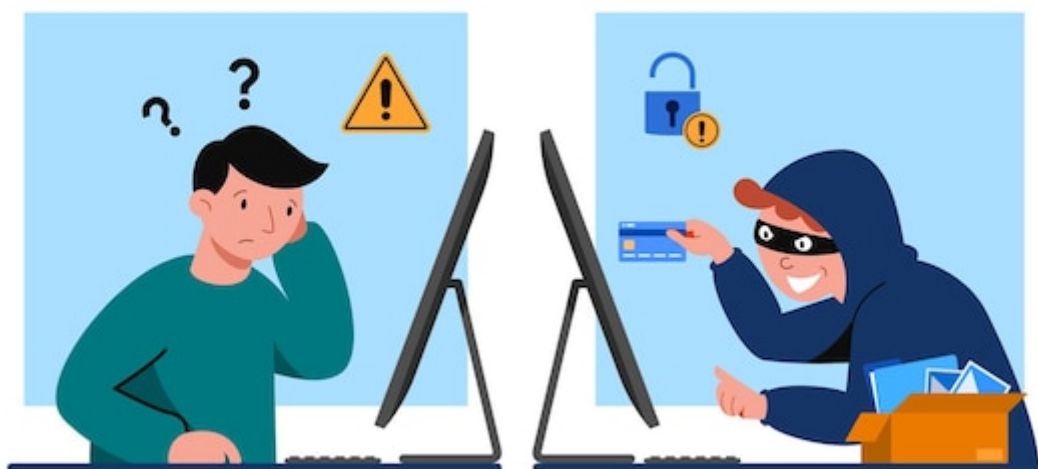




Plan van aanpak digitale criminaliteit 2023-2026

Plan van aanpak digitale criminaliteit 2023-2026

Dit is het Plan van aanpak digitale criminaliteit, een werkplan wat richting geeft aan de aanpak van deze vorm van criminaliteit. In het meerjarenplan veiligheidsplan (2022-2026) worden drie prioriteiten genoemd waarop de gemeente Diemen in deze periode zal inzetten. Eén van deze prioriteiten richt zich op digitale criminaliteit. Het Jaarplan van 2023 stelt dat in dit jaar extra aandacht zal worden geschonken aan dit thema. Dit stuk geeft invulling aan dat voornemen. *Digitale criminaliteit* valt binnen het bredere concept digitale veiligheid. Onder het concept digitale veiligheid vallen drie thema's, namelijk de digitale veiligheid (informatieveiligheid) van de eigen organisatie, digitale veiligheid in de context van crisisbeheersing en het tegengaan van slachtoffers van digitale criminaliteit. *Digitale criminaliteit* is een verzamelnaam voor een groot aantal criminele gedragingen. De diverse strafbare feiten hebben als gemeenschappelijke deler dat deze gepleegd worden met ICT of gericht zijn op ICT. Dit plan van aanpak richt zich primair op de personen en bedrijven met een hoger risico op slachtofferschap in de gemeente. Dit zijn: jongeren, ouderen en het midden- en kleinbedrijf (mkb). Per doelgroep worden een aantal actiepunten omschreven die bijdragen aan het verhogen van de weerbaarheid.

Jongeren

Voor jongeren wordt de focus gelegd op drie onderwerpen. Het ontwikkelen van vaardigheden voor veilig gedrag online, het voorkomen van misbruik van seksueel beeldmateriaal en geldezelen. Op basisscholen zal het programma HackShield weer actief onder de aandacht worden gebracht. Deze game leert kinderen over veilig internet gebruik en over digitale criminaliteit. Naast het stimuleren van HackShield op basisscholen zal aan stichting Halt gevraagd worden om actief voorlichting aan te bieden ten aanzien van digitale criminaliteit. Daarnaast zal aan zowel de kinderen- als de jongerenraad gevraagd worden om mee te denken over digitale criminaliteit. Tot slot, zullen er incidentele campagnes worden gelanceerd.

Ouderen

Voor ouderen wordt ingezet op digitale fraude, in het bijzonder vriend-in-noodfraude (WhatsAppfraude). Een initiatief is het opzetten van een netwerk van wijkambassadeurs. Wijkambassadeurs digitale veiligheid zijn vrijwilligers die zich inzetten voor het cyberveilig maken van Diemen. Zij zijn een vraagbaak voor bewoners en helpen bij het organiseren van evenementen. Zij kunnen ook een rol spelen bij het organiseren van activiteiten dicht bij huis. Dit kan gaan om computercursussen en veilig online winkelen maar ook hacken voor ouderen en het herkennen van oplichting. In aanvulling op incidentele informatiecampagnes zal een nieuwsbrief worden gestart voor geïnteresseerde bewoners (65+). Door middel van deze nieuwsbrief zullen bewoners, na aanmelding, op de hoogte worden gehouden van actualiteiten rondom digitale veiligheid.

Mkb

Bij het midden- en kleinbedrijf (mkb) wordt de nadruk gelegd op het verstrekken van voorlichting aan bedrijven om de weerbaarheid van hun medewerkers te vergroten en het bewustzijn over technische beveiligingsmaatregelen te verhogen. Hierbij speelt samenwerking met Ondernemersvereniging Ondernemend Diemen, het Platform Veilig Ondernemen-Amsterdam Amstelland (PVO-AA), het Digital Trust Center (DTC) en het team Ruimtelijk Beleid in het bijzonder de beleidsadviseurs economische zaken (kortweg: EZ) een belangrijke rol. Zo wordt de website van de gemeente aangepast om de informatie van het DTC aan te bieden aan de ondernemers. Verder zal samen met EZ aandacht voor het onderwerp komen via nieuwsbrieven en congressen. Het netwerk van EZ wordt bovendien gebruikt om training en voorlichting vanuit het PVO-AA te delen met de ondernemers.

