PLATFORM IVZ
SAMEN STERK VOOR EEN VEILIG TWENTE

VOORSTEL
DISTRICTELIJK
VEILIGHEIDSOVERLEG TWENTE

ONDERWERP
EVALUATIE PROJECTENAANPAK GEDIGITALISEERDE CRIMINALITEIT 2022-2023 EN GOVERNANCE DIGITALE VEILIGHEID

AGENDAPUNT -VOLGT

DATUM
14 DECEMBER 2023

OPENBAAR
JA

BEHANDELD DOOR
S. FAAL EN J. SLOT

TELEFOONNUMMER
06-10041762

PORTEFEUILLEHOUDER
DORET TIGCHELAAR

ADVIES AAN HET DVO

1. Kennis nemen van de evaluatie van de projectenaanpak gedigitaliseerde criminaliteit van het Platform IVZ 2022-2023 en de overwegingen hieruit mee te nemen bij de opstelling van het nieuwe programma voor 2024 e.v..
2. Opdracht te geven aan secretaris van het AB/DVO tevens voorzitter van het Platform IVZ om ambtelijk te verkennen hoe alle onderdelen van Digitale Veiligheid in onderlinge samenhang aangestuurd en geborgd kunnen worden.

Inleiding
Onze samenleving digitaliseert en ontwikkelingen volgen elkaar in een razend tempo op. Het digitaliseren van de samenleving levert voordelen op zoals online dienstverlening en snelle/goede informatie-uitwisseling, maar ook nadelen omdat digitale onveiligheid zich in de samenleving nestelt. Denk aan: uitval, verstoring, misbruik, fraude, etc. Regelmatig worden overheden, bedrijven en inwoners slachtoffer, met alle gevolgen van dien. De politie ziet in alle klassieke misdrijven steeds vaker een digitale component.

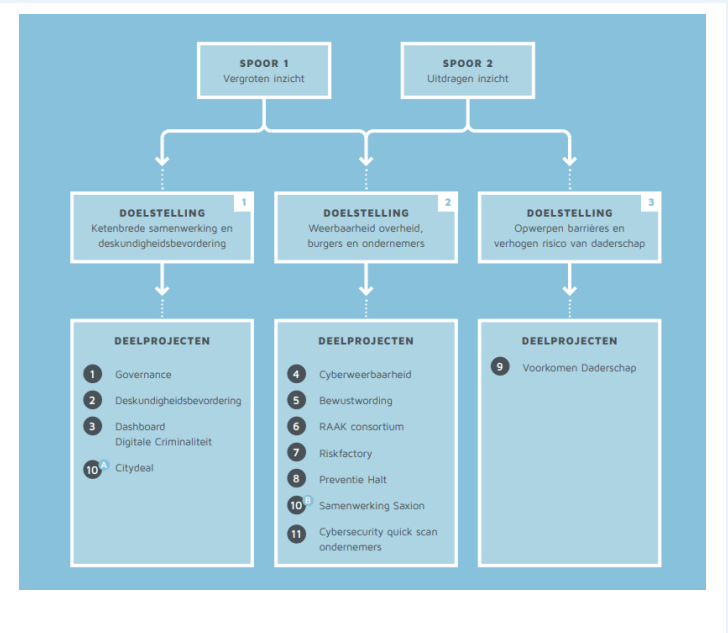
Uit ervaring blijkt dat vitale organisaties als gemeenten, ziekenhuizen, universiteiten, etc. kwetsbaar zijn voor de gevolgen van een cyberaanval. De continuïteit van deze organisaties raakt hierdoor in het geding voor onze samenleving. Digitale veiligheid kan dan ook niet meer gezien worden als een losstaand werkveld, maar is inherent verbonden aan de overige veiligheidstaken. Dit vraagt om een integrale aanpak waarbij digitale veiligheid geprioriteerd is bij de partners en een heldere brede governance structuur krijgt die passend is bij de aanpak van de problematiek. In dit advies wordt hiervoor een voorstel gedaan. Daarnaast wordt de projectenaanpak gedigitaliseerde criminaliteit van het Platform IVZ in de afgelopen twee jaar beschreven en geëvalueerd.

Beslispunt 1 Projectenaanpak gedigitaliseerde criminaliteit 2022-2023
Het Platform IVZ heeft een projectenaanpak ontwikkeld waarbij verschillende activiteiten ontplooid en uitgevoerd zijn. Hierbij is de Twentse aanpak gericht geweest op:

1. Een weerbare overheid en maatschappij tegen cybercrime en gedigitaliseerde criminaliteit. Het weerbaar maken van de overheid, burgers en ondernemers door bewustwording, deskundigheidsbevordering en het aandragen van handelingsperspectieven;
2. Een ketenbrede samenwerking en deskundigheidsbevordering. De samenwerking op zoeken in de aanpak van digitale criminaliteit met o.a. (veiligheids)partners, kennisinstituten, CCV, VNG en het veiligheidsnetwerk Oost-Nederland;
3. Het creëren van een ongunstig klimaat voor cybercrime en gedigitaliseerde criminaliteit door het opwerpen van barrières en het verhogen van het (ervaren) risico van daderschap.

