PLATFORM IVZ

SAMEN STERK VOOR EEN VEILIG TWENTE

PROJECTEN AANPAK
DIGITALE CRIMINALITEIT TWENTE

2022 / 2023

PLATFORM IVZ

SAMEN STERK VOOR EEN VEILIG TWENTE

De veiligheidspartners in de regio Twente willen de komende jaren samen met ondernemers en inwoners de strijd aan gaan tegen digitale criminaliteit. Vanuit het Platform IVZ Twente is de ‘expertgroep digitale criminaliteit’ bezig met de uitvoering van deze aanpak. De expertgroep zet zich in voor bewustwording, deskundigheids-bevordering, communicatie en intelligence. De expertgroep is daarbij vooral faciliterend, stimulerend en ondersteunend. De aanpak is gericht op alle 14 Twentse gemeenten en de veiligheidspartners in Twente. Met het Veiligheidsnetwerk Oost-Nederland trekken we gezamenlijk op in de aanpak. Waar het Platform IVZ zich focust op de aanpak van digitale criminaliteit, richt Veiligheidsregio Twente zich op digitale weerbaarheid en crisisbeheersing.

Susan Faal
Regionaal projectleider Digitale criminaliteit
Veiligheidscoördinator gemeente Rijssen-Holten

VOORWOORD

Digitale criminaliteit is van alle dag. Er zijn vele verschillende delicten en het aantal slachtoffers neemt fors toe. Op dit moment zien we een verschuiving van klassieke criminaliteit naar gedigitaliseerde criminaliteit. Dit betekent niet dat het om dezelfde daders gaat. Iedereen kan vroeg of laat het slachtoffer worden van deze vorm van criminaliteit. De samenleving digitaliseert en de ontwikkelingen volgen elkaar in een razend tempo op. Digitale criminaliteit is een fenomeen dat we beter in kaart (willen) brengen en willen aanpakken.

Gezien de toenemende omvang en de impact van digitale criminaliteit erkennen de veiligheidspartners in het district Twente het belang van de aanpak ervan. Eind 2020 is om deze reden een gezamenlijke projectopdracht voor Twente bestuurlijk vastgesteld om een aanpak te ontwikkelen op digitale criminaliteit door het Platform IVZ. Ook gemeenten als regievoerders op het terrein van integrale veiligheid onderkennen het belang van lokale inspanningen en zien een duidelijke verschuiving in de lokale criminaliteit van traditionele misdrijven (high volume crime zoals diefstal, vernielingen en high impact crime zoals woninginbraak, overvallen) naar criminaliteit met een digitale component. Digitale criminaliteit valt tegenwoordig onder de categorie veel voorkomende criminaliteit.

Onderliggende regionale aanpak bestaat uit verschillende projecten op het gebied van digitale criminaliteit. Een aantal projecten hebben een regionaal karakter en een aantal projecten worden eerst op kleine schaal ontwikkeld en uitgeprobeerd. Over digitale criminaliteit en de aanpak is nog veel te ontdekken en te leren. Dit maakt dat we werken op basis van ‘learning by doing’. Ik hoop dat we elkaar blijven opzoeken en dat we met elkaar in gesprek blijven om kennis en ervaringen uit te wisselen. We kunnen van elkaar blijven leren en de aanpak verbeteren door projecten gezamenlijk te ontwikkelen en tot uitvoering te brengen, uiteraard met lokaal maatwerk.

Ik wens u veel leesplezier.

Doret Tigchelaar
Portefeuillehouder Digitale criminaliteit
Cyberburgemeester
Burgemeester van Wierden