Wij zijn ons bewust van de ontwikkelingen op dit thema, daarom is het belangrijk om te benadrukken dat dit een dynamisch werkdocument is. De focus of de prioriteiten zullen worden aangepast wanneer daar aanleiding toe is. In januari 2025 zal een geüpdatete versie van dit plan volgen.

Inhoud

Voorwoord.....	5
Digitale criminaliteit in cijfers (Gemeente Diemen)	6
Doelstelling.....	7
Aandacht voor alle ondernemers en bewoners van Diemen	7
Focus op de doelgroep	7
Jongeren	7
De in dit plan aangedragen interventies voor jeugd richten zich in het bijzonder op deze twee vormen van digitale criminaliteit. Ouderen	8
Mkb	8
Incidentele campagnes	8
Digitale veiligheid in de eigen organisatie	10
Digitale veiligheid in de crisisbeheersing	11
Training	11
Draaiboek gemeentelijk actiecentrum	11
Centraal meldpunt cybercrime.....	11
Jongeren en digitale criminaliteit	12
Wat kunnen we nog doen?	12
Actief promoten van Hackshield	12
Voorlichting Halt	13
Bespreken van digitale criminaliteit in de kinder-/jongerenraad	13
Ouderen en digitale criminaliteit	14
Wat kunnen we nog doen?	14
Wijkambassadeurs digitale veiligheid	14
Activiteiten dicht bij huis	14
Nieuwsbrief	15
Mkb en digitale criminaliteit.....	16
Wat kunnen we nog doen?	16
Platform Veilig Ondernemen Amsterdam-Amstelland	16
Samenwerking met het Digital Trust Center	16
Samenwerking met ondernemersvereniging Ondernemend Diemen, in contact met de ondernemer..	17
Tot slot	18

Voorwoord

In het meerjarenplan veiligheid (2022-2026) worden drie prioriteiten genoemd waarop de gemeente Diemen in deze periode zal inzetten. Eén van deze prioriteiten richt zich op digitale criminaliteit. Het Jaarplan van 2023 stelt dat in dit jaar een stap zal worden gezet op dit thema. Dit plan van aanpak digitale criminaliteit geeft invulling aan dit voornemen en dient als een leidraad voor de aanpak van deze vorm van criminaliteit.

Digitale criminaliteit is een verzamelnaam voor een groot aantal criminele gedragingen. Deze strafbare gedragingen hebben als gemeenschappelijke deler dat deze gepleegd worden met ICT of gericht zijn op ICT.¹ In het algemeen wordt een onderscheid gemaakt tussen *gedigitaliseerde criminaliteit* en *cybercriminaliteit*.

- Bij gedigitaliseerde criminaliteit maakt de crimineel gebruik van ICT middelen om traditionele delicten te plegen zoals oplichting en stalking.
- Bij cybercriminaliteit gaat het over (relatief) nieuwe strafbare feiten die niet alleen gebruik maken van de ICT maar ook gericht zijn op ICT. Bekende vormen zijn hacken van een account, Ransomware en DDOS-aanvallen.

In dit plan van aanpak zal gebruik worden gemaakt van het container begrip: digitale criminaliteit.

Digitale criminaliteit is onderdeel van het bredere thema digitale veiligheid. Onder digitale veiligheid vallen naast het voorkomen van digitale criminaliteit nog twee andere onderdelen. Allereerst de cyberveiligheid van de eigen organisatie. In andere woorden het voorkomen van kwetsbaarheden binnen de eigen organisatie en systemen. Dit wordt niet verder besproken in dit plan van aanpak omdat de informatieveiligheid wordt georganiseerd binnen Duo+. Ten tweede kennen we de cyberveiligheid in de context van ramp- en crisisbestrijding. Hiervoor worden de voorbereidingen getroffen door de 'gewone crisisorganisatie', dit gaat bijvoorbeeld om het trainen van de crisisorganisatie op cyber scenario's. OOV richt zich op het vergroten van weerbaarheid van bewoners en ondernemers. De gemeente ziet kansen in de preventie van digitale criminaliteit. De aanpak van reeds gepleegde digitale criminaliteit ligt bij de strafrechtketen, zij hebben de mogelijkheden om daders op te sporen en te vervolgen.

Tot slot, is digitale criminaliteit zonder twijfel een thema waarop zich in hoog tempo ontwikkelingen voordoen. De voortdurende digitalisering en voortschrijdende technologische vooruitgang creëren voortdurend nieuwe mogelijkheden voor criminelen. Bovendien staat dit onderwerp hoog op de landelijke veiligheidsagenda, wat leidt tot tal van diverse initiatieven. Wij zijn ons hiervan bewust, daarom is het belangrijk om te benadrukken dat dit een dynamisch werkdocument is. De focus of de prioriteiten zullen worden aangepast wanneer daar aanleiding toe is.

* De foto voorpagina is [hier](#) terug te vinden.

¹ ICT staat voor Informatie- en Communicatie Technologie.

Digitale criminaliteit in cijfers (Gemeente Diemen)

Helaas zijn er enkel beperkte cijfers beschikbaar die inzicht geven in dit fenomeen. Er wordt bestuurlijk op aangedrongen om hier verandering in te brengen. De wens is een goed dashboard met cijfers over dit fenomeen. Dit overzicht zou inzicht moeten verschaffen in de verschillende verschijningsvormen en ontwikkelingen op het gebied van digitale criminaliteit.