De ontwikkelde projectenaanpak is daarbij opgebouwd aan de hand van twee sporen die in alle deelprojecten zijn weerslag hebben gevonden. Het eerste spoor betrof het vergroten van het inzicht in het brede spectrum van digitale criminaliteit. Om digitale criminaliteit tegen te gaan, is het nodig om dit fenomeen eigen te maken. Er is nog veel onbekend over het thema bij de overheid en de samenleving. De uitdaging zit daarbij voornamelijk in kennisopbouw, bewustwording en communicatie. Het tweede spoor had betrekking op het uitdragen van het verworven inzicht.

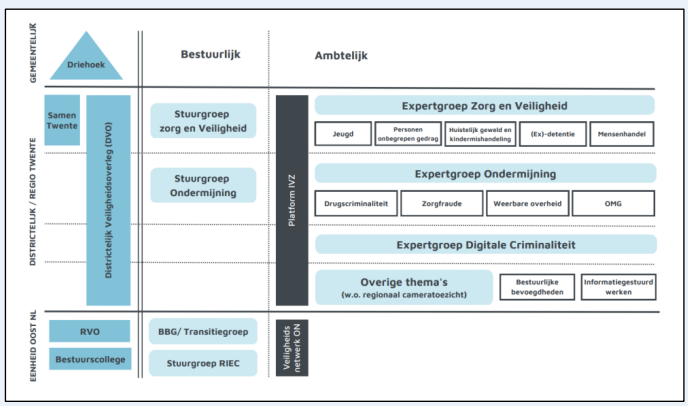
In onderstaand overzicht is de projectaanpak met bijbehorende deelprojecten schematisch weergegeven.



In bijlage 1 van deze adviesnota zijn de activiteiten en (waar mogelijk) de resultaten van de verschillende deelprojecten uit de projectenaanpak beschreven. Er is best veel werk verzet in de afgelopen 2 jaar op dit thema door de expertgroep gedigitaliseerde criminaliteit. De implementatie van het aangeboden materiaal laat echter nog wel te wensen over. De actiebereidheid en het urgentiebesef op dit thema moet duidelijk vergroot worden bij de Twentse gemeenten en veiligheidspartners.

Beslispunt 2 Governance aanpak Digitale veiligheid

Digitale veiligheid is een gezamenlijk probleem en vormt een gezamenlijke uitdaging als overheid. De huidige aanpak van digitale onveiligheid ligt echter nog gefragmenteerd bij de verschillende veiligheidspartners. De huidige aanpak van digitale veiligheid is niet zoals bij de aanpak van Ondermijning en Zorg & veiligheid breed geborgd in een integrale aansturingsvorm (governance). Voor de programma-aanpak van ondermijning is een stuurgroep ingesteld alsmede ook voor Zorg, Veiligheid & Straf. Zie hiervoor onderstaande huidige governance structuur.



Voorgesteld wordt om eerst ambtelijk te verkennen op welke wijze de aanpak van Digitale Veiligheid net als bij de overige geprioriteerde veiligheidsthema's integraal en in onderlinge samenhang bestuurlijk aangestuurd kunnen worden zodat alle facetten geborgd zijn. Te denken valt aan het instellen van een stuurgroep met meerdere portefeuillouders voor de verschillende onderdelen van digitale onveiligheid en vertegenwoordigers van politie, OM, VRT (cririsbeheersing & informatieveiligheid), Onderwijs, Bedrijfsleven, etc. Dit geldt dan ook voor het verbreden van de ambtelijke expertgroep gedigitaliseerde criminaliteit met de overige onderdelen van digitale onveiligheid.

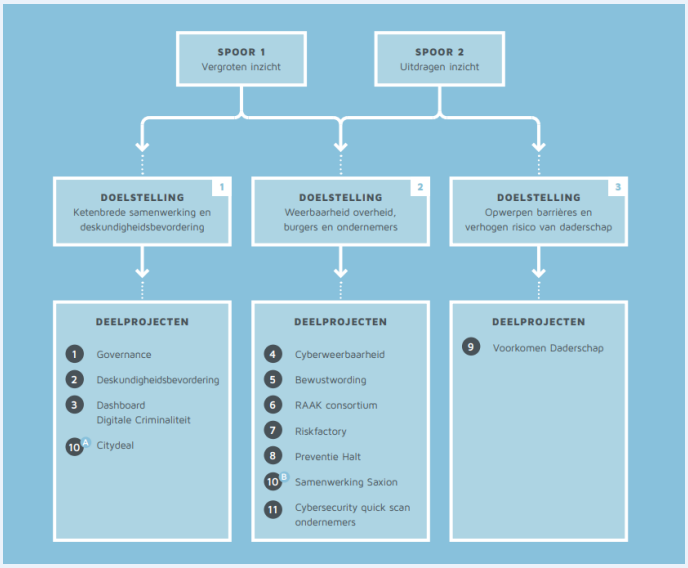
Zoals uit voorgaande evaluatie van de projectenaanpak gedigitaliseerde criminaliteit (Platform IVZ) blijkt, is de urgentie tot actiebereidheid op dit thema onvoldoende. Er is behoefte aan erkenning van een gezamenlijke verantwoordelijkheid. Zowel districtschef van politie als huidige bestuurlijk portefeuillehouder gedigitaliseerde criminaliteit hebben de behoefte kenbaar gemaakt tot het instellen van een brede stuurgroep Digitale Veiligheid, zodat alle facetten van digitale onveiligheid integraal worden aangestuurd en zijn geborgd.