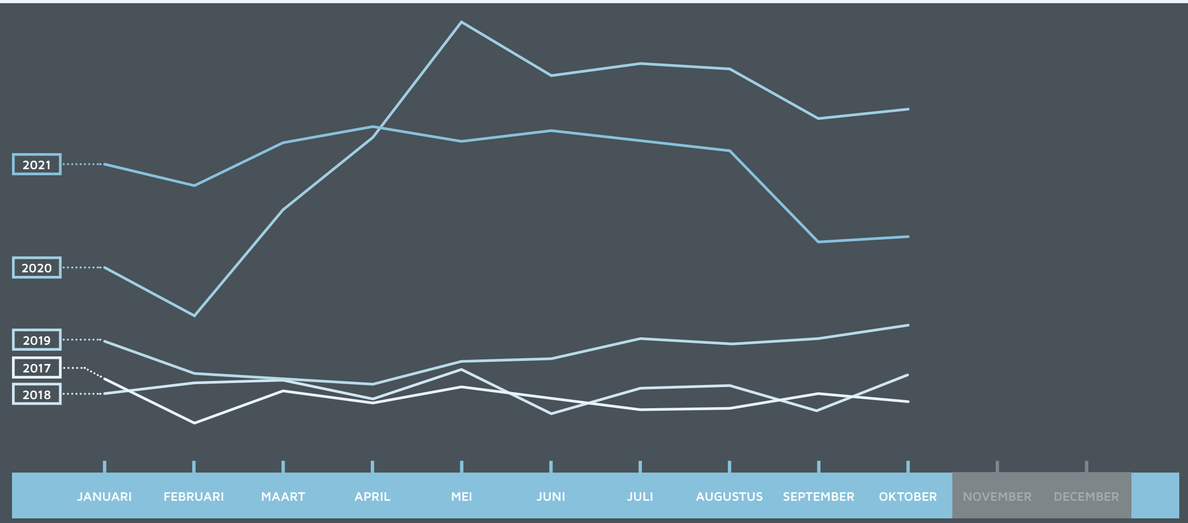
PLATFORM IVZ
SAMEN STERK VOOR EEN VEILIG TWENTE

1 AANLEIDING

De samenleving digitaliseert en de ontwikkelingen volgen elkaar in een razend tempo op. Het digitaliseren van de samenleving brengt ook met zich mee dat de criminaliteit zich in de digitale samenleving nestelt. Digitale criminaliteit is een fenomeen dat we beter in kaart willen brengen. Hoewel digitale criminaliteit voor de coronacrisis al de snelst groeiende vorm van criminaliteit was in Twente, is het probleem tijdens de coronacrisis alleen nog maar urgenter geworden. Tijdens de coronacrisis is het aantal politie-registraties van 'cybercrime', zowel landelijk als in Twente, flink gestegen. De meest waarschijnlijke oorzaak hiervan is het intensievere gebruik van digitale (communicatie) middelen door thuiswerken en het wegvallen van fysiek contact. Daar komt bij dat het aantal geregistreerde gevallen waarschijnlijk nog maar het topje van de ijsberg is. Het werkelijke aantal digitale criminaliteitsincidenten, en dus slachtoffers hiervan, ligt vermoedelijk vele malen hoger.

In de grafiek hiernaast is vanaf maart 2020 een sterk toenemende trendlijn te zien van het aantal incidenten digitale criminaliteit in de regio Twente.

(Bron: dashboard digitale criminaliteit Platform IVZ).



2 DOELSTELLING EN EFFECTEN

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 voornamelijk in kennisopbouw, bewustwording en communicatie.

Integrale samenwerking is hierbij essentieel. Met de Twentse aanpak van digitale criminaliteit willen we bijdragen aan:

- de weerbaarheid van overheid, burgers en ondernemers;
- een keten brede samenwerking en deskundigheidsbevordering;
- het creëren van een ongunstig klimaat voor digitale criminaliteit door het opwerpen van barrières en het verhogen van het (ervaren) risico van daderschap.

Hierbij worden twee sporen gevolgd die in alle deelprojecten (zoals beschreven in hoofdstuk 5) in dit plan zijn weerslag vinden:

1. Het vergroten van het inzicht in het brede spectrum van digitale criminaliteit.
2. Het uitdragen van het verworven inzicht.

Gedurende het project en bij de evaluatie bezien en/of meten we de prestatie indicatoren, zoals gesteld in het projectplan cybercrime Twente.

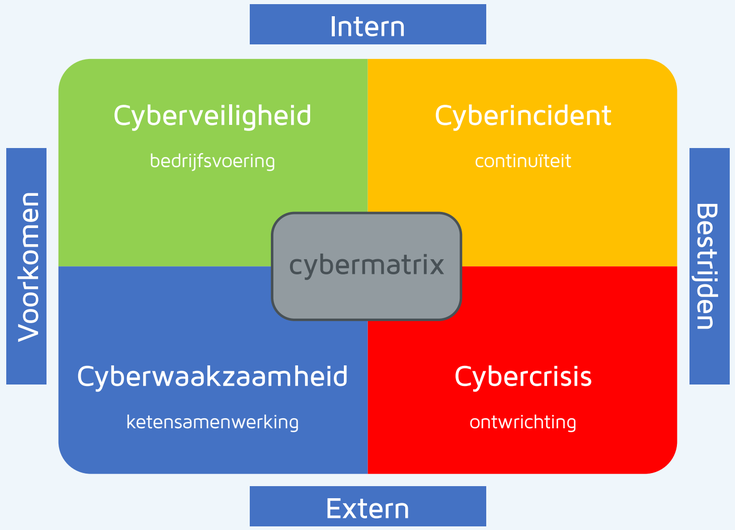
3 BEGRIPPEN EN AFBAKENING

De gehanteerde begrippen in dit programma vragen om een nadere toelichting, te weten:

- **Gedigitaliseerde criminaliteit:** bestaat uit strafbare feiten waarbij gebruik gemaakt wordt van een ICT middel, zoals bijvoorbeeld vriend in nood fraude, online oplichting via whats app, facebook, marktplaats, etc.
- **Cybercrime:** omvat strafbare feiten die worden gepleegd via een ICT middel én die gericht zijn op een ICT middel, zoals hacking, DDoS-aanvallen, en ransomware.
- **Cybersecurity en -safety:** alle beveiligingsmaatregelen die getroffen worden om schade te voorkomen door een storing, uitval of misbruik van een informatiesysteem of computer (‘eigen huis op orde’). Hieronder vallen ook de maatregelen die worden genomen om schade te beperken en/of te herstellen als die is ontstaan. Het betreft zowel technisch maatregelen als maatregelen gericht op bewustzijn en gedrag.
- **Digitale criminaliteit:** cybercrime en gedigitaliseerde criminaliteit tezamen wordt ook wel ‘digitale criminaliteit’ genoemd.

De aanpak vanuit de expertgroep van het Platform IVZ focust zich op de criminaliteitsvormen die vallen onder het begrip ‘digitale criminaliteit’. Hoofddoel is het verhogen van de weerbaarheid van de samenleving voor digitale criminaliteit.

Waar het Platform IVZ zich focust op de aanpak van digitale criminaliteit (cyberwaakzaamheid) richt Veiligheidsregio Twente zich op alle 4 kwadranten van cyberweerbaarheid.



De bovenste helft van de matrix betreft de cyberveiligheid en continuïteit van de eigen organisatie. Rechtsonder betreft de rol van de VRT bij een cybercrisis in de regio.
Het Platform IVZ focust zich op de aanpak van digitale criminaliteit, wat in het blauwe kwadrant cyberwaakzaamheid valt.

