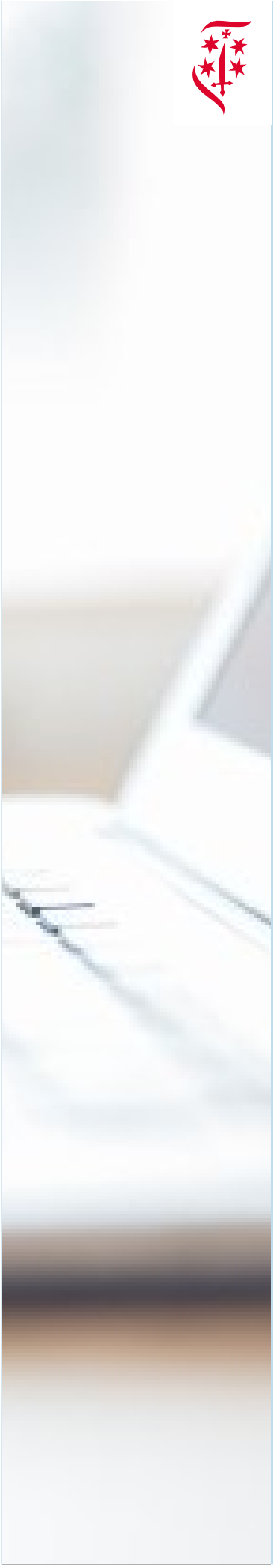
Gemeente Haarlem



Aanpak cybercriminaliteit en digitale veiligheid

27 oktober 2020

Lynn van Meijgaard
Afdeling Veiligheid & Handhaving

Inhoudsopgave

1. Inleiding

In de afgelopen twee jaar zijn begrippen als digitale veiligheid en cybercriminaliteit snel opgekomen in het gemeentelijke veiligheidsdomein. Cybercriminaliteit heeft zich inmiddels dusdanig doorontwikkeld dat bijna elke vorm van criminaliteit een digitale variant kent. Steeds meer vormen van cybercriminaliteit, zowel op internationaal als op lokaal niveau, raken inwoners en ondernemers in gemeente Haarlem. Denk hierbij aan sexting, phishing-mails en online oplichting. Dat cybercriminaliteit een aanzienlijk probleem is wil echter niet zeggen dat dit zorgt voor meer onveiligheid in Haarlem. Het aantal slachtoffers van digitale delicten stijgt, terwijl het aantal slachtoffers van 'normale' criminaliteit daalt. Het is voor criminelen vaak voordelig om via het internet criminaliteit te plegen omdat criminelen op het internet een groot bereik hebben, er weinig toezicht is en een kleine pakkans hebben.

Deze rapportage is bedoeld om inzicht te geven in het begrip digitale veiligheid en cybercriminaliteit, bezien vanuit het gemeentelijke perspectief. Enerzijds schetst het een beeld van de reikwijdte van cybercriminaliteit en digitale veiligheid binnen de gemeentegrenzen. De rapportage gaat daarbij in op de raakvlakken van cybercriminaliteit en digitale onveiligheid met het werkveld van de openbare orde en veiligheid in Haarlem. Anderzijds wordt ingegaan op de Haarlemse aanpak van cybercriminaliteit. Onze lokale rol kenmerkt zich door inzet op bewustwording, het verhogen van de weerbaarheid bij inwoners en ondernemers en inzet op daderpreventie.

Cybercrime kent, naast een lokale aanpak, ook een regionale aanpak waarop gemeente Haarlem is aangesloten. In het Integraal Meerjarenbeleidsplan Veiligheid (IMV) 2019-2022 is cybercrime als een regionale prioriteit van de eenheid Noord-Holland benoemd. In het projectteam van Noord Holland Samen Veilig (NHSV) wordt met politie, 34 gemeenten en het openbaar ministerie samengewerkt op het thema cybercrime. Regionaal wordt ingezet op (1) het vergroten van de digitale weerbaarheid van de jeugd, (2) het versterken van de informatiebeveiliging van gemeenten, (3) de organisatie van trainingen en webinars om expertise op gebied van cyber bij ambtenaren te vergroten en (4) de ontwikkeling van rapportages die inzicht bieden in de grootte van het probleem.

Wat is cybercriminaliteit?
Criminaliteit waarbij men een computersysteem aanvalt of misbruikt voor criminele activiteiten. Net als ondermijning is het een containerbegrip. Cybercriminaliteit omvat verschillende type online delicten zoals bedreiging, fraude, smaad, hacken, witwassen en stalking.

Grofweg wordt er onderscheid gemaakt tussen twee type cyberdelicten, namelijk:

1. Cybercriminaliteit in brede zin. Dit zijn alle strafbare activiteiten waarbij iemand een informatiesysteem of computer gebruikt. Denk aan diefstal en vervalsing van betaalpassen, oplichting, afpersing, kinderporno, slachtofferschap door sexting, racisme en belediging.
2. Cybercriminaliteit in enge zin. Ook wel cybercrime genoemd. Hierbij gebruikt men informatiesystemen en computers niet alleen als middel, maar zijn ze ook een doel. Bij *cybercrime* gaat het om misdaad gepleegd met ICT, gericht op ICT. Het strafbare feit wordt dus gepleegd met een computer, smartphone, smartwatch of tablet, kortom alles waar een processor in zit. Cybercrime voorbeelden zijn hacking, DDoS-aanvallen, ransomware, virussen, malware, enzovoort.