In bijgevoegde memo is een uitgebreidere toelichting opgenomen m.b.t. de governance.

Bijlagen:

1. Terugblik projectenaanpak gedigitaliseerde criminaliteit Platform IVZ 2022-2023
2. Memo governance digitale veiligheid
3. Cyberwegenkaart CCV

Bijage 1 Terugblik deelprojecten Gedigitaliseerde Criminaliteit

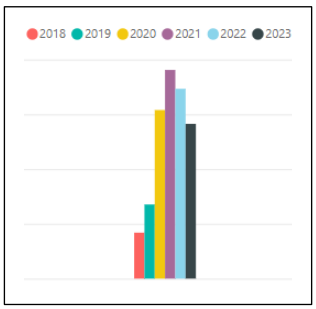


Deelproject 1 Governance

In de afgelopen periode is bij de uitvoering van de projectenaanpak onvoldoende stil gestaan bij de governance, de bestuurlijke en integrale aanpak van digitale veiligheid. De werkzaamheden zijn onder de vlag van het Platform IVZ uitgevoerd door de expertgroep gedigitaliseerde criminaliteit bestaande uit vertegenwoordigers van gemeenten, politie en OM. De werkzaamheden waren met name gericht op bewustwording, deskundigheids-bevordering en het bieden van handelingsperspectieven voor de verschillende doelgroepen. Er is daarbij geen verbinding gelegd met de andere onderdelen van digitale veiligheid. Vandaar dat wordt voorgesteld om voor de komende beleidsperiode ambtelijk verkennen op welke wijze alle facetten van digitale onveiligheid zowel ambtelijk als bestuurlijk vorm gegeven kan worden, zodat dit thema integraal en in onderlinge samenhang aangepakt kan worden.

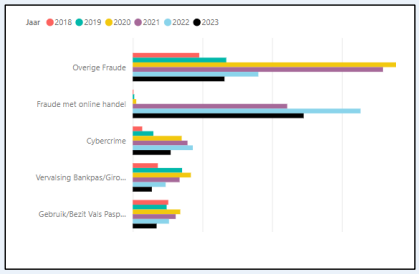
Deelproject 2 Deskundigheidsbevordering

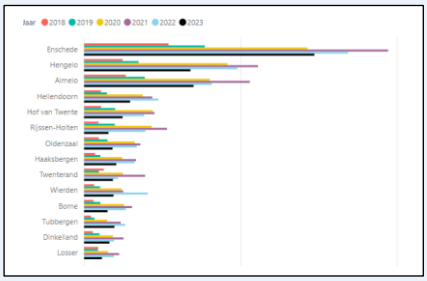
Op 24 mei 2022 en op 16 november 2023 zijn er vanuit het Platform IVZ twee bijeenkomsten georganiseerd om de bekendheid en deskundigheid rondom het thema digitale criminaliteit te bevorderen. In 2022 werd in het algemene gedeelte een interessante casus en hun aanpak toegelicht door het OM en politie. Daarnaast zijn er wokshops georganiseerd door het CCV, Hackshield en een gemeente Utrecht die landelijk gezien één van de koplopers is in de aanpak van digitale criminaliteit. In november 2023 wordt het HUB team door het OM toegelicht, komt het tegengaan van online ordeverstoringen aan bod en geeft Saxion Hogeschool een toelichting op het Raakconsortium , waarbij verschillende handelingsperspectieven voor de diverse doelgroepen geboden worden. Het Centrum voor Veiligheid en Digitalisering komt langs en belicht de risico’s voor MKB-ers in het kader van Cybersecurity. Tot slot worden twee campagnes die opgeleverd zijn door het Platform IVZ: “Echt Nep en Het stopt bij jou”, toegelicht en aangeboden aan de Twentse gemeenten. De opkomst bij beide bijeenkomsten is helaas laag: slechts 40 deelnemers per bijeenkomst. Dit geeft aan dat het thema onvoldoende leeft en weinig prioriteit krijgt. De aanwezigen beoordeelden de bijeenkomst als goed en waardevol.