Op dit moment registreert de politie alleen de categorie 'oplichting en fraude'. In totaal zijn er in de periode van 1-1-2022 t/m 1-10-2023 **483** registraties opgenomen in het systeem van politie. De registraties kunnen niet cijfermatig worden uitgesplitst, de politie geeft wel aan wat de meest voorkomende incident-codes zijn:

- Fraude met onlinehandel
- Identiteitsfraude
- Horizontale fraude
- Telekomfraude
- Beleggingsfraude.
- Cybercrime
- Oplichting

Sextortion, is een vorm van afpersing en valt dus niet onder de bovengenoemde fraudes.

De precieze verhouding tussen de verschillende registraties kunnen op dit moment niet uit het systeem van politie gehaald worden.

Diemen	totaal '21	totaal '22	totaal '23
Fraude (betaal-, horizontale-, ID-, online handel, cyber)	191	92	114

Doelstelling

De gemeenteraad heeft in het meerjarenplan veiligheid de volgende doelstelling geformuleerd:

Meer aandacht voor het voorkomen van digitale criminaliteit.

Deze doelstelling benadrukt de rol van de gemeente in de preventie van digitale criminaliteit. De ambitie uit het meerjarenplan resulteert in de volgende doelstelling:

Digitale criminaliteit wordt tegengegaan door de weerbaarheid te vergroten van bewoners en ondernemers in de gemeente Diemen.

De ICT is onmisbaar geworden in het dagelijks leven van zowel bewoners als bedrijven. Dit betekent dat iedereen op elk moment slachtoffer zou kunnen worden van digitale criminaliteit. Daarom richt deze doelstelling zich in principe op alle bewoners en ondernemers binnen de gemeente. Desalniettemin geven verschillende studies aan dat er drie groepen zijn waarbij sprake is van een verhoogde kwetsbaarheid voor digitale criminaliteit: jongeren, ouderen en het midden- en kleinbedrijf (mkb). Van kwetsbaarheid is sprake wanneer er een verhoogd risico op slachtofferschap bestaat. Dit plan van aanpak richt zich primair op de personen en bedrijven met een hoger risico op slachtofferschap in de gemeente.

Aandacht voor alle ondernemers en bewoners van Diemen

Naast aandacht voor de risico doelgroepen zet de gemeente zich ook in op bewoners en ondernemers in de bredere zin. Zo zal er extra aandacht zijn voor dit thema op de Veiligheidsdag en de Week van de Veiligheid. Daarnaast zal de gemeente ook gebruik maken van incidentele campagnes. Deze campagnes worden door de gemeente verspreid via (sociale) media en de website. Maar eventueel ook via flyers, posters en ander fysiek campagne materiaal in de gemeente. Per campagne wordt gekeken wie de doelgroep is en hoe de doelgroep het beste bereikt kan worden. Is de doelgroep bijvoorbeeld jongeren, dan zullen digitale materialen en verspreiding via jongerenwerkers en scholen een belangrijke rol spelen. Terwijl dit bij ouderen eerder zal gaan om fysiek materiaal een verspreiding via de ouderenbond PCOB, stichting Welzijn Diemen, buurtcentra, bibliotheek en locaties als de Bredehoed. Deze campagnes kunnen dus gaan om een specifiek onderwerp zoals ransomware, maar ook meer algemene thema's zoals *digitale fraude*. Hierbij zal worden aangesloten bij de Nederlandse Cybersecurity Strategie van het ministerie van Justitie en Veiligheid. Digitale fraude is een vorm van digitale criminaliteit die elke bewoner, werknemer en ondernemer van de gemeente Diemen op elk moment kan treffen. Criminelen bouwen websites na van banken, grootwinkelbedrijven en pornosites. In alle gevallen probeert de oplichter het slachtoffer te verleiden zijn of haar inloggegevens in te typen. Met deze geheime gegevens kan de oplichter naar de echte website en onder de naam van het slachtoffer in te loggen. Op die manier kan de oplichter geld van de rekening afschrijven. Phishing is oplichting via het internet, er zijn verschillende varianten.

Focus op de doelgroep

Digitale criminaliteit is een breed begrip. Elk van de drie genoemde doelgroepen heeft een verhoogd risico bij specifieke misdrijven. Zo worden ouderen minder snel slachtoffer van sextortion dan jongeren, en het mkb sneller van ransomware dan jongeren. Mede daarom zal binnen de doelstelling focus worden aangebracht per doelgroep, gebaseerd op literatuuronderzoek.

Jongeren

Uit onderzoek blijkt dat jongeren (10-26 jaar) een verhoogd risico lopen om slachtoffer te worden van digitale criminaliteit. Dit gaat in het bijzonder om interpersoonlijke digitale criminaliteit, dit zijn strafbare feiten waar

de persoonlijke levenssfeer wordt aangetast. In het bijzonder gaat dit om twee type delicten: misbruik van seksueel beeldmateriaal en geldezelen.

- Misbruik van seksueel beeldmateriaal wordt ook wel **sextortion** genoemd. Sextortion is afpersing met een seksueel getinte foto of video van het slachtoffer. Dit kan een naaktfoto of video van het slachtoffer zijn, maar het kan ook zijn dat webcambeelden van iemand zo gemonteerd worden dat het lijkt alsof het om het slachtoffer gaat, zodat ook op deze manier gechanteerd wordt met het online zetten van materiaal.
- Bij **geldezelen** wordt de bankpas en de pincode van de jongere (de geldezel) uitgeleend aan criminelen die de bankrekening gebruiken om gestolen geld weg te sluizen. Geld dat ze van een andere rekening hebben gestolen, bijvoorbeeld door mensen op te lichten, storten ze op de rekening van het slachtoffer (de geldezel). Dan halen de criminelen het geld van de rekening met de geleende pinpas. Een geldezel maakt zich schuldig aan het strafbare feit witwassen en moet daarnaast al het gestolen geld terugbetalen. De criminelen zijn vervolgens spoorloos, zij kunnen over het weggesluisde geld beschikken zonder dat iemand weet dat zij erachter zitten. Vaak wordt over pinpasfraude gesproken.