2. Beeld

Haarlemmers zijn steeds vaker slachtoffer van cybercriminaliteit. In 2019 is 14,6% van de Haarlemmers slachtoffer geworden van cybercriminaliteit. Evenals het slachtofferschap van traditionele criminaliteit varieert het slachtofferschap van cybercriminaliteit naar leeftijd. Ook hier is het totaalbeeld dat jongere leeftijdsgroepen vaker slachtoffer zijn dan oudere generaties. De groei van cybercriminaliteit is een landelijke trend. Het CBS vermeldt dat het slachtofferpercentage van de 70.000+ gemeenten in Haarlem met 1,6% hoger ligt dan het landelijk gemiddelde (CBS, 2020). Dit komt voornamelijk doordat Haarlemmers vaker slachtoffer worden van aan- en verkoopfraude dan gemiddeld (zie pagina 5).

Vaak wordt gesproken van “cybercriminaliteit” als zijnde één type delict, maar dat is niet helemaal juist. Cybercriminaliteit kent veel vormen. Daardoor wordt het zo langzamerhand een containerbegrip voor alle strafbare activiteiten waarbij een crimineel een computer, telefoon of informatiesysteem gebruikt. Door de reikwijdte van cybercriminaliteit is het een uitdaging een compact beeld te schetsen op de digitale veiligheid in Haarlem. Daarom wordt bij het beeld ingegaan op de meest voorkomende cyberdelicten in de voor gemeenten bekende veiligheidsvelden. Deze velden zijn ontwikkeld door de Vereniging van Nederlandse Gemeenten (VNG) en laten zien hoe cybercriminaliteit zich manifesteert in elk veiligheidsveld. Ze worden ook gebruikt in de Veiligheidsanalyse 2018 en het Integraal Veiligheids- en Handhavingsbeleid 2019-2022.

Er wordt onderscheid gemaakt tussen vijf veiligheidsvelden, namelijk:

1. Veilige woon- & leefomgeving

2. Bedrijvigheid & veiligheid

3.Jeugd& veiligheid

4. Fysieke veiligheid & crisisbeheersing

5. Integriteit & veiligheid

Deze rapportage is opgebouwd aan de hand van bovenstaande veiligheidsvelden. Bij de totstandkoming van het beeld is gebruik gemaakt van de veiligheidsmonitor van het CBS en verhalen van geanonimiseerde Haarlemmers. Ook is gebruik gemaakt van binnengekomen aangiften en meldingen bij de politie. Deze cijfers zijn echter niet leidend omdat de aangiftebereidheid bij cybercriminaliteit over het algemeen vrij laag is en varieert per type delict.

Bij sommige delicten zoals hacken en sexting doen maar weinig slachtoffers aangifte. Bij andere delicten zoals online aan- en verkoopfraude ligt dit percentage vijf keer zo hoog. Daardoor ontstaan misvattingen over de grootte van de problematiek en ontstaat een scheef beeld. Daarnaast geven registraties van de aangiftes bij de politie vaak een vertekend beeld. Digitale en klassieke vormen van criminaliteit lopen vaak dwars door elkaar heen. Neem als voorbeeld dit filmpje, waarbij het de vraag is of dit wordt geregistreerd onder cybercriminaliteit of autodiefstal?

2.1 Veilige woon- en leefomgeving

Leven in een omgeving waar je je veilig voelt, is voor veel mensen erg belangrijk. Incidenten zoals overlast, inbraken en oplichting hebben een negatieve invloed op de veiligheid in de woon- en leefomgeving. Tot zo'n 25 jaar geleden speelde dit soort problematiek zich vooral af in de "fysieke wereld". Door de digitalisering is te zien dat leefbaarheidsproblematiek en criminaliteit zich deels hebben verplaatst naar het digitale domein. Dit veiligheidsveld gaat in op vier veelvoorkomende vormen van cybercriminaliteit in de woon- en leefomgeving van inwoners, namelijk: helpdeskfraude, phishing, hacken en vriend-in-nood-fraude.

Helpdeskfraude/digitale babbeltrucs
Een van de meest voorkomende vormen van cybercriminaliteit is helpdeskfraude. Vooral 58-plussers worden slachtoffer van helpdeskfraude (politie, 2020). Bij deze vorm van fraude doet de dader zich voor als een medewerker van een softwarebedrijf en overtuigt het slachtoffer dat zijn/haar computer problemen heeft. Vervolgens is de dader bereid om tegen betaling het niet-bestaande probleem te verhelpen en installeert hij/zij software op de computer van het slachtoffer waardoor de dader toegang krijgt tot de computer van het slachtoffer. De dader kan vervolgens de computer van het slachtoffer overnemen, bestanden gijzelen en bankrekeningen plunderen. Jaarlijks doen 10 tot 30 Haarlemmers aangifte van helpdeskfraude bij de politie. Vermoedelijk ligt het daadwerkelijke aantal slachtoffers een stuk hoger.

Een 74-jarige inwoonster uit Haarlem werd op haar huistelefoon gebeld door een Engels sprekende man, met Indiaas accent. De man deed zich voor als een werknemer van Microsoft en vertelde dat haar laptop problemen had. De man gaf aan haar laptop te kunnen maken voor een geldbedrag van slechts 9 euro. Hier ging de vrouw mee akkoord. De man nam op afstand de besturing van haar laptop over en uiteindelijk raakte de vrouw, door een bankoverboeking op afstand, niet door haar gegeven, een aanzienlijk geldbedrag kwijt.

Phishing
Phishing is een vorm van digitale oplichting en gebeurt via e-mail, WhatsApp en sms. Vaak worden de slachtoffers naar een valse website gelokt waar ze betaalgegevens of persoonlijke gegevens achterlaten. Volgens CBS (2020) is het afgelopen jaar 0,5% van de Haarlemmers (15+) slachtoffer geworden van phishing. Dit zijn dat zo'n 677 Haarlemse slachtoffers in slechts één jaar tijd.

Een 55-jarige Haarlemmer ontving een e-mail van de ING bank. Deze e-mail leek heel erg op de ING e-mails die hij vaker als ING klant ontvangt. In de geopende mail komt de man op een website en leest hij dat hij zijn kaartnummer en bankpasnummer moet verifiëren. Via een ontvangen SMS bericht, met hierin TAN-codes, die hij vervolgens invult op de website, raakt hij ongewild een flink geldbedrag kwijt.