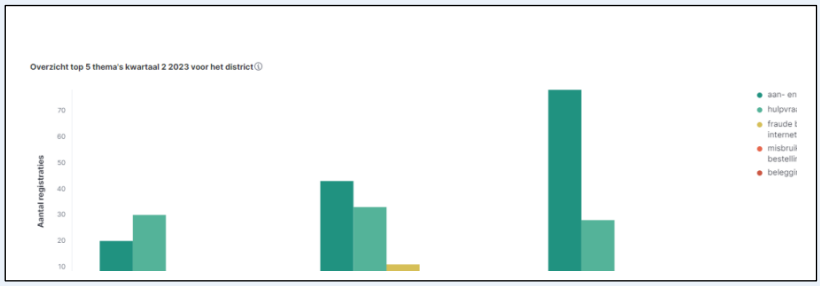
Deelproject 3 Dashboard digitale criminaliteit / cyberbeelden politie

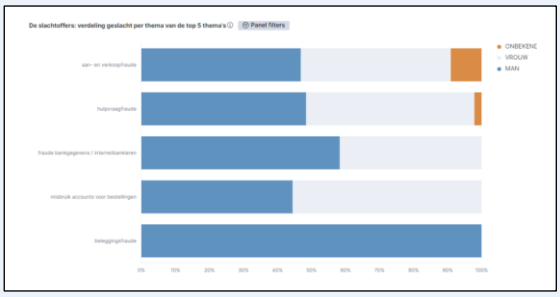
Door het Platform IVZ is een dashboard Digitale Criminaliteit ontwikkeld en beschikbaar gesteld aan de Twentse gemeenten waartoe de veiligheids-coördinatoren toegang hebben. Hiernaast zijn een aantal visuals weergegeven vanuit dit dashboard. Hoewel digitale criminaliteit voor de coronacrisis al groeiende was, is het probleem tijdens de crises nog groter en zichtbaarder geworden. Maar ook na de crises blijft digitale criminaliteit urgent.





Vanuit politie Oost Nederland worden sinds enige jaren per kwartaal cyberbeelden opgesteld en verspreid. Het doel hiervan is om gemeenten handvatten te geven voor het vormgeven van een lokale aanpak tegen digitale criminaliteit. In deze beelden wordt informatie verstrekt over de verschillende vormen van online criminalieit in het district als ook informatie over slachtofferschap (leeftijd, geslacht, etc.).





Onlangs is ten behoeve van voorliggende evaluatie geïnventariseerd onder gemeenten of zij de cyberbeelden regelmatig ontvangen van politie en zo ja, wat zij er vervolgens mee doen. Uit deze inventarisatie blijkt dat bijna alle gemeenten aangeven de beelden tot nu toe niet te hebben ontvangen. Zij zouden dit wel heel graag willen zodat zij gerichter kunnen inspelen op het thema. Dit helpt mogelijk ook bij het toenemen van het gezamenlijke urgentiebesef en actiebereidheid.

Deelproject 4 Cyberweerbaarheidsmonitor

In samenwerking met Saxion Hogeschool is het initiatief ontstaan om de weerbaarheid in gemeenten en het zelfbeschermend gedrag van doelgroepen te onderzoeken aan de hand van een cyberweerbaarheidsmonitor om zodoende risico communicatie op maat te kunnen bieden. Vanuit Twente hebben de gemeenten Almelo, Hengelo en Rijssen-Holten een lokale cyberweerbaarheidsmonitor laten uitvoeren. De resultaten van de cyberweerbaarheidsmonitors van de drie gemeenten zijn vergeleken. De belangrijkste bevindingen zijn als volgt:

- In alle drie de gemeenten heerst een sterk optimistische bias; mensen geloven dat cybercriminaliteit anderen treft en niet henzelf.
- Er is echter wel behoefte aan meer informatie over zelfbescherming, het herkennen van pogingen tot cybercriminaliteit en wat te doen bij vermoedelijk slachtofferschap.
- Respondenten geven de voorkeur aan het ontvangen van deze informatie via de rijksoverheid, internetproviders, politie en de gemeente.

De aanbevelingen richten zich voornamelijk op het doorbreken van de optimistische bias, omdat het iedereen kan overkomen. Het is essentieel om het risicoperceptie te verhogen door op maat gemaakte interventies toe te passen. Daarnaast wordt aanbevolen om lokale, brede samenwerking op het gebied van cyberweerbaarheid te bevorderen.

Deelproject 5 Bewustwording

Binnen dit deelproject is ingezet op bewustwording en aandacht voor het thema digitale criminaliteit gericht op drie doelgroepen: jongeren, senioren en MKB-bedrijven. Door het CCV is berekend dat de jaarlijkse schade voor inwoners van Twente ca €10 miljoen bedraagt. Voor deze doelgroepen zijn verschillende activiteiten ontplooit vanuit het Platform IVZ.