De in dit plan aangedragen interventies voor jeugd richten zich in het bijzonder op deze twee vormen van digitale criminaliteit. Ouderen

Ouderen lopen een hoger risico om slachtoffer te worden van financiële digitale criminaliteit. Hierbij wordt door middel van ICT geld buitgemaakt. Een bekend fenomeen binnen deze doelgroep is vriend-in-noodfraude, ook wel WhatsApp-fraude genoemd.

- Bij **vriend-in-noodfraude** wordt het slachtoffer benaderd door een zogenaamd(e) vriend, familielid of bekende. Deze verstuurt een bericht dat hij of zij dringend financiële hulp nodig heeft. De bekende zit bijvoorbeeld zogenaamd in het buitenland vast en is zijn geld, telefoon en papieren kwijt. Of hij heeft zijn telefoon per ongeluk in de wasmachine gedaan en kan daarom niet internetbankieren. Deze 'bekende' vraagt om snel geld over te maken. Als hieraan wordt meegewerkt, volgt er vaak een tweede verzoek. Achteraf blijkt het account van deze vriend gehackt te zijn.

Mkb

Het midden- en kleinbedrijf (mkb) hebben een verhoogd risico om slachtoffer te worden van financiële en digitale criminaliteit en cybercriminaliteit. Bij financiële digitale criminaliteit zijn gelden en persoonlijke informatie het doelwit. Cybercriminaliteit is gericht op IT systemen, in het bijzonder gaat het hier om ransomware.

- Een populair middel bij cybercriminelen is **ransomware**. Dit is een vorm van ongewenste, kwaadaardige software (ook wel een virus genoemd), die alle bestanden van een bepaald bedrijf versleutelt. Het bedrijf kan de bestanden alleen terugkrijgen als er losgeld wordt betaald. Als de bestanden weer vrij worden gegeven is het onduidelijk wat precies met de bestanden is gebeurd tijdens deze 'gijzelingsperiode'.

Incidentele campagnes

Naast de gerichte interventies op specifieke doelgroepen zal de gemeente ook gebruik maken van incidentele campagnes. Deze campagnes worden door de gemeente verspreid via (sociale) media en de website. Maar eventueel ook via flyers, posters en ander fysiek campagne materiaal in de gemeente. Per campagne wordt gekeken hoe de doelgroep het beste bereikt kan worden. Is de doelgroep bijvoorbeeld jongeren, dan zullen digitale materialen en verspreiding via jongerenwerkers en scholen een belangrijke rol spelen. Terwijl dit bij

ouderen eerder zal gaan om fysiek materiaal een verspreiding via de bibliotheek en locaties als de Bredehoed. Deze campagnes kunnen dus gaan om een specifiek onderwerp zoals ransomware, maar ook meer algemene thema's zoals *digitale fraude*. Hierbij zal worden aangesloten bij de Nederlandse Cybersecurity Strategie van het ministerie van Justitie en Veiligheid. Digitale fraude is een vorm van digitale criminaliteit die elke bewoner, werknemer en ondernemer van de gemeente Diemen op elk moment kan treffen. Criminelen bouwen websites na van banken, grootwinkelbedrijven en pornosites. In alle gevallen probeert de oplichter het slachtoffer te verleiden zijn of haar inloggegevens in te typen. Met deze geheime gegevens kan de oplichter naar de echte website en onder de naam van het slachtoffer in te loggen. Op die manier kan de oplichter geld van de rekening afschrijven. Phishing is oplichting via het internet, er zijn verschillende varianten.

Digitale veiligheid in de eigen organisatie

De informatieveiligheid van de gemeente Diemen wordt georganiseerd vanuit het samenwerkingsverband Duo+. De uitvoering ligt bij de CISO, de FG en de Privacy Officers in samenwerking met de portefeuille houders (voor Diemen is dit Erik Boog) en de Gemeentesecretaris en de verantwoordelijke afdelingen

Vanuit Duo+ wordt voortdurend de verbinding gezocht met de organisatie. Zo wordt er aandacht besteed aan informatieveiligheid via Intercomm, krijgen medewerkers mailtjes en worden er presentaties en webinars gegeven. De medewerkers worden niet alleen geïnformeerd via deze weg, maar worden ook getoetst met bijvoorbeeld zogenaamde phishing mails. Als een medewerker toch onverhoopt op de link klikt wordt een korte training aangeboden om te voorkomen dat de medewerker bij een echte poging weer in de val trapt.

Jaarlijks wordt een *week van de informatieveiligheid* georganiseerd. Tijdens deze week worden er verschillende bijeenkomsten en activiteiten aangeboden.

Voor meer informatie kan gekeken worden op Intercomm of in het Tactisch en strategisch informatieveiligheidsbeleid.

Digitale veiligheid in de crisisbeheersing

Om tot een digitaal veilige gemeente te komen zijn er verschillende thema's die aandacht verdienen, waaronder cyber in de crisisbeheersing. Dit plan richt zich echter op de weerbaarheid van bewoners en ondernemers ten aanzien van digitale criminaliteit. Om tot een volledig beeld te komen van de maatregelen die binnen de gemeente Diemen genomen worden ten aanzien van digitale veiligheid wordt hier kort de crisisbeheersing besproken.

