaarheid van inwoners in Midden-Nederland, met speciale aandacht voor jeugd, senioren en het MKB. We bieden hierbij ondersteuning aan kleinere gemeenten met beperkte capaciteit, zodat ook zij zich effectief kunnen inzetten voor een veilige digitale samenleving.
Output	- Echt-Nep campagne: bereik van minimaal 300 senioren in de regio via Echt-Nep bijeenkomsten. - Echt-Nep Train-The-Trainer: opleiding van gemeentelijke trainers, zodat een meerderheid van de gemeenten zelfstandig de presentatie kan inzetten. - Bakfiets "Dubbel beveiligd is dubbel zo veilig": de bakfiets wordt beschikbaar gesteld aan alle gemeenten in de regio voor tijdelijke inzet in lokale campagnes. - Re_bootcamp: organisatie van een experience voor jongeren tussen de 12 en 25 met interesse in IT, om cybercrime te voorkomen en IT talent te behouden.

Actie 10: Actiedag #echtnietvandaag organiseren.	
Algemene info	Coördinatie: bestuurlijke werkgroep DVCC Status: Lopend tot september 2025 In samenwerking met: Digitaal District, Platform Veilig Ondernemen Midden-Nederland, Straatwaarden
Doel	Doel is de weerbaarheid van inwoners vergroten en kenbaar maken dat hun lokale overheid (samen met lokale, private organisaties) zich hiervoor inzet. Deze actiedag geeft een boost aan het in kaart brengen van het lokale netwerk dat zich wil inzetten in het vergroten van de weerbaarheid.
Output	- Kerngroep vormen waarmee doelstellingen actiedag mee worden bepaald. - Districtelijke ambtelijke werkgroepen aanzetten om lokaal publiek-privaat samen te werken om acties te organiseren tijdens de actiedag. - Onderwijsinstellingen (en dus studenten) uitnodigen om deel te nemen en/of bij te dragen aan de actiedag. - Via regionale omroepen aandacht genereren voor het thema online criminaliteit. Beoogd resultaat: Een mooie actiedag met minimaal 100 acties waar publieke en private organisaties hun verantwoordelijkheid pakken om de weerbaarheid van inwoners in Midden-Nederland een boost te geven. Beoogd resultaat: Opleveren van een overzicht in de eenheid van actieve organisaties die zich in (willen) zetten om, samen met ons, digitale criminaliteit tegen te gaan. Het netwerk dat je daarmee in kaart brengt kan in de toekomst (wellicht) vaker worden ingezet. (publiek-private samenwerking)

Actie 11: Huisbezoeken bij slachtoffers van online criminaliteit	
Algemene info	Coördinatie: Bestuurlijke werkgroep DVCC Status: Op te starten
Doel	Bekend is dat een slachtofferbezoek door een burgemeester in zijn/haar rol als burgervader/moeder goeddoet bij slachtoffers van high impact crimes, zoals bij woningovervallen en explosies. Wetende dat online criminaliteit ook als high impact crime gecategoriseerd kan worden, verkennen we in 2025 of burgemeesters in voorkomende gevallen ook huisbezoek afleggen bij slachtoffers. Ons doel is om dit mogelijk te maken eind 2025.
Output	- Afspraken maken met politie over richtlijnen voor het bezoeken van slachtoffers door bestuurders. - Afspraken eenheidsbreed onder de aandacht brengen (mbv netwerk digitaal politiewerk) Beoogd resultaat: in 2025 worden er minimaal 10 huisbezoeken afgelegd aan slachtoffers van online criminaliteit.

Bijlage 2

Van : Tineke Hendrikse
Aan : Bestuurlijke werkgroep Digitale Veiligheid en Cybercrime
Datum : 19 november 2024
Onderwerp : Verslag reflectiegesprekken

Aanleiding en doel
We zijn halverwege de looptijd van de huidige veiligheidsstrategie. Om die reden zijn in september en oktober met alle leden van de bestuurlijke werkgroep Digitale Veiligheid en Cybercrime (tussen)evaluatiegesprekken gevoerd over (de voortgang van) het programma Digitale Veiligheid en Cybercrime. Het doel van de gesprekken is om inzicht te krijgen in wat goed gaat, maar ook waar we de resterende tijd van de veiligheidsstrategie op moeten versnellen om het beoogde resultaat te behalen.