- Deelname van Hackshield door 9 gemeenten. HackShield is een online game die kinderen tussen de 8 en 12 jaar oud weerbaar maakt tegen cybercriminaliteit. Via deze spannende game worden kinderen opgeleid tot Junior Cyber Agents die zichzelf en hun omgeving kunnen beschermen tegen online gevaar. Zo leren ze niet alleen zélf iets; ze kunnen daarna anderen ook adviseren.
- Het delen van social media campagnes Echt Nep en Het Stopt bij jou.
- Het organiseren van week van de digitale veiligheid/cyberweken.
- Het ontwikkelen van een folder voor senioren.
- Het organiseren van wijksessies voor senioren in samenwerking met politie en Riskfactory. 200 senioren (klanten Univé)
- De inzet van escaperoom door politie in het voortgezet onderwijs en het mobiele media lab in gemeenten.

Deelproject 6 Raak consortium

Het Platform IVZ heeft via gemeente Enschede deelgenomen aan het Raak consortium waarin onder leiding van twee lectoraten (w.o. Saxion Hogeschool), enkele gemeenten en samenwerkingsverbanden in den lande hun krachten gebundeld hebben. Met als doel het ontwikkelen van een gemeentelijk offensief ter preventie van slachtofferschap van cybercrime. Met welke interventies kunnen coördinatoren integrale veiligheid de cyberweerbaarheid van burgers en bedrijven binnen hun gemeente vergroten.

Uiteindelijk zijn vier interventies ontwikkeld en na implementatie geëvalueerd:

- "Doorsturen doe je niet!"om jongeren weerbaar te maken tegen misbruik van seksueel beeldmateriaal;
- Instagram-campagne om jongeren weerbaar te maken tegen geldezelen;
- "Laat je geen h@ck zetten!' om ouderen weerbaarder te maken tegen digitale oplichting;
- MKB Cyber Buddy's om MKBérs weerbaarder te maken tegen ransomware.

De uitkomsten van het Raak consortium met bijbehorende interventies zijn 16 november 2023 gepresenteerd door Saxion Hogeschool tijdens de bijeenkomst deskundigheidsbevordering voor professionals w.o. gemeenten.

Deelproject 7 Riskfactory Twente

Vanuit het Platform IVZ is een subsidie aangevraagd en toegekend (€50.000) tot de ontwikkeling van een extra module/level van de game Hackshield voor basisschoolleerlingen die alleen gespeeld kunnen worden bij één van de drie riskfactories in Nederland. In dit level staat het veilig aanmaken van een profiel, hoe om te gaan met vriendschapsverzoeken en het cyberpesten centraal.
Hiernaast heeft Risfactory Twente twee internetveiligheid scenario's ontwikkeld voor leerlingen van het Middelbaar Onderwijs. Deze twee scenario's gaan in op sextorsion en geldezels.

Deelproject 8 Preventie lessen Halt

Halt Twente verzorgt in het kader van de projectenaanpak voorlichtingen op de ROC's in Twente aan de leerjaren 1 en 2 over online fraude en cybercriminaliteit. De les richt zich op de risico's en gevolgen, maar vooral ook op wat je moet doen om te voorkomen dat je slachtoffer of dader wordt van internetcriminaliteit. Helaas moet gemeld worden dat het geen storm loopt met de aanvragen vanuit gemeenten en onderwijs. Tot nu toe wordt alleen gebruik gemaakt van het aanbod in de gemeente Almelo.

Deelproject 9 Voorkomen daderschap

a) Reboot-camp: Vanuit eenheid Oost hebben 75 jongeren (w.o. uit Twente) deelgenomen aan het Reboot-camp georganiseerd door het Veiligheidsnetwerk Oost Nederland. Re-bootcamp is gebaseerd op ervaringen uit Engeland. Het doel is om jongeren te laten zien hoe ze hun digitale vaardigheden op een goede manier kunnen inzetten. Gemeenten, politie en Openbaar Ministerie hopen door het bieden van positieve alternatieven en trainingen cybercriminaliteit te voorkomen en de jongeren te laten zien dat ze een digitaal talent zijn. Het Cybercrimeteam van de politie en Team High Tech Crime (Landelijke Eenheid, Dienst Landelijke Recherche) vertelden over politie-onderzoeken op het gebied van cybercrime, wat wettelijk online wel en niet mag en over mogelijkheden om te werken bij de politie. Op deze wijze wordt geprobeerd om jong talent aan de overheid te verbinden en voor de goede kant van het spectrum te kiezen.

b) Cease and Disist: Insteek is om te komen tot het ontmoedigen van daderschap van cybercrime. Vanuit Engeland is een preventieve aanpak ontwikkeld welke in Twente als pilot getest gaat worden. Deze aanpak voorziet in een aantal preventieve interventies. De aanpak richt zich op

jongeren die betrokken zijn bij cybercrime. Het zijn jongeren die al een lichte strafbare feiten gepleegd hebben. De preventieve interventies voorzien in het voeren van stopgesprekken/waarschuwingsgesprekken met deze jongeren. Een en ander leidt uiteindelijk tot een reprimande. Deze aanpak van Openbaar Ministerie en politie is geëvalueerd en nu geheel geimplementeerd in de huidige werkwijze sinds 2021/2022.