In de crisisbeheersing wordt de zogenoemde 'koude' fase onderscheiden van de 'warme fase'. In de warme fase gaat het om situaties waarbij sprake is van een acute ramp of crisis, en bij de koude fase om de voorbereiding en de nafase. Ten aanzien van beide fasen worden maatregelen getroffen ten aanzien van digitale veiligheid.

Training

Rampen en crises zijn gelukkig geen alledaagse gebeurtenissen in de gemeente. Daarom is oefenen en training van vitaal belang voor de crisisbeheersing. Bij de trainingen wordt een bepaald thema of scenario gekozen. Er heeft inmiddels een cyber scenariotraining plaatsgevonden. Hierbij kregen de deelnemers een beeld bij welke aspecten en vraagstukken spelen bij een ICT-crisis. Bijvoorbeeld wat is de beste manier om met elkaar in tijde van een ICT-crisis te overleggen. Bij deze trainingen wordt in het bijzonder stilgestaan bij de splitsing tussen het bestrijden van cybercrime en het nemen van maatregelen tegen de gevolgen ervan. Het openbaar bestuur houdt zich namelijk enkel bezig met de gevolgbestrijding, zoals het opvangen van slachtoffers. Voor het organiseren van deze trainingen werkt OOV samen met de CISO.

Draaiboek gemeentelijk actiecentrum

Wanneer sprake is van een incident kan de betrokken ambtenaar (liaison Amstellandgemeente) een beroep doen op het gemeentelijk actiecentrum. In het actiecentrum zitten ambtenaren van verschillende afdelingen, zij vormen de uitvoerende kant van de gemeente. Er is nu een speciaal draaiboek geschreven voor ICT-incidenten. Hierin wordt beschreven wie van welke gemeente bij elkaar moeten komen en wat de leden van het actiecentrum moeten doen bij een ICT-incident. De Duo+ organisatie beheert de techniek en regelt de inhoudelijke oplossing van de ICT-storing.

Opleidingstraject communicatiemedewerkers

Binnenkort gaat een opleidingstraject crisisbeheersing van start voor de medewerkers van communicatie. Het doel is om niet alleen de communicatiemedewerkers te trainen die piketdiensten draaien, maar juist om alle medewerkers van communicatie mee te nemen. In deze training wordt in het bijzonder aandacht besteed aan situaties waarbij de systemen niet meer werken of er gegevens zijn gestolen.

Centraal meldpunt cybercrime

De wens is om in de regio Amsterdam-Amstelland een gezamenlijk meldpunt te hebben voor ICT-incidenten. Enerzijds voor het delen van ervaringen ("wij hebben last van") en anderzijds het gezamenlijk zoeken naar oplossingen. Stel er komt een melding binnen van een aanval op een havenbedrijf in Amsterdam, dan kunnen bijvoorbeeld ICT'ers van de gemeente ter plaatse gaan om hen hulp te bieden. Dit is werk in uitvoering.

Jongeren en digitale criminaliteit

De eerste geprioriteerde doelgroep is jongeren. Dit zijn personen in de leeftijdsgroep van 10 tot 26 jaar. Jongeren zijn een bijzondere doelgroep, zij zijn namelijk vrijwel altijd online. Des te opmerkelijker is het dat zij zich niet altijd bewust zijn de risico's die zij lopen. In andere woorden zij onderschatten de kans dat zij zelf slachtoffer worden.² Daarnaast is er binnen deze doelgroep niet alleen bijzonder snel sprake van slachtofferschap maar ook van daderschap. Zo doen jongeren regelmatig strafbare dingen waarvan zij zich niet realiseren dat dit verboden is. ID-kaarten worden bijvoorbeeld regelmatig uitgeleend, an sich geen strafbaar feit, wél als daar vervolgens ID-fraude mee wordt gepleegd. Hetzelfde geldt voor uitgeleende bankpassen die gebruikt worden om crimineel geld weg te sluizen. Ook andere, ogenschijnlijk, onschuldige gedragingen, zoals het gebruik maken van iemands wachtwoord of het verspreiden van een pikante foto van een klasgenoot zijn strafbaar. Het is daarom belangrijk om bij deze groep zowel bewustzijn te creëren over slachtoffer- als daderschap. Activiteiten en voorlichting richten zich in het bijzonder op drie thema's: geldezelen, sextortion en veilig internet gebruik. Voor deze thema's wordt zowel landelijk als regionaal aandacht gevraagd.

Vanuit het team Sociaal (in het bijzonder jeugd en preventie, kortweg: sociaal) en het team Openbare Orde, Veiligheid en Vergunningen (in het bijzonder vanuit OOV, kortweg: OOV) is al een start gemaakt om in te zetten op jongeren en digitale criminaliteit. Zo heeft de gemeente vorig jaar het programma *HackShield* onder de aandacht gebracht van de Diemense basisscholen en wordt er aandacht besteed aan digitale criminaliteit op de veiligheidsdagen. Deze inzet is echter incidenteel en komt dus te kort in structuur en blijvende aandacht.

Wat kunnen we nog doen?

Actief promoten van Hackshield

[HackShield](#) leert kinderen zich spelenderwijs te wapenen tegen cybercriminaliteit. Via een spannend spel leren ze over de gevaren van internet en ontwikkelen ze skills waarmee ze deze gevaren tegen kunnen gaan. HackShield heeft als doel het creëren van een cyberveilige generatie, die zorgeloos over het web kan navigeren en jongeren (Junior Cyber Agents) die de oudere generaties hierin kunnen bijstaan. De gemeente Diemen maakt sinds vorig jaar gebruik van HackShield. In november 2023 heeft er een huldiging plaatsgevonden door de burgemeester op basisschool De Ark.³ Het eerste jaar was dus een succes, het is echter van groot belang dat dit niet een eenmalige actie is. De ervaring leert dat de basisscholen enige aansporing nodig hebben om met dergelijke initiatieven aan de slag te gaan, dus zal HackShield jaarlijks proactief aangeboden moeten worden bij de basisscholen. Daarbij hoort ook een echte huldiging.

