Actieprogramma aanpak digitale veiligheid 2023-2024

Gooi en vechtstreek

Inleiding

Voor u ligt het actieprogramma aanpak digitale veiligheid van het district Gooi en Vechtstreek. Dit actieprogramma is de leidraad in prioritering voor de Gooise gemeenten in samenwerking met politie en openbaar ministerie in de aanpak van digitale criminaliteit.

Digitale veiligheid is in alle Gooise gemeenten opgenomen als prioriteit in de integraal veiligheidsplannen (IVP). Ook landelijk zijn steeds meer gemeenten te zien die dit onderwerp als prioriteit agenderen, dit laat eens te meer de ernst van dit probleem zien. Naast de prioritering bij gemeenten is digitale veiligheid ook in de regionale veiligheidsstrategie 2023-2026 opgenomen als prioriteit.

De regionale aanpak en afspraken voor 2023 en 2024 staat in grote lijnen in dit document beschreven. Gemeente Hilversum is voorzitter van de werkoverleggen en bewaakt de voortgang in de interventies en samenwerking.

Context

Cybercrime is criminaliteit dat met behulp van ICT-apparatuur (computers, tablets, smartphones) gepleegd is, gericht op ICT apparatuur. Vormen van cybercrime zijn;

- Hacking, inbreken in computersystemen of netwerken
- Ransomware, kaapt je computersysteem door bijv. foto's te blokkeren, er wordt gevraagd om een geldbedrag zodat het systeem weer open wordt gezet.
- Virussen, een klein programma dat de werking van je computer verstoort. Een virus kan gegevens op je computer beschadigen of verwijderen, je e-mailprogramma gebruiken om zichzelf te verspreiden of zelfs je hele harde schijf wissen.

Naast cybercrime is er ook steeds vaker sprake van gedigitaliseerde criminaliteit. Dat zijn 'klassieke' delicten in een 'digitaal' jasje zoals;

- Online identiteitsfraude, hier maakt iemand misbruik van je persoonlijke gegevens. Onder je naam worden er producten of diensten besteld, uitkeringen of creditcards aangevraagd, betalingen gedaan of bankrekeningen geopend.
- Internetoplichting, denk hierbij aan fenomenen zoals marktplaatsoplichting waarbij iemand een bepaald product aanschaft maar vervolgens dit product niet ontvangt.
- Sexting / sextortion, verspreiden van een naaktfoto of erotisch tekstbericht (met of zonder toestemming). Vervolg van het versturen van dergelijke berichten kan zijn dat slachtoffers worden afgeperst of gechanteerd.

In dit actieprogramma wordt gesproken over digitale veiligheid omdat dit beide vormen van criminaliteit bevat.

De reden dat digitale veiligheid in alle IVP's is opgenomen komt doordat de cijfers laten zien dat deze vorm van criminaliteit de traditionele criminaliteit heeft ingehaald. Daarbij moet vermeld worden dat

digitale criminaliteit een erg complex en snel evoluerend onderwerp is waardoor exacte cijfers nog altijd niet beschikbaar zijn. Ook worden niet alle incidenten door slachtoffers gemeld, redenen hiervoor zijn schaamte, gebrek aan vertrouwen dat hun zaak wordt opgelost of gebrek aan kennis hoe zij meldingen kunnen doen. Er wordt momenteel hard gewerkt bij de politie om een up to date overzicht te creëren met cijfers van aangiftes. In dit programma wordt hier niet over gesproken omdat de beschikbare cijfers verouderd zijn en geen recht doen aan het daadwerkelijke probleem.

Doelgroep verdeling Gooi- en Vecht

Ondanks de geringe cijfers die momenteel beschikbaar zijn, tonen verschillende studies en rapportages aan dat er drie doelgroepen zijn die extra kwetsbaar zijn. In onze regio hebben wij daarom een doelgroepenverdeling gemaakt waarbij elke gemeente met extra focus aan de slag gaat. De verdeling is als volgt:

Doelgroep	**Gemeente**	**Ondersteuning door**
Jongeren	Hilversum, Huizen	
MKB	Wijdemeren, Gooise Meren	
Ouderen	BEL	Huizen & Hilversum

Redenen dat voor deze doelgroepen is gekozen zijn:

1. **Jongeren**: zijn een van de belangrijkste doelgroepen om digitale onveiligheid voor nu en de toekomst te kunnen verminderen. In 2021 was gemiddeld 1 op de 5 jongeren het slachtoffer van internetcriminelen, zij zijn daarmee vaker slachtoffer dan ouderen. Dit heeft onder andere te maken met de hoeveelheid tijd dat zij online actief zijn, de onwetendheid en onzorgvuldigheid. Bij de jongeren komt veel phishing, afpersing en sextortion voor. Hilversum heeft deze doelgroep als focus opgenomen.
   Naast het slachtofferschap bij jongeren wordt in deze doelgroep ook gekeken naar daderpreventie. Voorlichtingen en interventies dienen er voor te zorgen dat deze jongeren niet voor het snelle geld kiezen.
2. **Senioren**: in onze regio wonen relatief veel senioren. Zij zijn dan ook de doelgroep die, wanneer zij online actief zijn, het meest kwetsbaar zijn voor digitale onveiligheid. Denk bij deze doelgroep bijvoorbeeld aan de fenomenen phishing (hengelen naar inloggegevens per mail), hulpvraagfraude (whatsappfraude of vriend in noodfraude) en spoofing (een crimineel neemt een andere identiteit aan zoals een bank of bekende). Hier is al een recentelijk voorbeeld in gang gezet waarbij er bij een verzorgingshuis veel babbeltrucs (criminaliteit in combinatie met digitale component) voorkwamen en er een presentatie is gegeven door de politie. Bij senioren heerst ook een groot onveiligheidsgevoel aangezien het voor deze doelgroep een vrij onbekend terrein is maar zij toch steeds meer worden gedwongen om online zaken te regelen. Het is daarom een taak om ook hierop in te spelen en er zorg voor dragen dat er vertrouwen ontstaat in de digitale wereld.
3. **MKB**: voor ondernemers staat er veel op het spel wanneer zij te maken krijgen met digitale criminelen. Vaak worden er namelijk enorme bedragen buit gemaakt. Ook komt het veel voor dat ondernemers meerdere malen te maken krijgen met digitale aanvallen omdat gegevens zoals wachtwoorden worden verkocht op het dark web. Uit onderzoek van het CBS blijkt dat ongeveer 60% van de bedrijven in Nederland te maken krijgt met cybercrime met

een gemiddeld schadebedrag per bedrijf van € 340.500. Bij het MKB komt veel Ransomware (gijzelen en versleutelen van bestanden), Phishing en Ddos (enorme hoeveelheden data naar een site sturen waardoor deze overbelast en dus onbereikbaar wordt) voor.

Fenomenen

De bovengenoemde doelgroepverdeling zorgt ervoor dat er gerichte inzet plaatsvindt op deze kwetsbare groepen met bestaande interventies. Daarnaast is het echter van belang om ruimte over te houden voor nieuwe fenomenen. Zoals eerder genoemd is digitale veiligheid een snel evoluerend onderwerp waardoor ook hierop ingespeeld moet kunnen worden. Als er bijvoorbeeld een nieuwe tactiek ontstaat bij hacking en dit veel voorkomt in onze regio kunnen we gezamenlijk hier een aanpak op inzetten.
De samenwerking met politie is erg belangrijk om fenomenen of veelvoorkomende digitale criminaliteitsvormen boven water te krijgen. De politie werkt naar een overzicht toe wat elke zes weken gedeeld kan worden met de gemeentes. In dit overzicht wordt weergegeven wat voor meldingen er binnen zijn gekomen, om welke doelgroepen dit gaat en in welke buurten dit voorkomt. Op deze manier kunnen we als regio maatwerk inzetten door in te springen op veel voorkomende digitale criminaliteit per locatie door preventieve maatregelen in te zetten zoals bijvoorbeeld voorlichtingen.

Jaaragenda

Om de integrale samenwerking binnen gooi en vecht goed te benutten wordt er een jaaragenda ontwikkeld waarin vaste data worden ingepland om interventies uit te voeren. Zo wordt er voor gezorgd dat er minimaal een X aantal interventies per doelgroep plaatsvinden en de agenda's op elkaar zijn afgestemd. Ook communicatiecampagnes kunnen elkaar middels een jaaragenda versterken door tegelijk bepaalde berichten te delen. Naast de jaaragenda blijft ook ruimte bestaan voor fenomenen zoals in het vorige punt benoemd.

Partners

Het is de bedoeling dat wij vanuit de gemeentes aanjager worden op het onderwerp gedigitaliseerde criminaliteit en dat partners zelf verantwoordelijkheid nemen. Zo zal er de komende tijd veel samen worden gewerkt met scholen, verzorgingstehuizen en ondernemersverenigingen. De bedoeling is om een standaard neer te zetten en dusdanige samenwerkingsafspraken dat digitale veiligheid standaard bij verschillende partners wordt belegd. Dit is een kwestie van de lange adem maar moet er uiteindelijk voor zorgen dat er overal in de regio een minimale borging van dit onderwerp ingebed is.

Doel

In de regionale samenwerking hebben wij gemeenschappelijke doelstellingen, dit zijn:

- **Inzicht krijgen in het probleem**
  In samenwerking met de politie dienen cijfers steeds duidelijker te worden. Binnen de politie wordt er hard gewerkt om cijfers steeds meer te duiden en te labelen aan de juiste vorm van criminaliteit. Zo is het de bedoeling dat bijvoorbeeld marktplaatsfraude of telefonische babbeltrucs ook als zodanig geregistreerd worden. Elke zes weken deelt de politie de laatste

cijfers omtrent digitale veiligheid waardoor er een helder beeld ontstaat van de fenomenen op dat moment.