c) In 2023 is gestart met 1 HUB binnen Oost Nederland, die 6 Basisteams bedienen waaronder Basisteam Midden-Twente. Basisteams hebben geen capaciteit om dieper onderzoek te doen naar achterliggende organisatie/ structuur en komen niet verder dan de aanpak van geldezels. HUB staat voor iets waar alles samenkomt, het is een manier van werken. Er wordt gewerkt volgens het regenboogmodel waarbij geel= bezocht, niks gekocht. Paars is= ik ben grootverbruiker. Doel is mensen te waarschuwen die zichzelf in een lastig parket brengen, preventie naar de dader is het. Voorkomen van daderschap.

<u>Deelproject 10 Overige activiteiten</u>
In de aanpak van digitale criminaliteit hebben de expertgroep digitale criminaliteit Twente, het Veiligheidsnetwerk Oost-Nederland, Hogeschool Saxion en het Safety & Security Lab de krachten gebundeld. Vanuit dit initiatief is een aanvullend pakket van activiteiten ontwikkeld waarbij studenten/stagiaires etc bijna continue worden ingezet om onderzoek te doen en activiteiten te ontplooien op het terrein van aanpak digitale criminaliteit.

<u>Deelproject 11 Cybersecurity check ondernemers</u>
Door samenwerking met het Platform IVZ en gemeenten wil Stichting Novel-T het onderwerp cybersecurity bespreekbaar maken én MKB ondernemers op weg helpen met het in kaart brengen van hun belangrijkste cybersecurity risico's. Dit gebeurt door het uitvoeren van een risicoanalyse (cybersecurity quick scan) bij MKB bedrijven. Deze worden uitgevoerd door een ervaren cybersecurity professional. Met de scan krijgt de ondernemer concrete adviezen en handelingsperspectief om de eigen organisatie cyberweerbaar te maken. Provincie Overijssel heeft deze campagne financieel ondersteund waardoor MKB ondernemers relatief goedkoop (€250 i.p.v. €1.000) de cyber security check kunnen afnemen. Helaas is er vanuit het MKB zeer geringe belangstelling geweest voor dit aanbod. Dit geldt ook voor het MKB cyberbuddy project binnen het Raakconsortium. Dit geeft aan dat het urgentiebesef bij deze doelgroep ook laag is en de actiebereidheid onvoldoende. Dit terwijl het CCV heeft berekend dat de jaarlijkse schadepost voor het MKB in Twente zeker € 90 miljoen bedraagt.

Bijage 2 Memo governance digitale veiligheid / cyberveiligheid

Inleiding

Onze samenleving digitaliseert en ontwikkelingen volgen elkaar in een razend tempo op. Het digitaliseren van de samenleving levert voordelen op zoals online dienstverlening en snelle/goede informatie-uitwisseling, maar ook nadelen omdat digitale criminaliteit zich in de samenleving nestelt. Denk aan: uitval, verstoring, misbruik, fraude, etc. Regelmatig worden overheden, bedrijven en inwoners slachtoffer, met alle gevolgen van dien. De politie ziet in alle klassieke misdrijven steeds vaker een digitale component. Door het Centrum van Criminaliteitspreventie en Veiligheid (CCV) is berekend dat de omvang van de schade op jaarbasis in Twente circa €10 miljoen bedraagt voor inwoners en €90 miljoen voor MKB ondernemers. Een flinke schadepost, waarbij veiligheidspartners willen helpen om potentiële slachtoffers beter te informeren over risico's en het treffen van preventieve maatregelen.
Doordat processen van digitalisering zich in volle vaart blijven voltrekken, is het niet te verwachten dat het aandeel van verstoringen of digitale criminaliteit minder wordt. Daarbij blijkt uit ervaring dat vitale organisaties als gemeenten, ziekenhuizen, universiteiten, etc. kwetsbaar zijn voor de gevolgen van een cyberaanval. De continuïteit van deze organisaties raakt hierdoor in het geding. Digitale veiligheid kan dan ook niet meer gezien worden als een losstaand werkveld, maar is inherent verbonden aan de overige veiligheidstaken. Dit vraagt om een integrale aanpak waarbij digitale veiligheid geprioriteerd is bij de partners en een heldere brede governance structuur krijgt die passend is bij de aanpak van de problematiek. Voordat hier op in wordt gegaan, wordt eerst beschreven wat digitale veiligheid/cyberveiligheid inhoudt.

Digitale veiligheid/Cyberveiligheid

Zoals ook al blijkt uit bovenstaande inleidende tekst worden er verschillende termen gebruikt binnen het thema.