Vriend-in-nood-fraude
Sinds de coronacrisis is fraude via WhatsApp flink toegenomen, zo meldt de politie-eenheid NH. De 'vriend-in-nood-fraude' is een relatief nieuwe vorm van internetoplichting, waarbij de ontvanger een appje van een familielid of vriend ontvangt. Die zegt een nieuw nummer te hebben, even met een noodsituatie zit en vraagt om met spoed geld over te maken. Het is onbekend hoeveel Haarlemmers de afgelopen periode slachtoffer zijn geworden.

Hacken
5.9% van de Haarlemmers is het afgelopen jaar gehackt. Bij hacking probeert iemand binnen te dringen in andermans computer. Doel van de criminele hacker is de computer overnemen of gegevens stelen of onbruikbaar maken. Bij de meeste Haarlemmers (2,2%) wordt ingebroken op een website/profielsite. Daarnaast geeft 1,9 % van de Haarlemmers aan dat er ingebroken wordt op het emailaccount en bij 0,4% op de computer (CBS, 2020).

2.2 Veilig ondernemen

In dit hoofdstuk wordt uiteengezet voor welke vormen van cybercrime consumenten en ondernemers kwetsbaar zijn. Daarnaast wordt ingegaan op hoe online oproepen tot fysieke evenementen de openbare orde en veiligheid in gevaar kunnen brengen.

Veilige online winkelen
Een van de grootste stijgers binnen het cyberdomein is aan- en verkoopfraude. In de meeste gevallen koopt het slachtoffer bij dit type fraude online een product, maar krijgt hij/zij dit product niet geleverd. In twee jaar tijd (2017-2019) is het aantal slachtoffers met 95% gestegen. In 2019 is 5,5% van de Haarlemmers slachtoffer geworden van aan- en verkoopfraude (CBS, 2020). De meeste slachtoffers zijn tussen de 22 en 56 jaar. Haarlemmers die ouder zijn dan 72 jaar worden zelden slachtoffer van aan- en verkoopfraude. In 2019 hebben 622 Haarlemmers aangifte gedaan van aan- en verkoopfraude. Volgens het CBS (2020) doen Haarlemmers vaker (7,3% boven het gemiddelde) aangifte bij de politie dan andere Nederlanders.

> Een 38-jarige vrouw uit Haarlem werd verdacht van het plegen van identiteitsfraude, gepleegd via internet. Zij maakte gebruik van andermans identiteit en bestelde artikelen op diverse consumentenwebsites. Zij liet de artikelen afleveren (met de mogelijkheid: achteraf betalen) bij een afhaalpunt van DHL of Post NL. Nadat zij deze artikelen had opgehaald, wilden de webwinkels op later moment geld incasseren en bleek dat de rekening terecht kwam bij nietsvermoedende burgers in Haarlem, waarvan hun identiteit was gebruikt. Na uitgebreid onderzoek door de politie is de vrouw aangehouden.

Een andere veelvoorkomende vorm van cybercriminaliteit is misbruik van accounts voor bestellingen. Digitale criminelen maken gebruik van inloggegevens uit uitgelekte databases en verkopen grote aantallen accounts. Zodoende worden op de gehackte accounts bestellingen geplaatst voor dure producten waarna de factuur bij de eigenaar van het account terecht komt. Een nieuwe variant “misbruik accounts voor bestellingen” wordt sinds 2019 waargenomen. Hierbij worden nieuwe accounts geregistreerd met de gegevens van het slachtoffer. Op deze accounts worden net als bij gehackte accounts aankopen op afbetaling gedaan. Dit type delict komt voor bij alle generaties, met uitzondering van de generatie van 73+. Zij kopen minder via het internet.

Veilige bedrijven: slachtofferschap bij ondernemers
Hoewel veel ondernemers denken dat cybercriminelen vaak alleen grote bedrijven aanvallen, is dat juist niet het geval. Mkb-ondernemers wanen zich vaak ten onrechte veilig omdat ze denken dat bij hen betrekkelijk weinig valt te halen. Het tegendeel is waar, mkb’ers worden maar al te vaak slachtoffer, omdat ze hun beveiliging niet op orde hebben. Uit een enquêtes van het Regionaal Platform Criminaliteitsbeheersing (51 respondenten), blijkt dat behoorlijk wat Haarlemse ondernemers denken dat het belang van digitale veiligheid niet van toepassing is op hun bedrijf omdat zij zich te klein of niet belangrijk vinden. Dit ten onrechte, want 93% van de respondenten heeft een website, 70% slaat data op van klanten en 29% van de respondenten heeft een webshop.

Maar liefst 30% van de Nederlandse ondernemers werd in 2019 slachtoffer van cybercrime, zo blijkt uit het Cybersecurity Onderzoek van Centraal Beheer. Het grootste gevaar komt van phishing: mails die nauwelijks van echt zijn te onderscheiden. Door op een 'valse' link te klikken wordt malware binnengehaald, waarna de ellende begint. Ook ransomware – kwaadaardige software die een computer in gijzeling neemt – vormt een gevaar voor ondernemers. Pas na betaling van losgeld worden bestanden weer toegankelijk. Hackers eisen gemiddeld 5330 euro losgeld (KPN, 2020).

Een 51-jarige man uit Sneek doet aangifte van digitale fraude. Hij is de eigenaar van een bedrijf dat een speciale applicatie (APP) ontwikkeld. Voor de verdere ontwikkeling van deze app, konden investeerders zich aanmelden om obligaties te kopen. Een fraudeur heeft de website nagemaakt, waardoor geïnteresseerde investeerders daadwerkelijk dachten de correcte website te bezoeken. Ook deed de fraudeur zich telefonisch voor als de eigenaar van het bedrijf. Benadeelden zijn voor bedragen tussen de € 5000 en € 85.000 benadeeld. Uit onderzoek door de politie blijkt de verdachte uit Haarlem te komen.