In de bijlage staan de vragen die ter voorbereiding zijn verstuurd.

Resultaten
Samenvattend kwamen de volgende evaluatiepunten naar voren in de gesprekken die gevoerd zijn.

1. Actiestand wordt gewaardeerd, maar wordt het scherpe gesprek voldoende gevoerd?
Sinds het ingaan van de veiligheidsstrategie is ingezet op actie. Hiertoe zijn ambtelijke werkgroepen gevormd in ieder district. Deze actiestand wordt gewaardeerd. Maar richten we onze pijlen op het juiste doel (zie ook nr. 2), wordt het scherpe gesprek voldoende gevoerd en blijft de aanpak niet te vrijblijvend (zie ook nr. 5)?

2. Informatiepositie van het lokale bestuur moet beter
Het lokale bestuur krijgt geen periodieke informatie vanuit politie over slachtoffer- en daderschap van online criminaliteit in de eigen gemeente. Dit maakt dat bestuurders het gevoel hebben achter de zaken aan te lopen. De wens is om beter zicht te hebben op het probleem in eigen gemeente, zodat gericht tot actie kan worden overgegaan. Er is behoefte aan informatie met betrekking tot modus operandi, maatschappelijke impact, link naar andere vormen van criminaliteit, criminele hotspots, etc.

3. Professionaliseren vakmanschap
Voor iedere professional in onze regio vraagt digitalisering verandering in zijn/haar werk, niet alleen voor medewerkers in het veiligheidsdomein (en) met cyber in functiebeschrijving. Toch verloopt de ontwikkeling binnen het vakmanschap van onze medewerkers te traag, mede door koudwatervrees. Prio Digi wordt genoemd als mooi project om dit koudwatervrees weg te nemen.

4. Meer communiceren
Als gezamenlijke (lokale) overheid trekken we (te) weinig met elkaar op om zichtbaar te maken welk leed er is, maar ook wat wij doen om dit te beperken. Daarom zouden we meer (gezamenlijk) moeten communiceren om te problematiseren, urgentie te vergroten en inspanningen zichtbaar te maken.

5. Urgentie voor het probleem bij bestuurders blijft (soms) achter
Digitalisering heeft impact op elke inwoner én organisatie. Dit vraagt nú om actie. Niet alleen met betrekking tot het weerbaar maken van inwoners, maar ook tot weerbaar maken van de eigen organisatie (eigen huis op orde). Dit urgentiegevoel voelt nog lang niet iedere lokale bestuurder.

6. Wat is de voortgang?

Het blijft te vaag welke stappen er gezet worden lokaal en regionaal: hoe gaat het, wat moet beter, wat is de maatschappelijke impact? Laten we dit beter in kaart brengen, zodat we beter zicht krijgen op of we het goede doen.

Voorbereidende vragen

1. We zijn een "actieprogramma" met als doel: slachtofferschap voorkomen, daderschap voorkomen en daders pakken.
    a. Wat vindt u van de samenwerking die hiertoe moet leiden (district/regionaal)?
    b. Welke extra inspanningen zou u graag zien in het samenwerkingsverband van gemeenten, politie, Openbaar Ministerie, Bureau RVS?
    c. Etc.
2. Hoe tevreden bent u over de informatiepositie die u heeft over:
    a. Incidenten/slachtoffers/daders/Modus Operandi
    b. Ontwikkelingen in het district / regionaal / landelijk
    c. Etc.
3. Hoe tevreden bent u over de Kennis en Expertise (-overdracht) in ons samenwerkingsverband?
    a. Wat moeten we anders gaan kunnen met elkaar?
    b. Welke doelgroepen moeten we betrekken?
    c. Etc.
4. Hoe tevreden bent u over de snelheid van verandering in ons samenwerkingsverband?
    a. Versnellen we op de juiste zaken tot heden / doen we het goede?
    b. Hoe tevreden bent u over de bijdragen van eenieder aan de benodigde verandering?
    c. Etc.
5. Communicatie intern (in en tussen onze organisaties) / extern (naar de samenleving)
    a. Benutten we communicatie voldoende / hoe tevreden bent u hierover?
    b. Welke communicatiekansen ziet u?
    c. Etc.