4 TWENTSE AANPAK DIGITALE CRIMINALITEIT

De Twentse aanpak digitale criminaliteit is gericht op:

1. het organiseren en faciliteren van regionale en lokale activiteiten voor gemeenten, (veiligheids)partners, ondernemers en inwoners;
2. het weerbaar maken van de overheid, burgers en ondernemers door bewustwording, deskundigheidsbevordering en het aandragen van handelingsperspectieven;
3. het opwerpen van barrières voor daders van digitale criminaliteit;
4. de samenwerking opzoeken in de aanpak van digitale criminaliteit met o.a. (veiligheids)partners, kennisinstituten, CCV, VNG en het veiligheidsnetwerk Oost-Nederland;
5. het onderzoeken van - en experimenteren met landelijke en regionale pilots op het gebied van de aanpak van digitale criminaliteit.

PROJECTEN AANPAK DIGITALE CRIMINALITEIT TWENTE 2022 / 2023

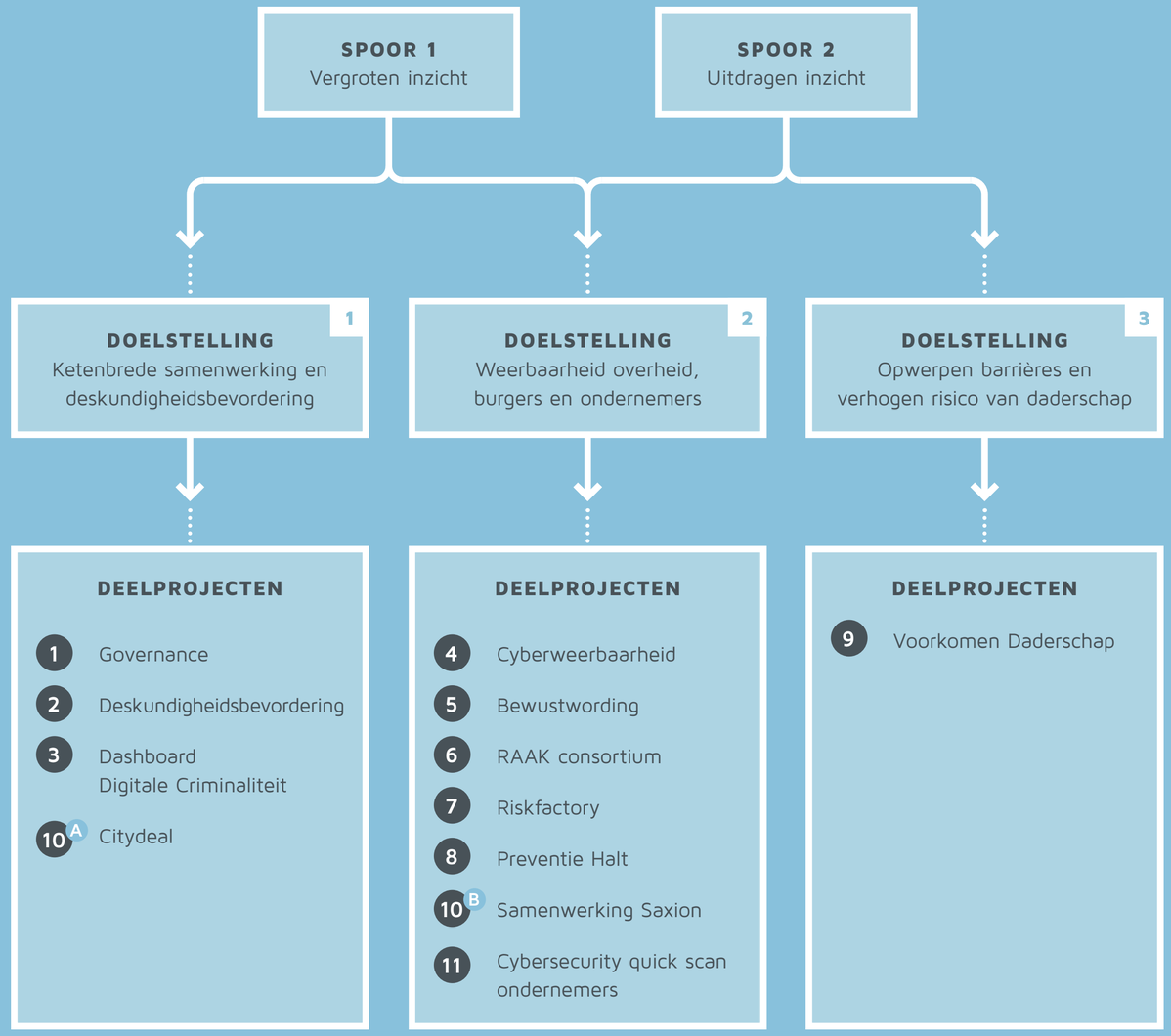
1. GOVERNANCE
2. DESKUNDIGHEIDSBEVORDERING
3. DASHBOARD DIGITALE CRIMINALITEIT
4. CYBERWEERBAARHEID
5. BEWUSTWORDING
6. RAAK CONSORTIUM
7. RISKFACTORY
8. PREVENTIE HALT
9. VOORKOMEN DADERSCHAP

OVERIGE ACTIVITEITEN:

10A CITYDEAL

10B SAMENWERKING SAXION

11 CYBERSECURITY QUICK SCAN ONDERNEMERS



PLATFORM IVZ
SAMEN STERK VOOR EEN VEILIG TWENTE

1 GOVERNANCE NETWERK DIGITALE CRIMINALITEIT TWENTE

PARTNERS:
- REMCO SPITHOVEN (HOGESCHOOL SAXION)
- POLITIE TWENTE / OOST-NEDERLAND
- OPENBAAR MINISTERIE OOST-NEDERLAND
- TWENTSE GEMEENTEN
- ONDERNEMERS (BRANCHEVERENIGINGEN)
- PRIVATE SECTOR ZOALS (VERZEKERINGS)BANKEN

CONTACTPERSONEN:
SUSAN FAAL-TAKAK
PROJECTLEIDER EXPERTGROEP CYBERCRIME TWENTE

MARISKA RIJNEVELD
VEILIGHEIDSNETWERK OOST-NEDERLAND

REMCO SPITHOVEN
HOGESCHOOL SAXION

Doelstelling
Inzicht verschaffen in het 'governance network' in de aanpak van digitale criminaliteit.