Randvoorwaarden:

- Afstemming met team sociaal (jeugd en preventie)
- Afspraken met de basisscholen over gebruik Hackshield
- Vast agendapunt bij het scholenoverleg

² 'Cyber veilige inwoners', ccv.nl; Cyberweerbaarheid. Een gemeentelijk offensief ter preventie van slachtofferschap van cybercrime, 2022.

³ [Diemen huldigt de beste Cyber Agents - \(diemernieuws.nl\)](#)

Voorlichting Halt

De gemeente werkt samen met stichting Halt voor het organiseren van voorlichting op de zeven basisscholen. Halt biedt diverse voorlichtingspakketten, van vuurwerk tot de gevaren van het maken en delen van naaktfoto's. De basisscholen maken zelf de keuze waarover zij voorlichting willen van Halt. Op dit moment stuurt de gemeente stichting Halt dus nog niet in het aanbod. In overleg met team Sociaal zal de gemeente Halt een ambitie meegeven: volgend schooljaar op minimaal vier basisscholen voorlichting geven met een thema binnen digitale criminaliteit/veiligheid. Mogelijke trainingen zijn: Gedrag online, Voorlichting Sexting education en Geldezels.

Randvoorwaarden:

- Duurzame afstemming met team Sociaal (jeugd en preventie)
- Afspraken met stichting Halt
- Monitoring van de ambitie

Bespreken van digitale criminaliteit in de kinder-/jongerenraad

De gemeente Diemen beschikt over verschillende adviesraden, waaronder een kinder- en een jongerenraad. In de kinderraad zitten ongeveer 17 kinderen (twee kinderen uit groep 7 en 8 van elke basisschool in de gemeente Diemen). Samen praten zij over belangrijke onderwerpen voor kinderen in Diemen en oefenen zij invloed uit op de lokale politiek. Elk jaar wordt een nieuwe kinderraad samengesteld, het voorstel is dan ook om het onderwerp digitale criminaliteit jaarlijks op de agenda te zetten. Zodat jaarlijks gekeken kan worden of het nog gaat om de juiste onderwerpen en of er leuke creatieve manieren zijn om de kinderen in Diemen te bereiken. Naast een kinderraad is er ook een jongerenraad, deze bestaat uit zeven tot zeventien jongeren uit Diemen tussen 15 en 26 jaar. Ook bij deze adviesraad zal het thema worden geagendeerd. Hiervoor is het van belang om advies te vragen over hoe jongeren uit deze leeftijdsgroep bereikt kunnen worden door de gemeente.

Randvoorwaarden:

- Agenderen digitale criminaliteit kinderen-/jongerenraad

Ouderen en digitale criminaliteit

Daar waar jongeren zijn opgegroeid in een samenleving mét ICT, kan de gedigitaliseerde samenleving voor ouderen aanvoelen als een (digitaal) doolhof. Dit maakt deze groep kwetsbaar voor digitale criminaliteit. Criminelen maken gebruik van deze kwetsbaarheden door ouderen op verschillende manieren te benaderen, denk aan e-mail, telefonisch, SMS en chatapplicaties zoals WhatsApp en Facebookmessenger. Vooral tijdens de 'Corona-periode' zag de politie een stijging in het aantal oudere slachtoffers van vriend-in-noodfraude en verschillende vormen van phishing. Helaas blijkt de stijging in incidenten niet beperkt te blijven tot de Corona-periode. De politie ziet dat een aantal criminelen hun 'werkveld' hebben verlegd van criminaliteit in de fysieke wereld naar het plegen van strafbare feiten in de digitale wereld. Het is daarom van belang om te blijven inzetten op voorlichting voor deze doelgroep.

Naar aanleiding van de stijging tijdens de Corona-periode is de politie in samenwerking met de gemeente Diemen aan de slag gegaan met een uitvoerige informatiecampaigned voor de 65+ bewoners. Deze campagne resulteerde in een fijne samenwerking met een grootbereik. De sterke en verbeterpunten van deze campagne worden meegenomen in de interventies in dit plan.

Wat kunnen we nog doen?

Wijkambassadeurs digitale veiligheid

Samenwerking met en betrokkenheid van bewoners is onmisbaar in het informeren en bereiken van bewoners. Daarom is een van de aanbevelingen het ontwikkelen van een netwerk van wijkambassadeurs digitale veiligheid. Dit initiatief is ontstaan in de gemeente Breda en is later ook toegepast in Utrecht en Alkmaar. Deze wijkambassadeurs zijn vrijwilligers die zich inzetten voor het cyberveilig maken van Diemen. Alle vrijwilligers zijn woonachtig in Diemen, idealiter komen zij uit de verschillende wijken in de gemeente. Deze vrijwilligers fungeren als vraagbaak voor de wijk. De wijk kan bij hen terecht voor vragen als: hoe herken ik digitale criminaliteit? Hoe voorkom ik dat ik slachtoffer word? Waar kan ik meer informatie vinden over cybercrime? Enzovoorts. Bij het opzetten van de wijkambassadeurs kan gebruik gemaakt worden van de handreiking van gemeente de Utrecht. Zij hebben namelijk een document gemaakt wat andere gemeente helpt bij het overnemen van dit initiatief. Er zullen enige kosten gebonden zijn aan de start van dit initiatief, zo wordt voor de wijkambassadeurs een VOG aangevraagd, moeten wat materialen worden gemaakt zoals flyers, posters en eventueel jassen om de kenbaarheid van de wijkambassadeurs digitale veiligheid te vergroten.