Bij de Haarlemse veiligheidscheck in oktober 2019 bleek dat bij een derde van de ondervraagde ondernemers (102 respondenten) wel eens een spookfactuur of phishingmail is binnengekomen. De kans dat Haarlemse ondernemers slachtoffer kunnen worden is aanzienlijk. Toch heeft slechts 20% van de ondernemers een digitaal beleid, werkt nog geen 20% van de ondernemers met een passwordmanager en geven 18% van de ondernemers toe slechts 1 wachtwoord te hebben voor al hun accounts. Minder dan 20% maakt een dagelijkse back-up van het werk, een kwart doet dit heel soms of nooit.

Veilige evenementen: online oproepen voor bijeenkomsten/demonstraties
Evenementen worden steeds vaker via het internet georganiseerd. Via social media en WhatsApp worden inwoners uitgenodigd voor spontane evenementen en demonstraties. In bijna alle gevallen gaat dit goed, maar het kan ook uit de hand lopen. Zoals bijvoorbeeld Project X in Haren. Dergelijke incidenten geven aan dat de online wereld een enorme impact kan hebben op de openbare orde en veiligheid in de gemeente. Een goede online informatiepositie binnen de gemeente wordt dan ook steeds belangrijker. Via sociale media zijn in de regio Kennemerland en in Haarlem meerdere illegale feesten ontdekt door politie en gemeente waarbij preventief ingegrepen kon worden.

2.3 Jeugd en Veiligheid

Jongeren zijn relatief vaker slachtoffer en dader van cybercriminaliteit. In totaliteit is in 2019 het aandeel 15–24-jarige slachtoffers met 18 procent ongeveer 2,5 keer zo groot als het aandeel 65-plussers (7 procent). Naast misbruik van accounts en bestellingen, aan- en verkoopfraude zijn sexting en cyberpesten twee veelvoorkomende cyberdelicten onder de jeugd (CBS, 2020).

Sexting
Sexting - het sturen of ontvangen van seksueel getinte filmpjes of video's - is voor jongeren meestal een onderdeel van seksueel experimenteren. Zolang de beelden binnen een gelijkwaardige relatie uitgewisseld worden en daar blijven, lopen verzender en ontvanger weinig risico. Het wordt een ander verhaal als een foto of filmpje door anderen wordt

verspreid via social media. Met grote gevolgen van dien zoals (cyber)pesten, ernstig persoonlijk leed, schooluitval en problemen bij het vinden van een baan. Daarnaast verkeert

> Een minderjarige jongen uit Haarlem zit thuis op zijn pc, bezoekt een online virtuele wereld waar je kunt chatten, lopen, vrienden maken en ontmoeten. Hier ontmoet hij een persoon die kennelijk op afstand andere pc's kan aanvallen met als gevolg dat de pc (tijdelijk) niets meer doet (DDOS). Later blijkt uit onderzoek door de politie dat deze persoon andere jeugdigen dwingt om naaktfoto's te sturen. Doen ze dit niet dan wordt hun pc aangevallen. Zodra er naaktfoto's zijn verstuurd worden de slachtoffers verder gechanteerd. De verdachte woont in een ander deel van Nederland.

de geportretteerde in een chantabele positie wat hem/haar kwetsbaar maakt. Soms kan dit leiden tot sextortion. Sextortion is afpersing met een seksueel getinte foto of video van het slachtoffer.

In het tweede kwartaal van 2019 is door de gemeente Haarlem onderzoek gedaan naar sexting onder 145 tieners (gemiddeld 14 jaar) die in Haarlem op school zitten. 15% van de respondenten geeft in een enquête aan dat zij wel eens een sexy filmpje/foto verstuurd hebben. Opvallend is dat 20% van deze leerlingen dat zij hier een negatieve ervaring mee hebben gehad doordat het filmpje of de video is doorgestuurd naar derden. Uit gesprekken met veiligheidscoördinatoren van middelbare scholen blijkt dat er gemiddeld zo'n 2 keer per jaar per middelbare school een sexting-incident plaatsvindt. Dit betekent dat er in Haarlem op jaarbasis op zijn minst 30 sexting-incidenten op middelbare scholen plaatsvinden. Van zowel sexting als van sexortion wordt jaarlijks 2 tot 4 keer aangifte gedaan.

Digitaal pesten
Digitaal pesten is een vorm van pesten. Het gebeurt via internet, sociale media en mobiele telefoon. Voorbeelden van digitaal pesten zijn het verspreiden van gênante foto's, het aanmaken van een nepprofiel of het versturen van bedreigende berichtjes. Digitaal pesten is soms extra vervelend omdat het pesten 24 uur per dag door kan gaan, er een groot publiek bereikt kan worden en de pester anoniem kan blijven en daardoor verder durft te gaan. Ook blijft digitaal pesten vaker verborgen voor volwassenen. Het CBS (2020) meldt dat 7% van de 15-25-jarigen in Haarlem wel eens is digitaal gepest.

De jeugd is niet alleen vaak slachtoffer van criminaliteit, maar ook dader. In sommige gevallen zijn de jeugdigen zich er niet van bewust dat ze een strafbaar feit plegen. In andere gevallen weten ze goed waar ze mee bezig zijn. Twee typerende 'daders' zijn de geldezels en script kiddies (jongeren die proberen in te breken in systemen).