Project
De aanpak van digitale criminaliteit vraagt (mogelijk) om een andere aanpak dan de aanpak van klassieke criminaliteit zoals vernielingen in de openbare ruimte. Bij de bestrijding van vernielingen is het grotendeels duidelijk wie welke taken en verantwoordelijkheden heeft in de aanpak. Dit in tegenstelling tot digitale criminaliteit en verantwoordelijkheden van de verschillende partners publiek en privaat inzichtelijk te hebben. Waarbij de samenwerking, taken en verantwoordelijkheden, de actoren en de aanpak nog niet volledig zijn uitgekristalliseerd.

Resultaat
Een infographic en/of een beschrijving van het 'governance network' in de aanpak van digitale criminaliteit. Vanuit lokaal, regionaal en/of landelijk perspectief. We hanteren voor dit project het begrip governance network: "groups of three or more legally autonomous organizations that work together to achieve not only their own goals but also a collective goal" (Provan en Kenis 2008 - p. 231).

(mogelijke) Koppelingen
In samenwerking met het Veiligheidsnetwerk Oost-Nederland wordt het 'governance network' in kaart gebracht voor de regio Oost-Nederland (incl. regio Twente).

Planning
Medio 2022 opleveren 'governance network' digitale criminaliteit.

Randvoorwaarden
Samenwerking Veiligheidsregio Oost-Nederland en partners.

PLATFORM IVZ
SAMEN STERK VOOR EEN VEILIG TWENTE

PARTNERS:
- GEMEENTEN
- OPENBAAR MINISTERIE OOST-NEDERLAND
- POLITIE DISTRICT TWENTE
- INHUUR VAN EXPERTS

CONTACTPERSONEN:
JOP WIEFFER
COMMUNICATIE PLATFORM IVZ

REMCO AAGTJES
POLITIE TWENTE

STAGIAIRE
HOGESCHOOL SAXION

2 DESKUNDIGHEIDSBEVORDERING PROFESSIONALS

Doelstelling
Professionals zijn zich bewust van de ontwikkelingen op het gebied van (de aanpak van) digitale criminaliteit. Professionals weten welke rol zij zelf kunnen spelen in het voorkomen van digitale criminaliteit dan wel het beperken van de gevolgen ervan.

Project
Door middel van actieve inzet worden professionals in de veiligheidsketen deskundig gemaakt op het gebied van (de aanpak van) digitale criminaliteit. Deze kennisbevordering vindt plaats door middel van:
- webinars;
- workshops;
- instructiemateriaal bijvoorbeeld factsheets en infographics.

Als onderdeel van de deskundigheidsbevordering worden de professionals gewezen op handelingskaders bij de voorkoming en aanpak van digitale criminaliteit. Deze kennis dient voor intern gebruik (weerbare overheid), maar evenveel voor extern gebruik - bijvoorbeeld in klantcontact, communicatie, casuïstiek (weerbare maatschappij).

De doelgroep voor deze bevordering bestaat uit:
- gemeentelijke medewerkers;
- medewerkers Openbaar Ministerie;
- de deskundigheidsbevordering is ook voor politie bestemd.

Daarnaast heeft de politie ook intern een programma (cyber & leren).

Resultaat
Een afwisselend programma van bevorderingsactiviteiten, dat bij voorkeur in een voorspelbare cyclus/ritmiek door het jaar heen wordt aangeboden.

(mogelijke) Knelpunten
Mogelijke hindernissen in deze deskundigheidsbevordering zijn:
- onvoldoende sense of urgency bij de professionals;
- tijd en ruimte voor professionals om deel te nemen aan events.

Planning
Doorlopend. Op te stellen aan de hand van gekozen activiteiten.

Randvoorwaarden
Incidenteel budget ten behoeve van experts voor verzorgen webinar, workshop, e.d.

PLATFORM IVZ
SAMEN STERK VOOR EEN VEILIG TWENTE

PARTNERS
- POLITIE OOST-NEDERLAND
- OPENBAAR MINISTERIE OOST-NEDERLAND
- GEMEENTEN

CONTACTPERSOON

SUZANNE COEHORST
VEILIGHEID GEMEENTE ENSCHEDE

JANE SLOT
PLATFORM IVZ TWENTE

3 INTELLIGENCE (DASHBOARD DIGITALE CRIMINALITEIT)

Doelstelling
Sturingsinformatie in het veiligheidsdashboard Twente te genereren in de aanpak van digitale criminaliteit dmv. zicht in de aard en omvang van:
- de diverse verschijningsvormen in Twente zoals online fraude, whats app fraude, vriend in nood;
- de doelgroepen van slachtoffers in Twente;
- daderprofielen.

Project
Om alle taken en bevoegdheden op het terrein van de openbare orde en veiligheid, leefbaarheid en zorg voor inwoners goed in te kunnen vullen, is een goede informatiepositie voor gemeenten steeds belangrijker. Een goede informatiepositie stelt de burgemeester in staat regie te voeren op veiligheid. In 2019 is gestart met de ontwikkeling van een veiligheidsdashboard voor alle Twentse gemeenten. Dit dashboard is inmiddels voor alle gemeenten beschikbaar. Nu ligt de wens om dit dashboard verder door te ontwikkelen voor wat betreft de aanpak van digitale criminaliteit. Dit geeft ons beter inzicht in trends en ontwikkelingen zodat we zowel repressief als preventief beter kunnen interveniëren. In het dashboard zijn geen persoonsgegevens opgenomen maar is data te herleiden naar locaties (tot op buurtniveau) en op verschillende verschijningsvormen en slachtoffers daarvan.