Cybercrime

Met de opkomst van het internet en de computer is een nieuwe soort criminaliteit ontstaan: cybercrime. Onder cybercrime vallen delicten die zich richten op ITC (Informatie- en Communicatie Technologie). Bij dit type criminaliteit wordt dus een ICT-systeem gebruikt als middel om het delict te plegen en is een ICT-systeem het doelwit van het delict. Denk hierbij bijvoorbeeld aan het hacken.

Gedigitaliseerde criminaliteit

Onder gedigitaliseerde criminaliteit vallen delicten die buiten de digitale wereld ook plaats vinden. Denk bijvoorbeeld aan oplichting door middel van babbeltrucs of verkoopfraude. Door het gebruik van ICT kunnen deze delicten op grotere schaal en sneller gepleegd worden. Voorbeelden hiervan zijn: WhatsAppfraude, marktplaatsfraude of digitale stalking.

In deze memo wordt gesproken over Digitale Veiligheid/Cyberveiligheid voor het totale spectrum waartoe beide onderdelen behoren. Hierbij moet rekening worden gehouden dat de definities van cybercrime en gedigitaliseerde criminaliteit elkaar in de praktijk niet volledig uitsluiten. Zo kan een dader een social-media account van iemand hacken (cybercrime) om vervolgens een andere persoon te stalken (gedigitaliseerde criminaliteit) of een phishing-mail

sturen (gedigitaliseerde criminaliteit) met een link waarmee een account of apparaat gehackt wordt (cybercrime).

Aanpak van digitale veiligheid/Cyberveiligheid

Naast cybercrime en gedigitaliseerde criminaliteit, waarvan hierboven de definities zijn beschreven, onderscheidt het CCV nog drie wegen op de cyberwegenkaart om een cyberweerbare overheid te zijn (zie bijlage A):

1) Eigen huis op orde**:** verantwoordelijkheid nemen voor het goed functioneren van de eigen digitale systemen.
2) Cyberincidenten en cybercrises**:** voorbereid zijn op incidenten en crises.
3) Cybercrime en gedigitaliseerde criminaliteit: het weerbaar maken van bewoners en bedrijven.
4) Online aangejaagde ordeverstoring: goed zicht hebben op onrechtmatige activiteiten die online afspelen en daarmee fysieke ordeverstoringen voorkomen.

Veiligheidsregio Twente heeft de afgelopen jaren gewerkt aan de uitvoering van pijlers 1 en 2 van de cyberwegenkaart. Pijlers 3 en 4 hebben in Twente vorm en inhoud gekregen binnen de projectenaanpak gedigitaliseerde criminaliteit van het Platform IVZ. Ook voor de komende jaren is het streven hierin voort te zetten.
De VNG 'Agenda Digitale veiligheid 2022-2026' kerntaak voor gemeenten kent ook een dergelijke indeling van pijlers, waarvan twee pijlers geborgd moeten worden in de aanpak van de lokale overheid. Ook hierbij weer het onderscheid in taken van VRT en Platform IVZ.

Pijler 1: Digitale weerbaarheid van de overheid, bedrijven en maatschappelijke organisaties (VRT):
Deze pijler ziet toe op de digitale weerbaarheid van deze partijen. Hierbij gaat het om het vermogen om (relevante) risico's tot een aanvaardbaar niveau te reduceren door middel van een verzameling van maatregelen en cyberincidenten te voorkomen en wanneer cyberincidenten zich hebben voorgedaan deze te ontdekken, schade te beperken en herstel eenvoudig te maken.

Pijler 2: Cybersecurity-arbeidsmarkt, onderwijs en digitale weerbaarheid van burgers (Platform IVZ):
Deze pijler richt zich op de mens achter de techniek en de digitale weerbaarheid van burgers. Voor de samenleving als geheel is een belangrijke rol weggelegd om digitale vaardigheden te ontwikkelen van basiskennis en -vaardigheden tot aan een hoogwaardige kennis en specialistische cybersecurityvaardigheden. In de volgende paragraaf wordt ingegaan op de governance structuur om bovenstaande pijlers van Digitale Veiligheid in onderlinge samenhang integraal aan te kunnen sturen.