Geldezels
Cybercriminele netwerken die zich bezighouden met phishing, ransomware en online oplichting hebben vaak lokale netwerken van geldezels nodig om geld ongezien weg te kunnen sluizen van de bankrekeningen van slachtoffers naar de leden van een criminele groep. Geldezels zijn personen die – bewust of onbewust – hun bankrekening laten misbruiken voor criminele activiteiten. Geldezels zorgen dat het spoor doorbroken wordt door het geld cash op te nemen en mee te geven aan ronselaars die weer in contact staan met de criminele netwerken. Geldezels vormen daarmee een belangrijke schakel in cybercriminele netwerken.

Het Landelijk Meldpunt Internet Oplichting (LMIO), een organisatieonderdeel van de politie, geeft aan dat er in 2019 zo'n 70 verdachten zijn in Haarlem waarvan wordt vermoed dat zij fungeren als geldezel. Tegen de geldezels is 292 keer aangifte gedaan door mensen uit het hele land. Kenmerkend is dat het merendeel van de verdachten mannen tussen de 17 en 23 jaar

zijn. Vaak ontvangen zij een geldbedrag per transactie die zij doen. Een aantal verdachten zijn reeds bekend bij gemeente en politie doordat zij onderdeel zijn van de Persoonsgerichte Aanpak (PGA) of betrokken zijn bij het dealen van drugs.

Niet alle geldezels zijn zich bewust van het feit dat zij geld witwassen en dus strafbaar bezig zijn. Sommige geldezels worden er ingeluisd en denken slechts iemand te helpen. Geldezels kunnen online geronseld worden via bijvoorbeeld social media en online vacatures. Ook vindt

> Een 15-jarige Haarlemmer wordt door een kennis gevraagd of de kennis zijn salaris op de bankrekening van de 15-jarige jongen mag storten. De 15-jarige gaat akkoord en ontvangt het geldbedrag op zijn rekening. Daarop wordt de jongen gevraagd het bedrag direct te pinnen. Door de grootte van het bedrag is dit niet mogelijk. De jongen schakelt daarop zijn ouders in. Zij vertrouwen het niet en bellen de politie. De jongen blijkt gebruikt te zijn als geldezel.

het ronselen lokaal plaats: via scholen, sportverenigingen en in het uitgaansleven. Op het moment dat een geldezel wordt gepakt wordt zijn/haar bankrekening geblokkeerd en kan de geldezel geen nieuwe rekening meer openen, vaak ook niet bij een andere banken. Bovendien loopt de geldezel het risico aansprakelijk te worden gesteld voor het verdwenen geld.

Netwerkanalyses van het LMIO wijzen uit dat het netwerk in Haarlem niet alleen lokaal is, maar dat het zich uitstrekt naar Zaanstad, Haarlemmermeer en Amsterdam. Politie en jongerenwerkers bevestigen dat enkele geldezels die wel in beeld zijn, bekenden zijn en behoren tot de PGA-jeugd.

Script Kiddies
Script kiddies zijn jongeren die in proberen in te breken in systemen. Soms is het alleen om te zien hoever ze kunnen komen of omdat ze online kattenkwaad uit willen halen en rotzooi willen trappen. Script kiddies doen dit meestal niet voor financieel gewin. Maar de schade kan alsnog wel degelijk worden aangericht, omdat ze niet precies weten wat ze doen of niet doorhebben wat de consequenties zijn van hun vandalisme. Script kiddies maken graag gebruik van nieuwe kwetsbaarheden in systemen, waarmee ze binnen kunnen komen bij bedrijven of instanties waar deze nog niet zijn aangepakt of opgelost. Een standaard wachtwoord of een verkeerd gekozen gebruikersnaam kunnen al reden genoeg zijn voor een script kiddie om daar misbruik van te maken.

In Haarlem is casuïstiek bekend van script kiddies die de camera van hun buren hacken. Ook zijn er meerdere middelbare scholen die aangeven dat de script kiddies hebben ingebroken in de schoolsystemen om hun cijfer te veranderen. Speciaal voor jonge hackers tussen de 12 en 23 is door de landelijke eenheid “Hack_Right” ontwikkeld; een alternatief, onderdeel of aanvulling op een strafrechtelijk traject. Met als doel: deze ‘first offenders’ op het rechte pad krijgen en houden.

2.4 Fysieke veiligheid

De samenleving wordt steeds afhankelijker van digitale systemen. Dat wordt pas gemerkt als één van die systemen niet goed werkt. Denk bijvoorbeeld aan pintransacties die niet doorkomen, geannuleerde vluchten door stroomstoringen of hacks op ICT-afdelingen van ziekenhuizen. Zulke gebeurtenissen kunnen grote invloed hebben op onze fysieke veiligheid en

daarmee vervelende maatschappelijke gevolgen veroorzaken. Als sprake is van zulke gebeurtenissen noemen we dat digitale ontwrichting of cybergevolgbestrijding.

" Digitale ontwrichting ligt op de loer" – Cybersecuritybeeld Nederland

Er is sprake van digitale ontwrichting als een digitaal (ICT) systeem, onbedoeld, moedwillig of door een fout, verstoord raakt en daarmee de fysieke veiligheid of de openbare orde in gevaar brengt. De oorzaak van de verstoring kan zowel in het digitale als het fysieke zijn oorzaak vinden. Zo kan niet alleen een hack (digitaal) leiden tot digitale ontwrichting, maar ook een brand in een datacentrum (fysiek). Daarom spreken we niet over cybercrime, maar ook over digitale ontwrichting. Er is bij digitale ontwrichting niet altijd opzet in het spel.

Dit jaar inventariseert de VRK samen met de crisispartners wat de mogelijke effecten kunnen zijn van een cybercrisis/digitale ontwrichting op de sociale en maatschappelijke omgeving.

2.5 Integriteit en veiligheid

Binnen dit veiligheidsveld vallen een aantal verschijnselen die meer fundamenteel onze rechtsorde en veiligheid bedreigen zoals radicalisering en polarisatie, georganiseerde (ondermijnende) criminaliteit en informatieveiligheid.