Resultaat
Een dashboard met actuele informatie van diverse partners zoals politie, Openbaar Ministerie, gemeenten.

(mogelijke) Koppelingen
Door Politie Oost- Nederland is een monitor Cybercrime ontwikkeld. Bekeken moet worden in hoeverre hiermee een koppeling gemaakt kan worden. Daarnaast wordt onderzocht welke data en partners relevant zijn om het dashboard te verrijken. Tevens volgen we landelijke ontwikkelingen en eventuele landelijke integrale monitors die in ontwikkeling zijn.

(mogelijke) Knelpunten
Er zijn veel dataleveranciers bij betrokken waardoor de complexiteit toeneemt m.b.t. beschikbaarheid en kwaliteit van data maar ook commitment van partners.

Planning
Een prototype is gereed maar dient nog verder ontwikkeld te worden waaronder afstemming met monitor Cybercrime Politie Oost Nederland. Er wordt naar gestreefd om medio 2022 een integraal dashboard digitale criminaliteit gerealiseerd te hebben.

PLATFORM IVZ
SAMEN STERK VOOR EEN VEILIG TWENTE

4 CYBERWEERBAARHEIDSMONITOR

PARTNERS
- GEMEENTEN
- BURGERPANEL GEMEENTEN
- HOGESCHOOL SAXION
- VEILIGHEIDSNETWERK OOST-NEDERLAND
- KENNISPUNT TWENTE

CONTACTPERSOON
SUSAN FAAL
PROJECTLEIDER EXPERTGROEP CYBERCRIME TWENTE

REMCO SPITHOVEN
HOGESCHOOL SAXION

MARISKA RIJNEVELD
(VEILIGHEIDSNETWERK OOST-NEDERLAND

Doelstelling
De monitor heeft als doel om de cyberweerbaarheid en het zelf beschermend gedrag van doelgroepen op lokaal niveau te onderzoeken en risicocommunicatie verder op maat aan te kunnen bieden.

Project
In samenwerking met Hogeschool Saxion is het initiatief ontstaan om de weerbaarheid in gemeenten te onderzoeken aan de hand van een lokale cyberweerbaarheidsmonitor. Hierbij wordt (vaak) een vragenlijst uitgezet middels een bestaand burgerpanel. In afstemming met de deelnemende gemeenten aan de monitor kan, waar mogelijk, een gezamenlijk regionaal advies en risicocommunicatie worden gegeven.

Resultaat
Inzicht verkrijgen in de weerbaarheid en het zelf beschermend gedrag lokaal bij inwoners (verschillende doelgroepen). Daarnaast een advies op maat over hoe de lokale cyber-weerbaarheid van specifieke doelgroepen te verbeteren is.

(mogelijke) Koppelingen
Voor dit project wordt samengewerkt met het Veiligheids-netwerk Oost-Nederland. De uitvraag voor deelname aan de lokale Cyberweerbaarheidsmonitor vindt breed plaats onder gemeenten in de regio Oost-Nederland.

(mogelijke) Knelpunten
- Het onderzoek is afhankelijk van de resultaten van de lokale Cyberweerbaarheidsmonitor.
- Deelname gemeenten in Twente (en Oost-Nederland) aan de lokale Cyberweerbaarheidsmonitor.
- Gemeenten die een lokaal burgerpanel hebben kunnen alleen deelnemen.

Planning
Periode 2022 opleveren van lokale adviezen aan gemeenten en regionaal advies regio Twente en Oost-Nederland

Randvoorwaarden
- Budget: ca. € 8.500 (excl. btw) per gemeente.
- Capaciteit gemeenten voor opstarten van de monitor lokaal.
- Lokaal burgerpanel.

PLATFORM IVZ
SAMEN STERK VOOR EEN VEILIG TWENTE

PARTNERS
- GEMEENTEN
- POLITIE DISTRICT TWENTE
- HOGESCHOOL SAXION
- VEILIGHEIDSNETWERK OOST NEDERLAND
- BEDRIJFSLEVEN

CONTACTPERSONEN
JOP WIEFFER
COMMUNICATIE PLATFORM IVZ

REMCO SPITHOVEN
HOGESCHOOL SAXION

STAGIAIRE
HOGESCHOOL SAXION

5 BEWUSTWORDING DIGITALE CRIMINALITEIT

Doelstelling
Inzetten op bewustwording en aandacht voor het thema digitale criminaliteit in Twente.

Project
Het weerbaarder maken van inwoners en ondernemers tegen de gevaren van digitale criminaliteit begint bij bewustwording. Weten dat het er (in sterk toenemende mate) is en welke grote gevolgen het voor je kan hebben, is essentieel in de actiebereidheid om jezelf ertegen te beschermen.

Door:
- inzicht in bewustwordingsinterventies. Er is en wordt veel op dit thema gedaan en gemaakt. Een goed overzicht (denk aan een toolbox) van wat er al is en wat werkt, zorgt voor goede keuzes in de toe te passen interventies;
- uitvoering van bewustwordingsinterventies. Nadat er goed zicht is op welke interventies er zijn en goed werken, kan het Platform IVZ verschillende interventies initiëren en dit samen uitvoeren samen met de verschillende partners;
- in samenwerking met Hogeschool Saxion (stageopdracht) nader onderzoeken hoe inwoners van middelbare leeftijd bewuster met de gevaren van digitale criminaliteit kunnen omgaan. De bevindingen zullen gedurende de stageperiode (tot februari 2022) en na afloop de basis vormen voor de verdere uitwerking van dit project.

De bewustwordingsinterventies hebben vooral betrekking op:
- Jongeren;
- Ouderen;
- MKB-bedrijven.