Bijlage 3

Programma Digitale veiligheid & cybercriminaliteit; Doelen-Inspanningen-Netwerk

Ambitie

In Midden-Nederland gaan we slachtoffer- en daderschap van gedigitaliseerde criminaliteit en cybercrime voorkomen en daders hiervan pakken. Hiertoe hebben we kundige professionals waarvoor integraal samenwerken tussen gemeenten, politie en OM vanzelfsprekend is. Data wordt gebruikt om capaciteit gericht in te zetten. De potentiële slachtoffers en daders worden weerbaar tegen gedigitaliseerde criminaliteit en cybercrime.

Doelen

- **Voorkomen Slachtoffer- en daderschap en daders pakken**
- **Kundiger organisaties en medewerkers**

Baten

- Integraal sturen vindt plaats op basis van informatiebeeld
- Slachtoffers hebben een hogere melding- en aangifte-bereidheid
- Onze professionals zijn bewust en bekwaam t.a.v. DV&CC
- Effectiever (voorkomen en) aanpakken daders
- Onze inwoners weten beter hoe ze hun slachtofferkans kunnen verkleinen

Inspanningen en resultaten

Informatiebeeld

- Samenbrengen databronnen (directe en indirecte partners, zicht op cyber); **Informatiebeeld DV&CC**

Communicatie

- Communicatie Campagne: **communicatie-uitingen met groot bereik binnen MN**
- Verhalen verzamelen voor media en relatiebeheer: **publicaties in regionale media**
- Communicatie toolbox ontwikkelen; **toolbox**

Actiegericht (samen)werken

- Overzicht creëren rollen en relaties + afhankelijkheden; **overzicht DV&CC profs**
- Hulp en advies aan **zelfstandige werkgroepen met actieplannen**
- Vergroten handelingsperspectief en innovatie
- Gerichte acties voor slachtoffers, potentiele daders en daders
- Adequaat reageren op signalen slachtoffers zodat ze zich gehoord en geholpen voelen

Kennis- en expertiseoverdracht

- Best practice gespreksronde (binnen en buiten MN); **kennisdeling**
- Driemaandelijkse nieuwsbrief DV&CC MN **Kennisdeling**
- Organiseren themagroepen (o.a. communicatie, ciso); **prof. leergemeenschap**

Cyclisch werken binnen het programma door in te zetten op werkvormen die het Weten (o.a. communicatieuitingen en themagroepen), Kunnen (o.a. workshops en trainingen), Doen (o.a. werkgroepen en actieplannen) en Leren (o.a. evaluaties en leerpunten) mogelijk maken.

Doelgroepen

- Politie: eenheidsleiding, politiechefs, DRIO, recherche, basisteams
- OM: OM-leiding, OvJ's, afdeling Beleid & Strategie
- Gemeenten: burgemeester, GS, GR, Hoofd veiligheid, veiligheidsprofessionals
- Indirect: (potentieel) slachtoffers en daders

Programmastrategie

- Optreden als één overheid
- Smeden van maatschappelijke coalities
- Integrale uitvoeringspraktijk

Randvoorwaarden voor succes

- Het speelveld door en door kennen: wie is waarvan en hoe raakt eenieder aan DV&CC?
- Partners geven ons inzicht in hun organisatie
- Lokale vertaling van (csv) informatie om tot prioritering in casuïstiek te komen
- Versterken van de Informatie en Expertise om meer (beter) effect in de aanpak te bereiken: actiegericht
- Impactvolle communicatie: niet alleen over interventies maar ook op effecten van die interventies
- Samenwerkingskunde: zicht op elkaars ambitie, belangen, mogelijkheden en werken aan relaties
- Partners delen en vertalen visie en afspraken op integrale aanpak in de eigen organisatie (thuisfrontmanagement)
- Ieders betrokkenheid in tijd, geld en het leveren van capaciteit
- Blijvend leren van elkaar

Bureau
Regionale
Veiligheidsstrategie

Kroonstraat 25 - Postbus 8300 - 3503 RH - Utrecht - 06 148 73 690 - secretariaat@rvs-mn.nl - www.veiligheidscoalitie.nl

Kroonstraat 25 - Postbus 8300 - 3503 RH - Utrecht - 06 148 73 690 - secretariaat@rvs-mn.nl - www.veiligheidscoalitie.nl