CTER
Internet en sociale media worden als middel gebruikt voor discriminatie, polarisatie, radicaal gedachtegoed, complottheorieën en extremistische of gewelddadige beelden. Denk bijvoorbeeld aan het internetforum 8chan. Met "omarm schandaal" als motto, is de website een plaats voor radicalisering en extreemrechts ideeën.

Door de grote hoeveelheid berichten en de filterbubbel - waarbij websites en zoekmachines hun resultaten afstemmen op het eerdere online zoekgedrag – krijgen inwoners nauwelijks nog objectieve zoekresultaten te zien. Mensen die op zoek zijn naar zingeving, status of antwoorden omtrent hun eigen identiteit, kunnen in een bubbel (of *echokamer*) terechtkomen waarin iedereen dezelfde overtuigingen heeft. Het is dan moeilijk om zelf een mening te vormen die gebaseerd is op diverse, wetenschappelijk onderbouwde, bronnen. Zo'n bubbel heeft invloed op hoe wij onszelf, de ander of de wereld zien. De kans is aanwezig dat radicale denkbeelden ontwikkeld of aangewakkerd worden op thema's zoals 5G, extreem rechts of het jihadisme (mediawijsheid, 2020).

Met name sinds de coronacrisis, is een toename waargenomen van online activiteit door extremisten en personen die meegaan in extremistisch gedachtegoed. In de eenheid Noord-Holland zijn door monitoringsacties in het online domein nieuwe signalen opgepikt van haatpredikers en extremisten op jihadistisch en rechtsextremistisch gebied. Online worden ideologieën gedeeld en wordt opgeroepen tot actie. De regionale werkgroep CTER van Noord Holland Samen Veilig onderzoekt momenteel de mogelijkheden voor het versterken van online monitoring.

Georganiseerde (ondermijnende) criminaliteit
Het dark web staat is het verbogen gedeelte van het wereldwijde web dat niet toegankelijk is met normale webbrowsers. Hoewel het dark web ook een veilige plek is voor journalisten, klokkenluiders en burgers uit gecensureerde landen, staat het dark web vooral bekend als plek

waar criminelen anoniem zaken kunnen doen. Op het dark web kunnen ze op anonieme wijze hun illegale producten over de hele wereld adverteren. Er zijn erg veel webshops die drugs aanbieden. Ook handel in kinderporno vindt op het dark web plaats. Het betaalmiddel van het dark web is in bitcoins, een gedecentraliseerde, onafhankelijke en virtuele valuta.

De verzending van de op het dark web gekochte producten gaat per post. Zo kunnen kleine hoeveelheden drugs per post worden verstuurd. Wapens kunnen per onderdeel gekocht worden, verspreid over pakketjes, om zo het risico op detectie te verkleinen. Door de anonimiteit is het onbekend hoeveel Haarlemmers zich bevinden op het dark web.

Informatiebeveiliging
De beveiliging van de interne informatiesystemen van de Gemeente Haarlem is een belangrijk onderdeel van dit thema. Informatie, waaronder privacygevoelige gegevens, is één van de belangrijkste bedrijfsmiddelen van de gemeente Haarlem. Deze informatie moet goed beschermd worden, zodat cybercriminelen geen toegang hebben. Er wordt dan ook hard gewerkt aan de informatieveiligheid van de gemeente. Hier leest u meer over de laatste stand van zaken rondom de informatiebeveiliging in Haarlem.

3. Aanpak

In maart 2019 is gestart met het opzetten van de aanpak cybercriminaliteit. Het uitgangspunt is ondernemers, inwoners en de jeugd de komende jaren weerbaarder te maken voor cybercriminaliteit. Door in te zetten op bewustwording, het vergroten van kennis en het veranderen van onveilig online gedrag moet slachtofferschap voorkomen worden. Van belang is dat er de komende jaren intensief wordt samengewerkt met politie, openbaar ministerie, en de wetenschap zodat digitale criminelen sneller kunnen worden opgespoord en vervolgd.

3.1 Terugblik 2019

Netwerk opbouwen
2019 is een jaar geweest waarin aandacht is uitgegaan naar het opbouwen van een netwerk van cybercollega's en experts zodat de gemeente Haarlem toegang heeft tot de expertise die nodig is voor de ontwikkeling van de lokale aanpak cybercriminaliteit. Deze expertise is schaars en bevindt zich in klein en landelijk netwerk bij diverse afdelingen van de politie, publieke partijen zoals het CCV en de ministeries, regionale samenwerkingsverbanden, het OM, wetenschappelijke partijen en private partijen. De gemeente is in juni 2019 aangesloten bij het consortium cybercrime, bestaande uit zo'n 12 gemeenten, vier regionale samenwerkingsverbanden en vier onderzoeksinstituten. Doel van dit consortium is om expertise uit te wisselen, gezamenlijk interventies te ontwikkelen en het effect van deze interventies te meten. Het consortium is verbonden aan HackShield en het geldezelproject (zie volgende paragraaf: aanpak 2020).

Inzicht in aard en omvang
In 2019 is ingezet op het verkrijgen van inzicht in de aard en omvang van cybercriminaliteit. De rapportage die u nu leest is het resultaat en biedt handvaten voor het aanpakken van cybercriminaliteit en digitale onveiligheid. Voor de periodieke informatievoorziening zijn door het regionale samenwerkingsverband Noord Holland Samen Veilig afspraken gemaakt met

politie over de ontwikkeling van periodieke rapportages. Deze rapportages zijn eenheidsbreed en geven inzicht in de ontwikkeling van cybercriminaliteit. De regionale rapportages bieden handvaten om op lokaal niveau gericht in te zetten op risico-communicatie en het ontwikkelen van campagnes.