Resultaat
Door het uitvoeren van verschillende bewustwordingsinterventies zijn jongeren, ouderen en MKB bedrijven in Twente zich bewuster van de gevaren van digitale criminaliteit en hebben zij hun gedrag en handelen hierop aangepast.

PLATFORM IVZ
SAMEN STERK VOOR EEN VEILIG TWENTE

(mogelijke) Koppelingen

- Resultaten cyberweerbaarheidsmonitor (zie project 4).
- RAAK consortium (zie project 6).
- In samenwerking met Veiligheidsnetwerk Oost-Nederland en Hogeschool Saxion ontwikkelen van communicatie- en voorlichtingsmateriaal.
- In samenwerking met Safety & Security Lab onderzoeken en ontwikkelen van interventies.

(mogelijke) Knelpunten

- Onvoldoende prioriteit/zicht op de rol van gemeenten in de bijdrage aan bewustwording op dit thema.
- Beschikbare capaciteit en ruimte in communicatiekalenders van de verschillende partners, met name gemeenten.
- Dynamisch fenomeen: de verschillende vormen van crimineel gedrag veranderen in snel tempo. Waar we vandaag voor willen waarschuwen, kan morgen vervangen zijn door een nieuwe vorm van digitale criminaliteit.

Planning

Communicatieacties zijn doorlopend en afhankelijk van de ondernomen acties en activiteiten vanuit de verschillende projectonderdelen. In ieder geval focus op communicatie op dit thema op de volgende momenten:

- Feestdagen einde van het jaar (bewustwording – slachtofferschap).
- Cyberweken Twente (voorjaar en najaar).

Randvoorwaarden:

Mogelijk (minimaal) budgetten voor de uitvoering van bewustwordingsinterventies. Te denken valt aan afhuur ruimtes, opmaken van middelen (zie communicatie of het aanschaffen van al bestaande bewustwordingsinterventies).

PLATFORM IVZ
SAMEN STERK VOOR EEN VEILIG TWENTE

PARTNERS
- HOGESCHOOL SAXION
- HAAGSE HOGESCHOOL
- NEDERLANDS STUDIECENTRUM VOOR CRIMINALITEIT EN RECHTSHANDHAVING (NSCR)
- GEMEENTEN (LANDELIJK)
- VEILIGHEIDSNETWERKEN (MEERDERE REGIO'S)

CONTACTPERSONEN

SUZANNE COEHORST
VEILIGHEID GEMEENTE ENSCHEDE

REMCO SPITHOVEN
HOGESCHOOL SAXION

6 RAAK CONSORTIUM

Doelstelling
Een gemeentelijk offensief ter preventie van slachtofferschap van cybercrime ten behoeve van kwetsbare doelgroepen en bijbehorende typen cyberdelicten.

Project
We nemen deel aan het RAAK consortium cyberweerbaarheid. Binnen het consortium staan onderstaande kwetsbare doelgroepen en bijbehorende typen cyberdelicten centraal. Naar deze kwetsbare doelgroepen en bijbehorende typen cyberdelicten vindt nader onderzoek plaats en worden gericht interventies ontwikkeld.

Het gaat om:
1. Jongeren: sextortion;
2. Jongeren: money muling;
3. Ouderen: vriend-in-nood fraude (whatsapp-fraude);
4. MKB'ers: ransomware;
5. Alle doelgroepen: phishing.

Resultaat
- Vergroten van netwerk op het gebied van de aanpak van digitale criminaliteit.
- Verkrijgen van inzicht in kwetsbare doelgroepen en bijbehorende typen cyberdelicten.
- Gezamenlijk ontwikkelen van interventies voor de verschillende doelgroepen.

(mogelijke) Koppelingen
De interventies die uit het RAAK consortium voortvloeien zullen waar mogelijk gekoppeld worden aan de overige projecten van de expertgroep Twente.

(mogelijke) Knelpunten
Het RAAK consortium betreft een landelijk abstract kader.

Planning
Het streven is om voor maart 2022 inzichtelijk te hebben welke interventies passend zijn voor welke doelgroepen, en om daadwerkelijk interventies ontwikkeld en ingezet te hebben.

PLATFORM IVZ
SAMEN STERK VOOR EEN VEILIG TWENTE

PARTNERS
- GEMEENTEN
- POLITIE
- MINISTERIE JUSTITIE EN VEILIGHEID
- PUBLIEKE PARTNERS

CONTACTPERSONEN

STEFAN MUES
RISK FACTORY TWENTE

JANE SLOT
PLATFORM IVZ TWENTE

7 RISKFACTORY

Doelstelling
Het herhaaldelijk aanbieden van een risicoboodschap geeft een beter en duurzamer geeft. Om deze reden wordt het concept Risk Factory voor minimaal 2 schooljaren (pilot) uitgebreid met een programma voor leerlingen van het voortgezet onderwijs. Het doel is om hiermee een leerlijn te creëren. Het idee is om kinderen in twee levensfasen te ontvangen in de Risk Factory Twente. Hierdoor krijgen zij meer inzicht in onveiligheden en daar bijbehorende handelingsperspectieven.

Het lesprogramma voor het voortgezet onderwijs is in ontwikkeling en kent dezelfde opbouw als de primaire doelgroep. Vastgesteld is dat cybercrime onderdeel wordt van het nieuwe lesprogramma. Dit scenario moet onderdeel zijn (of aansluiten op) bestaande programma's m.b.t. cybercrime.

Project
Risk Factory Twente is een veiligheidseducatiecentrum. 85% van alle Twentse basisschoolleerlingen worden veiligheidsbewust gemaakt door realistische scenario's aan den lijve te ondervinden. Hierbij zijn de belangrijkste uitgangspunten dat veiligheid vanuit een breed perspectief wordt belicht, dat kinderen leren door te doen en dat het leereffect aantoonbaar is.