- **Verhogen aangiftebereidheid**
  Om ervoor te zorgen dat de politie beschikt over zoveel mogelijk informatie is het van belang dat er genoeg meldingen binnenkomen. De aangiftebereidheid rond digitale veiligheid ligt namelijk nog steeds erg laag, dit is een landelijk probleem. Binnen onze regio willen wij deze aangiftebereidheid verhogen door via communicatieboodschappen en presentaties aan te geven dat mensen zich niet moeten schamen en dat het doen van meldingen weldegelijk zin heeft. De cijfers vanuit de politie kunnen namelijk de koers bepalen hoe digitale veiligheid in Gooi en Vecht wordt opgepakt. Door te investeren in de aangiftebereidheid kan dit ertoe resulteren dat er meer meldingen van digitale criminaliteit worden gedaan. Dit staat haaks op het weerbaar maken van inwoners waarbij het doel is om als regio weerbaarder te worden. Als wij resultaten inzichtelijk maken kijken wij daarom niet alleen naar aangiftecijfers maar ook naar het gevoel van inwoners en het aantal interventies die wij hebben uitgevoerd.
- **Weerbaar maken inwoners**
  Met op elkaar afgestemde interventies en de doelgroep verdeling zorgen we er als regio voor dat er minimaal twee interventies per doelgroep plaatsvinden. Bij deze interventies is het doel om inwoners weerbaar en attent te maken op de veranderende criminaliteit en daarbij horende digitale gevaren. Ondanks dat we de meldingen dus omhoog willen krijgen gaan wij daarom ook voor een weerbare regio.
- **Handelingspersfectief bieden inwoners**
  Als onze inwoners, ondanks de interventies om hen weerbaar te maken, toch getroffen worden door digitale criminaliteit willen wij ervoor zorgen dat de gevolgen van een criminele aanval zo klein mogelijk blijven. Daarom is het ook van belang om bij inwoners duidelijk te maken wat zij wel of juist niet moeten doen als zij slachtoffer worden.

Overzicht activiteiten en projecten

Momenteel wordt er hard gewerkt aan uitvoeringsplannen en de jaaragenda. Daarom is het nog niet duidelijk welke interventies precies ingezet gaan worden. Ook is het mogelijk dat bepaalde interventies geschrapt of aangepast dienen te worden als deze niet het gewenste bereik hebben. Daarnaast moet er ruimte blijven voor de fenomenen waar op ingespeeld moet kunnen worden.

Doelgroep	**Projecten en activiteiten**	**Verwachte resultaat**	**Planning**	**Partijen**
Werkgroep Digitale Veiligheid Gooi en Vechtstreek	Project-voorbereiding	Gezamenlijke jaarplanning, gezamenlijke communcatie-campagnes, periodiek overleg.	2023 & 2024	Projectgroep gemeenten politie OM
Jongeren	Hackshield Cyber24	Bewuste jongeren tussen 8-12 jaar door de game Hackshield in en buiten de klas te spelen.	2023 2024	Gemeenten Boa's Politie Jongerenwerk

		Bewuste jongeren tussen 12-21 jaar door de koffers in de hele regio in te zetten.		
Senioren	Webinars, bijeenkomsten, trainingen en masterclasses	Bewustzijn, cyberweerbaarheid en handelingsperspectief vergroten. Er wordt gekeken naar landelijke initiatieven om deze via communicatiecampagnes te delen. Daarnaast worden ook eigen presentaties gegeven met de digitale wijkagenten.	2023	Seniorenverenigingen Gemeenten RVS
MKB	Storytelling	Ondernemers bewust maken van digitale gevaren door waargebeurde incidenten te laten vertellen door ondernemers.	2024	Ondernemers-verenigingen Gemeenten PVO
Communicatie	Gezamenlijke jaaragenda	Met een gezamenlijke agenda zorgen we ervoor dat er niet teveel interventies tegelijk plaatsvinden en gaan we gezamenlijk campagnes opzetten die elkaar versterken.	2023 & 2024	Gemeenten Politie

Financiën

Voor dit programma is nog geen budget geoormerkt bij de meeste gemeenten. Voorgesteld wordt om uit de reguliere middelen van openbare orde en veiligheid dekking te vinden voor het huidige plan van aanpak. Omdat de financiering van Digitale veiligheid en criminaliteit uit reguliere middelen zal worden gedekt, zal dit ten kosten gaan van andere verplichtingen (bijvoorbeeld jeugd of High Impact Crimes). Dit wordt binnen de eigen gemeente verantwoord.

In Q1 2024 worden de uitgevoerde interventies uit 2023 geëvalueerd met de daarbij horende kosten. Interventies die laag zijn in de kosten en een groot bereik hebben gehad zullen dan voortgezet / uitgebreid worden in de regio.