Digitaal veilige jeugd
In 2019 is gekozen om te focussen op de doelgroep jeugd omdat deze doelgroep kwetsbaar is voor zowel dader- als slachtofferschap. De jeugd wordt niet alleen vaak slachtoffer van cybercriminaliteit, maar is ook vaak dader. Het doel van 2019 was om meer zicht te krijgen op de grootte van de problematiek in Haarlem en de jeugd weerbaarder te maken tegen cybercriminaliteit.

Om meer inzicht te krijgen op de problematiek is door een masterstudent onderzoek gedaan onder 114 leerlingen naar sexting en digitaal pesten. Daarnaast heeft de afdeling Veiligheid & Handhaving gesprekken gevoerd met de veiligheidscoördinatoren van 12 middelbare scholen. Uit het onderzoek en de gesprekken bleek dat een handelingskader bij slachtofferschap door sexting vaak ontbreekt terwijl hier wel behoefte aan is. In samenwerking met de GGD, politie, HALT en veiligheidscoördinatoren is daarom het stappenplan sexting ontwikkeld. Hierbij wordt tevens focus gelegd op de noodzaak om als school melding te doen om zodoende beter inzicht te krijgen in de grootte van de problematiek.

In samenwerking met de GGD organiseerde de gemeente Haarlem in oktober 2019 twee masterclasses voor docenten uit het basis- en voortgezet onderwijs. Deze masterclasses gingen over mediawijsheid, digitaal pesten, geldezels en sexting. Doel van deze masterclasses was om docenten handvaten te geven voor deze relatief nieuwe onderwerpen. In totaal kwamen zo'n 120 docenten op deze avonden af en een vijftal jongerenorganisaties. Tijdens de masterclass voor docenten uit het voortgezet onderwijs is het stappenplan sexting gepresenteerd en verspreid. Daarnaast zijn de gratis, en reeds beschikbare, voorlichtingsprogramma's over sexting en digitaal pesten onder de docenten van het voortgezet onderwijs verspreid. Vanuit de afdelingen JOS en MO is in 2019 ingezet op het project Wijs en Weerbaar en de training "Rots en Water". Ook zijn theatervoorstellingen ingezet om digitaal pesten tegen te gaan.

Digitaal veilige ondernemers
In het voorjaar van 2019 startte de landelijke campagne Cybercrime van het Ministerie van Economische Zaken en Klimaat. Het RPCNH organiseert in het verlengde hiervan in een tiental gemeenten een vierwekelijks cybercrime traject dat afsluit met een training voor ondernemers. Haarlem startte als eerste gemeente met het vierwekelijkse traject. Allereerst is het thema cybercriminaliteit onder de aandacht van ondernemers is gebracht. Drie dagen lang zijn enquêteurs in Haarlem langsgegaan bij ondernemers en is hen gevraagd naar hun online gedrag. Via het ondernemersnetwerk, enquêteurs, social media en mupi's in de stad is vervolgens bekend gemaakt dat ondernemers een gratis training kunnen volgen rondom digitale veiligheid. Deze training heeft op 2 juli plaatsgevonden. Zo'n 50 ondernemers hebben deze training gevolgd.

In oktober is in de week van de veiligheid een veiligheidscheck georganiseerd door het Regionaal Opleidingen Centrum (ROC), politie, het RPC en gemeente Haarlem. Daarin zijn ondernemers bevraagd over hun digitale veiligheid. Deze gegevens zijn meegenomen in bovenstaand beeld. In november zijn de Haarlemse ondernemers uitgenodigd voor een gratis "avondje uit" met het thema cybercriminaliteit.

Ontwikkeling voorlichting aan- en verkoopfraude
In het najaar van 2019 is gemeente Haarlem samen met het Landelijk Meldpunt Internet Oplichting (politie) met het thema aan- en verkoopfraude geselecteerd door de VNG om mee te doen aan het Safety Lab op de Dutch Design week. Tijdens deze week zijn drie ontwerpers aan de slag gegaan met de vraag waarom mensen slachtoffer worden van online oplichting. Deze inzichten zijn gebruikt bij het ontwikkelen van een online voorlichtingscampagne “zelf in de hand” waarin met behulp van story-telling inwoners in korte video’s worden voorgelicht over online oplichting. Deze video’s laten “live” voorbeelden zien van aan- en verkoopfraude. In maart 2020 is de campagne van start gegaan, deze is echter na een week door de coronacrisis gestopt. Afhankelijk van de ontwikkelingen wordt gekeken wanneer dit weer opgepakt kan worden.

Meldingsbereidheid
In het Actieprogramma 2019 was ten doel gesteld om de meldingsbereidheid te verhogen. De politie kan door de hoeveelheid niet alle cyber gerelateerde aangiften en onderzoeken oppakken. Daarom is er voor gekozen de focus binnen de aanpak te verschuiven naar het voorkomen van cybercriminaliteit in plaats van de verhoging van de meldingsbereidheid.

3.2 Aanpak 2020

Cybercriminaliteit ontwikkelt zich gestaag door waardoor er continu nieuwe cybercrime fenomenen bijkomen. Het is daarom belangrijk dat inwoners van de veelvoorkomende ontwikkelingen op de hoogte zijn. Daarom zet gemeente in op risico-communicatie naar inwoners. Via de online kanalen van gemeente Haarlem worden inwoners over de nieuwe trends geïnformeerd. Dit kan bijvoorbeeld via de facebookpagina of een persbericht. Zodoende is de afgelopen periode over online oplichting, aan- en verkoopfraude en vriend-in-noodfraude gecommuniceerd.

Cybercriminaliteit komt in alle veiligheidsvelden voor en heeft impact op thema’s als de jeugd, crisisbeheersing, veilig ondernemen, ondermijning en CTER. Sinds maart 2019 is een projectcoördinator cybercrime voor 18 uur per week aangesteld. De projectcoördinator verbindt digitale veiligheid waar mogelijk met de gemeentelijke aanpak van de reguliere veiligheidsthema’s. Daarnaast wordt in 2020 ingezet op een viertal projecten, namelijk: HackShield, het geldezelproject, aan- en verkoopfraude en project Shitzooi.