(mogelijke) Koppelingen
Cybercrime is een breed begrip. Op het gebied van cybercrime lopen veel (gemeentelijke) projecten c.q. programma's. I.o.m. het Platform IVZ zal worden gekeken op welke programma's kan worden aangesloten.

Resultaat
Een scenario cybercrime welke onderdeel is van een volledig lesprogramma (4 scenario's). Sextorsion en geldezels lijken specifieke veiligheidsthema's die aansluiten bij deze doelgroep.

(mogelijke) Knelpunten
De kracht van het concept Risk Factory is dat deze aansluit op de belevingswereld van de doelgroep. Omdat deze leefwereld snel veranderd is het noodzakelijk te blijven door ontwikkelen.

Planning
Vanaf 1 februari wordt het lesprogramma inhoudelijk vormgegeven. Vanaf september 2022 worden de leerlingen van het Voortgezet Onderwijs ontvangen in de Risk Factory Twente.

PLATFORM IVZ
SAMEN STERK VOOR EEN VEILIG TWENTE

VERKENNING VIA PARTNERS
- V(S)O EN MBO SCHOLEN IN DE GEMEENTEN
- DE 14 TWENTSE GEMEENTEN
- POLITIE
- HOGESCHOOL SAXION

CONTACTPERSOON
JANNEKE RIPHAGEN
RELATIEMANAGER HALT

8 PREVENTIELESSEN HALT REGIONALE AANPAK
ONLINE CYBERCRIMINALITEIT EN ID-FRAUDE

Doel
Jongeren op alle V(S)O en MBO scholen leerjaar 1 en 2 in Twente bewust maken van de risico's en gevolgen van online fraude en cybercriminaliteit.

Project
Jongeren kunnen makkelijk in de verleiding komen om snel geld te verdienen. Daarom geeft Halt voorlichting in het voortgezet onderwijs 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. Onder andere komen de thema`s geldezels, identiteitsfraude, online oplichting en hulpvraagfraude in de les aan bod. De preventielessen zetten in op het vergroten van bewustwording en weerbaarheid bij jongeren en sluiten daarom goed aan bij het onderzoek naar weerbaarheid onder jongeren.

Resultaat
Jongeren zijn zich bewust van de risico`s en gevolgen van online fraude en cybercriminaliteit en laten zich minder snel misleiden en misbruiken waardoor ze minder snel dader en/of slachtoffer van online criminele activiteiten worden. Hiermee wordt de zelfredzaamheid van jongeren aangaande dit onderwerp vergroot.

(mogelijke) Koppelingen
Dit project heeft koppelingen met diverse partners namelijk: het onderwijs V(S)O en het MBO en koppelingen met de justitieketen te weten de politie en het OM. Samenwerking met overige netwerkpartners binnen dit project is daarnaast ook van groot belang.

(mogelijke) Knelpunten
Onvoldoende beschikbaarheid voorlichters van Halt. Niet alle scholen willen deelnemen, bijvoorbeeld door onvoldoende onderkenning van de noodzaak.

Planning
Periode 2022 januari-juli het uitvoeren van de preventielessen juli-december onderzoek verwerken.

Randvoorwaarden
Capaciteit voorlichters: Halt-medewerkers/studenten Saxion
Kosten zijn €267,- per voorlichting, dit zou bekostigd kunnen worden door NPO gelden die scholen en gemeenten ontvangen.

PLATFORM IVZ
SAMEN STERK VOOR EEN VEILIG TWENTE

PARTNERS
- BASISTEAMS POLITIE TWENTE
- LANDELIJK DADERPREVENTIE-TEAM LANDELIJKE EENHEID POLITIE
- OPENBAAR MINISTERIE / ZSM OOST-NEDERLAND
- CYBERCRIMETEAM OOST-NEDERLAND

CONTACTPERSOON
MARK IMBOS
OPENBAAR MINISTERIE
OOST-NEDERLAND

REMCO AAGTJES
POLITIE TWENTE

9 VOORKOMEN DADERSCHAP CYBERCRIME

Doelstelling
Voorkomen daderschap cybercrime.

Project
Insteek is om te komen tot het ontmoedigen van daderschap van cybercrime. Vanuit Engeland is een preventieve aanpak ontwikkeld welke in Nederland geïmplementeerd kan 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. Er gaat hierbij indirect een preventieve werking naar de omgeving van de betrokken jeugdige, maar in alle gevallen gaat het wel om een repressieve inzet. De gesprekken worden gevoerd door politiefunctionarissen die daartoe een specifieke cursus hebben gevolgd. In deze gesprekken wordt verwezen naar relevante persberichten naar aanleiding van andere cybercrimedelicten. Hierbij wordt met name gewezen op de impact van cybercrime op slachtoffers, maar ook op de strafrechtelijke gevolgen voor de daders.

In Twente zal in het gehele district een pilot ingevoerd worden. Zoals gemeld zal de politie de interventies bij de jongeren gaan uitvoeren. Er heeft afstemming met het Openbaar Ministerie plaatsgevonden. Indien jongeren na afloop van deze interventie alsnog de fout in gaan (wederom betrokkenheid bij cybercrime), dan zal de politie daarvan proces-verbaal opmaken en zal het Openbaar Ministerie voorzien in een passende strafrechtelijke interventie.

Resultaat
Pilot Twente (Cease & Desist).

(mogelijke) Knelpunten
Beschikbare capaciteit politie.

Planning
Start pilot Twente 1 juni 2021. Eerste evaluatiemoment september 2021. Eindevaluatie voorjaar 2022.