Randvoorwaarden:

- | | |
|--|--|
| - Budget (incidenteel, circa €3500) | - Begeleiden en onderhouden van het vrijwilligersnetwerk |
| - Een project coördinator | |
| - Succes is afhankelijk van het aanbod aan vrijwilligers | - Kenbaarheid geven aan het project |

Activiteiten dicht bij huis

Voor deze doelgroep is het belangrijk dat er fysieke activiteiten dicht bij huis worden georganiseerd. Om dit mogelijk te maken zal er samen worden gewerkt met de PCOB, de buurt- en wijkverenigingen en de politie. Zo zullen er voorlichtingsbijeenkomsten moeten worden georganiseerd, zoals dit ook wordt gedaan op de Veiligheidsdag. Naast het actief informeren van de doelgroep is het van groot belang dat zij ook de mogelijkheid hebben om vaardigheden aan te leren. Verschillende partijen en partners bieden de mogelijkheid om activiteiten te organiseren om de weerbaarheid van ouderen te vergroten. Dit kan gaan om computercursussen en veilig online winkelen, maar ook ethisch hacken voor ouderen en het herkennen van

oplichting. De gemeente heeft een regierol in het beschikbaar stellen van dergelijke activiteiten. Hier kunnen eventueel de digitaal wijkagent en de wijkambassadeurs digitale veiligheid een rol in spelen.

Randvoorwaarden:

- Uitzoeken welke activiteiten beschikbaar zijn voor de (oudere) bewoners
- Jaarlijks opmaken van een (interne) activiteitenagenda

Nieuwsbrief

Na de stijging in het slachtofferschap van digitale criminaliteit onder ouderen heeft er een grote informatiecampagne gedraaid. In deze campagne heeft de politie in samenwerking met de gemeente Diemen op verschillende manieren bewoners proberen te bereiken. Een van deze wegen was het aanschrijven van alle 65+ bewoners die nog zelfstandig woonden. Dit is weliswaar een grote investering, maar juist uitgevoerd, kan dit tot mooie resultaten leiden. Bovenal omdat er elk jaar nieuwe bewoners in deze doelgroep vallen. Het is echter arbeids- en kostenintensief om dit steeds opnieuw op te zetten. Daarom is het wenselijk om met een nieuwsbrief systeem te werken, dit doet de gemeente al voor ondernemers. Eenmalig wordt deze doelgroep weer geselecteerd en aangeschreven. In deze brief wordt de ontvanger de mogelijkheid geboden om zich aan te melden voor een kennisnetwerk, in principe via de mail maar eventueel ook via de post. Wanneer een bewoner zich aanmeldt voor dit netwerk zal deze een aantal keer per jaar informatie ontvangen. Dit kan bijvoorbeeld gaan om voorlichting over nieuwe oplichtmethodes, informatieve flyers en uitnodigingen voor cursussen of webinars. Op deze manier bereik je de personen die geïnteresseerd zijn in het thema en hoeft niet steeds weer een nieuwe lijst gemaakt te worden.

Als alternatief kan er gebruik worden gemaakt van de nieuwsbrieven van de ouderenbond, PCOB en Stichting Welzijn Diemen.

Randvoorwaarden:

- Eerste mailing na selectie
- Registratiesysteem
- Jaarlijks opmaken van een informatiekalender
- Elke twee jaar een nieuwe mailing naar iedereen om op te geven

Mkb en digitale criminaliteit

Het midden- en kleinbedrijf, kortgezegd het mkb, is de drijvende motor van de Nederlandse economie. Onder het mkb vallen alle bedrijven met een maximum van 250 medewerkers en een jaaromzet van maximaal €50 miljoen. In verschillende onderzoeken komt de kwetsbaarheid ten aanzien van digitale criminaliteit van deze doelgroep naar voren. Deze bedrijven vormen een aantrekkelijk doelwit voor digitale criminaliteit aangezien zij vaak matige of zelfs onvoldoende beveiligingsmaatregelen treffen. De financiële middelen van deze bedrijven zijn zowel direct als indirect het doelwit van de criminelen. Het geld van de onderneming kan worden buitgemaakt via fraude, bijvoorbeeld collega-in-noodfraude of vormen van phishing. Bij het voorkomen van deze vorm van criminaliteit staat de weerbaarheid van de persoon centraal, is de werknemer zich bewust van het feit dat hier sprake is van een poging tot phishing. Naast deze directe manier is ransomware een voorbeeld van een indirecte manier waarbij criminelen bedrijven geld afhandig maken. Bij het voorkomen van deze vorm van cyber criminaliteit zijn de technische maatregelen die een bedrijf neemt van groot belang. Om het bewustzijn van het mkb te vergroten zijn verschillende initiatieven gestart, waaronder het *digital trust center*, van het ministerie van economische zaken en klimaat.⁴

De gemeente zet zich al in voor de digitale weerbaarheid van het mkb in Diemen. Zo werkt de gemeente samen met het Platform veilig ondernemen Amsterdam-Amstelland (PVO-AA). Het PVO-AA is een privaat-publieke samenwerking waar het bedrijfsleven samen met de gemeente, politie en OM werkt aan een veilig ondernemersklimaat in de regio. Een van de onderwerpen waar zij aandacht aan besteden is digitale criminaliteit. Acties vanuit het PVO-AA bestaan uit voorlichting en training. Tot slot, wordt op de veiligheidsdagen ook aandacht besteed aan digitale veiligheid van ondernemers.

Wat kunnen we nog doen?