Hackshield
Project Hackshield is een regionaal project van het samenwerkingsverband Noord Holland Samen Veilig waaraan zeven gemeenten uit Noord Holland aan deelnemen, waaronder Haarlem. Het project is in 1 maart 2020 gestart. In het project zijn 8 t/m 12-jarigen kinderen uit Haarlem uitgedaagd om de training tot Junior Cyber Agent te volgen. De training bestaat uit een online game genaamd Hackshield die de kinderen leert zichzelf en hun omgeving te beschermen tegen online gevaren. Thema’s zoals sterke wachtwoorden, phishingmails herkennen en ransomware komen in de game aan bod. De oproep tot deelname is verspreidt via BSO’s, scholen, online forums voor kinderen, sportverenigingen en de pers.

Inmiddels zijn er in Haarlem 83 geregistreerde cyber agents. Volgens de ontwikkelaars van Hackshield hebben zo’n 640 Haarlemse kinderen de game gespeeld. Op 1 juli is de projectcoördinator cybercrime samen met de jeugdagent langsgegaan bij de drie beste Haarlemse spelers om hen te huldigen.

Het geldezelproject
In Haarlem wonen ongeveer 70 inwoners die er van verdacht worden geldezel te zijn. Een geldezel is iemand die zijn bankrekening laat misbruiken door, in dit geval, cybercriminelen. De cybercriminelen gebruiken de bankrekening van de geldezel om geld weg te sluizen en wit te wassen. Tegen deze Haarlemse geldezels is zo'n 292 keer aangifte gedaan.

De signalen vanuit politie en het gebrek aan efficiënte interventiemogelijkheden hebben ertoe geleid dat het Rechercheteam van Haarlem, het onderzoeksteam van het Nederlands Studiecentrum voor Criminaliteit en Rechtshandhaving (NSCR) en gemeente Haarlem de handen ineen hebben geslagen en besloten hebben om gezamenlijk een project op te zetten. Het uiteindelijke doel van dit project is om interventies te ontwikkelen die voorkomen dat geldezels meewerken met cybercriminele netwerken. De eerste stap in dit project is het verkrijgen van inzicht in de Haarlemse geldezels en hun netwerken. Het onderzoeksteam van NSCR helpt de stakeholders bij het in kaart brengen van de kenmerken en netwerken van geldezels in Haarlem door de afname van interviews. Nadat een compleet beeld is gevormd op de geldezels, wordt in samenwerking met de ketenpartners bepaalt welke interventie het beste aansluit bij de doelgroep. Het streven is om een structurele interventie te ontwikkelen.

Voor zover bekend is Haarlem de eerste gemeente in Nederland die samen met politie en wetenschap inzichten vergaart over geldezels en op basis van deze informatie een interventie ontwikkelt gericht op daders. Het project wordt gesubsidieerd door het Centrum voor Criminaliteitspreventie en Veiligheid (CCV), het ministerie van Binnenlandse Zaken en het ministerie van Justitie en Veiligheid. Tevens is dit project geselecteerd als "City Deal". Deze deal genereert landelijke bekendheid voor het project en dient te leiden tot een innovatieve oplossing voor de landelijke geldezelproblematiek.

Doorstart aan- en verkoopfraude
De voorlichting over aan- en verkoopfraude zoals ontwikkeld is door designers, VNG, gemeente en politie is, zoals hierboven aangegeven door de coronacrisis één week na de lancering week gestopt. Deze keuze is gemaakt omdat de online kanalen van de gemeente in de piek van de crisis gebruikt dienden te worden voor de communicatie over de crisis. Indien mogelijk, wordt de campagne 'zelf in de hand' hervat na de tweede coronagolf.

Ontwikkeling project Shitzooi
Momenteel wordt binnen de gemeente bekeken of het mogelijk is om het Shitzooi traject te draaien op de middelbare scholen in Haarlem. Het Shitzooi-traject biedt scholen de mogelijkheid om het thema 'sexting' preventief op de kaart te zetten door jongeren te wijzen op de risico's die het gebruik van social media met zich mee brengen. Het Shitzooi-project bestaat uit een interactieve game en een voorlichting, waardoor de jongeren het thema zowel 'beleven' als geïnformeerd worden. In de praktijk blijkt dit de perfecte combinatie. Daarnaast wordt op een laagdrempelige manier jongeren de gelegenheid geboden het onderwerp bespreekbaar te maken.

3.3 Vooruitblik 2021

In 2019 zijn er masterclasses voor ondernemers, veiligheidschecks en voorlichtingen voor middelbare scholen geweest. 2020 kenmerkt zich door de projecten, zoals hierboven beschreven, die een langere doorloop kennen van een aantal maanden. Het voorstel is om in 2021 deze projecten te blijven draaien en daarnaast de focus te leggen op het structureel en duurzaam kunnen borgen van de aanpak van cybercrime. Hierbij wordt gedacht aan een structurele interventie voor geldezels en trajecten zoals Shitzooi, waarbij voor langere termijn aandacht uitgaat naar het geven van voorlichtingen die worden gegeven door reeds bestaande partners zoals jongerenwerkers.

Daarnaast is de verbinding naar andere thema's zoals CTER, fysieke veiligheid en ondermijning van belang. Zoals omschreven in de analyse is de aanpak van cybercrime verbonden met alle veiligheidsvelden. Dit maakt dat samenwerking met een groot aantal projecten en organisaties voor het aanpakken van cybercrime erg belangrijk is. Dit wordt in 2021 verder gecontinueerd.

Dit is een uitgave van gemeente Haarlem,
27 oktober 2020

Postbus 511
2003 PB Haarlem
Tel. 14 023

haarlem.nl