PLATFORM IVZ
SAMEN STERK VOOR EEN VEILIG TWENTE

PARTNERS
- GEMEENTEN
- POLITIE
- JEUGDRECLASSERING
- RAAD VOOR DE KINDERBESCHERMING
- VNG
- VNON EXPERTTEAM JEUGD EN CRIMINALITEIT
- NJI
- CCV

CONTACTPERSOON
SYLVIA HUIS IN 'T VELD
REGIO-COÖRDINATOR
PLATFORM IVZ

10 OVERIGE ACTIVITEITEN DIGITALE CRIMINALITEIT

A City Deal Lokale Weerbaarheid Cybercrime

In deze City Deal gaan gemeenten, ministeries, veiligheids-organisaties, CCV en kennisinstellingen samen aan de slag om de digitale weerbaarheid te verhogen onder inwoners en bedrijven. Publieke en private koplopers gaan in de City Deal experimenteren met nieuwe aanpakken om de urgentie van cyberweerbaarheid over te brengen en om tot gedrags-verandering te komen. Toetreden aan de City Deal vanuit de regio Twente (IVZ Platform) was niet mogelijk. De resultaten van de City Deal zullen nauwlettend worden gevolgd en eventueel uitgevoerd in de regio Twente. In de City Deal is ook ruimte voor projecten op het gebied van bestuurlijke maatregelen gericht op de (online) openbare orde en veiligheid. Gemeenten kunnen geconfronteerd worden met openbare ordeverstoringen in de offline wereld, geïnitieerd en gevoed door ontwikkelingen in de online wereld. Burgemeesters hebben geen bevoegdheden om preventief online in te grijpen, maar kunnen toch bestuurlijk verantwoordelijk worden gehouden voor de gevolgen voor de openbare orde. Om burgemeesters handvatten te bieden om de (online) openbare orde en veiligheid te handhaven wordt er vanuit de regio IJsselland geëxperimenteerd. De APV is één van de maatregelen die onderzocht wordt. Om te bezien in hoeverre aanpassingen en/of nieuwe artikelen mogelijkheden bieden om een deel van online gedragingen binnen een gemeente te reguleren.

Bij online gedragingen valt te denken aan het online oproepen tot evenementen, de online oproep tot demonstraties. (Bron: notitie DVO IJsselland 10-2-2021).

Voorgaande ontwikkelingen worden door de expertgroep nagevolgd. Daarnaast is er regelmatig afstemming met de regio IJsselland.

10 OVERIGE ACTIVITEITEN DIGITALE CRIMINALITEIT

B Samenwerking activiteiten Saxion en Safety & Security Lab – Cyberweerbaarheid

In de aanpak van digitale criminaliteit hebben de expert-groep 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 dat bestaat uit:

1. Studentgroepen ter ondersteuning van gemeenten
   Groepen van studenten 'Integrale Veiligheidskunde' richten zich op de doelgroep(en) naar keuze van de opdracht-gevende gemeente en brengen passende bestaande interventies in beeld om de cyberweerbaarheid van de lokale samenleving of de eigen organisatie van de gemeente te vergroten en ontwikkelen een op maat communicatiestrategie. De animo onder studenten is echter bepalend voor de hoeveelheid projecten die van start kunnen.

2. Ontwikkeling van voorlichtingsmateriaal door een student-assistent
   Ontwikkelt in samenwerking met onder andere deelnemende gemeenten, de Fraudehelpdesk en de Hogeschool Saxion algemeen voorlichtingsmateriaal in begrijpelijke taal over wat is digitale criminaliteit en hoe kunt u zich ertegen beschermen. Dit wordt gedaan voor cybercriminaliteit in het algemeen, phishing in het algemeen, ransomware voor ondernemers, shame sexting en sextortion voor jongeren, money muling voor jongeren en internetoplichting voor senioren. Om deze activiteiten uit te kunnen voeren, is budget vanuit het Ministerie van BZK verkregen.

3. Aanvullend lokaal onderzoek naar de cyberweerbaarheid van de lokale samenleving.
   Zie project 4 Cyberweerbaarheidsmonitor hierboven.

PLATFORM IVZ
SAMEN STERK VOOR EEN VEILIG TWENTE

CONTACTPERSOON
LIESBETH HOLTERMAN
CYBERSECURITY EXPERT NOVEL-T

11 CYBERSECURITY QUICK SCAN ONDERNEMERS

Doelstelling
Middels de cybersecurity quick scan ondernemers concrete adviezen en handelingsperspectief bieden om de eigen organisatie cyberweerbaar te maken.

Project
Cybersecurity is voor veel MKB bedrijven in Overijssel nog niet ‘top of mind’. Door samenwerking met onder andere lokale gemeenten wil stichting Novel-T het onderwerp cybersecurity bespreekbaar maken én ondernemers op weg helpen met het in kaart brengen van hun belangrijkste cybersecurity risico’s. Dit doen we 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. Studenten van de Saxion worden ingezet om ervaring op te doen bij MKB bedrijven en hun cybersecurity skills te vergroten.

Resultaat
Door deze scan krijgt een bedrijf inzicht waar de sterke kanten zijn en waar nog aandachtspunten liggen. De scan wordt opgeleverd met een rapport dat inzicht geeft in korte, midden, en lange termijn oplossingen en het type maatregelen dat de onderneming zou moeten nemen om (nog) weerbaarder te worden. Middels een voucherregeling wordt 75% van de kosten vergoed waardoor de ondernemer een bedrag tussen de €250 en €500 betaald, afhankelijk van de grootte van de onderneming.

Planning
Eind 2022 moet het budget van provincie Overijssel op zijn (voucherregeling). Daarna mogelijke doorstart in samenwerking met Twentse gemeenten en onderwijs (studenten).

SAMEN STERK VOOR
EEN VEILIG TWENTE.

LOCATIE VEILIGHEIDSREGIO TWENTE
NIJVERHEIDSTRAAT 30, 7511 JM ENSCHEDE
POSTBUS 1400, 7500 BK ENSCHEDE

(088) 2567800
PLATFORMIVZ@VRTWENTE.NL