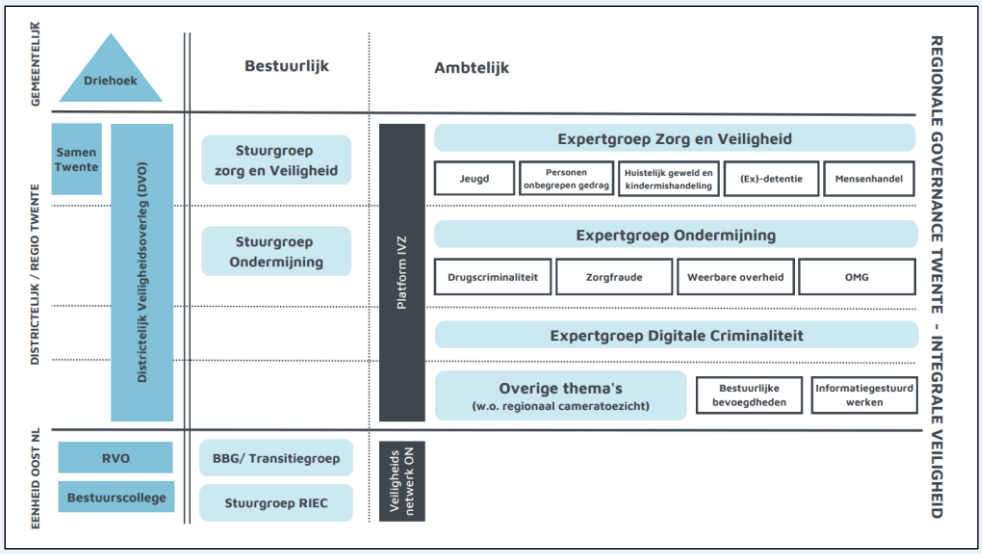
Governance Digitale Veiligheid

Al enige tijd wordt binnen het Platform IVZ gewerkt met een projectenaanpak gedigitaliseerde criminaliteit (2022-2023) met als doel het weerbaar maken van burgers en bedrijven.
Los van deze aanpak van het Platform IVZ houdt Veiligheidsregio Twente zich al lange tijd bezig met het eigen huis op orde krijgen en die van vitale sectoren en voorbereiding en voorkomen van cyberincidenten en crises. VRT neemt aan diverse afstemmingsoverleggen deel binnen Twente als het CISO netwerk

en het netwerk van Functionarissen Gegevensbescherming etc.en op Oost Nederland niveau (expertgroep cybercrises (zorg) en Cyberhub Oost NL etc.

Daarnaast geven politie (en het Openbaar Ministerie) een hoge prioriteit aan digitale veiligheid als één van de strategische thema's naast Ondermijning en Zorg & veiligheid in hun meerjarenbeleidsplan. De samenleving is steeds meer fysiek en digitaal met elkaar verweven. De verregaande digitalisering leidt tot een exponentiële toename van digitale criminaliteit. Criminelen grijpen hun kansen en gebruiken digitale middelen voor hun criminele activiteiten. De overheid heeft, naast wat burgers en organisaties zelf kunnen doen, als taak de samenleving tegen deze digitale vormen van criminaliteit te beschermen, te waarschuwen, slachtoffers te ondersteunen en daders aan te pakken. Het internet mag geen criminele vrijplaats zijn en misdaad mag niet lonen.

Kortom, digitale veiligheid is een gezamenlijk probleem en vormt een gezamenlijke uitdaging als overheidspartners. De huidige aanpak van digitale veiligheid ligt echter nog gefragmenteerd en afzonderlijk bij de veiligheidspartners en is niet zoals bij de aanpak van Ondermijning en Zorg & veiligheid breed geborgd in een integrale aansturingsvorm (governance). Voor de programma-aanpak van ondermijning is een stuurgroep ingesteld alsmede ook voor Zorg, Veiligheid & Straf. Zie hiervoor onderstaande huidige governance structuur.



Voorgesteld wordt om eerst ambtelijk te verkennen op welke wijze de aanpak van Digitale Veiligheid net als bij de overige geprioriteerde veiligheidsthema's integraal en in onderlinge samenhang bestuurlijk aangestuurd kunnen worden zodat alle facetten geborgd zijn. Te denken valt aan het instellen van een stuurgroep met meerdere portefeuillouders voor de verschillende onderdelen van digitale onveiligheid en vertegenwoordigers van politie, OM, VRT (cririsbeheersing & informatieveiligheid), Onderwijs, Bedrijfsleven, etc. Dit geldt dan ook voor het verbreden van de ambtelijke expertgroep gedigitaliseerde criminaliteit met de overige onderdelen van digitale onveiligheid.

Zoals uit voorgaande evaluatie van de projectenaanpak gedigitaliseerde criminaliteit (Platform IVZ) blijkt, is de urgentie tot actiebereidheid op dit thema onvoldoende. Er is behoefte aan erkenning van een gezamenlijke

verantwoordelijkheid. Zowel districtschef van politie als huidige bestuurlijk portefeuillehouder gedigitaliseerde criminaliteit hebben de behoefte kenbaar gemaakt tot het instellen van een brede stuurgroep Digitale Veiligheid, zodat alle facetten van digitale onveiligheid integraal worden aangestuurd en zijn geborgd.

Secretaris van Veiligheidsregio Twente (AB) tevens voorzitter van het Platform IVZ zal zorgdragen dat de ambtelijke vertegenwoordigers bijeen komen om te verkennen op welke wijze dit het beste vorm kan krijgen.

Bijlage 2A Cyberwegenkaart CCV