Platform Veilig Ondernemen Amsterdam-Amstelland

Onder meer door de aandacht van de gemeente Diemen voor digitale criminaliteit zal het PVO-AA zich komend jaar verder ontwikkelen op het thema van digitale criminaliteit. Samen met het PVO-AA wordt onderzocht hoe de digitale weerbaarheid van ondernemers in Diemen structureel en duurzaam kan worden vergroot. Er zullen in 2024 verschillende activiteiten worden georganiseerd zoals ondernemerscolleges en trainingen. Wanneer de planning bekend is zullen de activiteiten via de ondernemersnieuwsbrief worden gedeeld met de ondernemers. Daarnaast wordt onderzocht in hoeverre gebruik gemaakt kan worden van 'De Cybermonitor', een kant en klare training ontwikkeld door het PVO Midden-Nederland die organisaties inzicht geeft in basis risico's op mensen en techniek.⁵

Samenwerking met het Digital Trust Center

Het Digital Trust Center (DTC) biedt verschillende onlinemiddelen aan waarmee ondernemers het risico- en veiligheidsniveau kunnen bepalen van hun onderneming. Dit zijn nuttige 'tools' die de ondernemer in Diemen verder kunnen helpen, zowel in het voorkomen van slachtofferschap als in het bieden van een handelingskader bij slachtofferschap. De gemeente Diemen biedt al informatie aan voor ondernemers op de website, hier wordt een categorie 'digitale criminaliteit' aan toegevoegd. Waarin ondernemers naast voorlichting de tools van het DTC kunnen vinden. Bovendien werkt het DTC met een landelijk dekkend stelsel

⁴ [Home | Digital Trust Center \(Min. van EZK\)](#)

⁵ [Eerste vijftien bedrijven in Veenendaal halen het Cybercertificaat - \(pvo-middennederland.nl\)](#)

van samenwerkingen op het gebied van cyberweerbaarheid, waar de gemeente Diemen uiteraard deel van zal uitmaken.

Randvoorwaarden

- Aanmelden community DTC
- Aanpassen website van de gemeente Diemen
- Bijhouden aangeboden informatie

Samenwerking met ondernemersvereniging Ondernemend Diemen, in contact met de ondernemer

De gemeente heeft goed contact met de ondernemersvereniging Ondernemend Diemen. Wij willen dit goede contact gebruiken om de samenwerking te zoeken met de ondernemers in Diemen. Naast de samenwerking met de ondernemersvereniging is ook interne samenwerking van belang tussen OOV en Team Ruimtelijk Beleid, in het bijzonder de beleidsadviseurs Economische Zaken. Dit doen zij onder andere door middel van een nieuwsbrief en het organiseren van een jaarlijkse bijeenkomst met de ondernemersvereniging. OOV heeft hier eerder nog geen nadrukkelijke rol gespeeld in het aandragen van thema's. In november 2024 wordt weer een bijeenkomst georganiseerd, de bedoeling is om hier aandacht te vragen voor het thema digitale criminaliteit. Hierbij zal ook de samenwerking worden gezocht met het PVO-AA. Daarnaast zal EZ nadrukkelijker aandacht besteden aan digitale criminaliteit in de periodieke nieuwsbrief gericht aan de ondernemers in Diemen. Tot slot, zal de samenwerking tussen EZ, PVO-AA en OOV ervoor moeten zorgen dat de ondernemers in Diemen toegang hebben en op de hoogte zijn van alle lokale en regionale projecten, initiatieven en activiteiten met het thema digitale criminaliteit.

Tot slot

Dit plan van aanpak heeft als doel richting en structuur te geven aan de aanpak van digitale criminaliteit in de gemeente Diemen. Bovendien zijn er nog een aantal zaken die benoemd horen te worden die niet direct paste bij de bespreking van de drie doelgroepen. Deze zullen kort worden besproken.

Het basisteam van de politie is ook bezig met zich te ontwikkelen op het gebied van digitale criminaliteit. Zo is er sinds kort een digitale wijkagent aanwezig. De digitale wijkagent heeft naast zijn gebruikelijke politiewerk de ruimte om te werken aan de digitale veiligheid van de bewoners en ondernemers van de gemeente Diemen. Dit doet hij door voorlichting te geven, maar ook door online onderzoek. De digitale wijkagent is meegenomen bij het schrijven van dit plan van aanpak en zal ondersteunen waar mogelijk.

Ook op bestuurlijk niveau is er aandacht voor dit onderwerp. Het is bijvoorbeeld een aandachtspunt voor de lokale driehoek. Bij de lokale driehoek komen de burgemeesters van Diemen en Ouder-Amstel samen met de politie en het openbaar ministerie. Daarnaast is er een speciale cyber sub driehoek voor de regio Amsterdam-Amstelland, tevens een samenwerking tussen politie, gemeenten en het openbaar ministerie. Diemen is ambtelijk aangesloten bij deze cyber sub.

Daarnaast zal er altijd gekeken worden naar hoe incidenteel en ad hoc aandacht kan worden gevraagd voor dit onderwerp. Dit kan zijn door aan te sluiten bij landelijke campagnes maar ook de inzet van het mobiel media lab van de politie. Het mobiel media lab is een grote vrachtwagen die ingericht kan worden naar een bepaald onderwerp, hier kunnen bewoners en ondernemers dan naar binnen lopen. Op de Veiligheidsdag is deze bus al een keer aanwezig geweest in Diemen, hier zijn veel positieve reacties op gekomen.

Tot slot, is dit een dynamisch document. De focus of de prioriteiten zullen worden aangepast wanneer daar aanleiding toe is. In januari 2025 zal een geüpdatete versie van dit plan volgen.