Notitie

Aanpak veelvoorkomende digitale criminaliteit in de regio Rotterdam

Algemene overwegingen

Criminaliteit digitaliseert in razendsnel tempo.
Criminelen zijn creatief en wendbaar waardoor steeds nieuwe vormen ontstaan. Inwoners en ondernemers worden massaal slachtoffer van veel voorkomende vormen van digitale criminaliteit, zoals online fraude. De ontwikkelingen zijn dagelijks onderwerp van gesprek, zowel online als in de media.

De cijfers van digitale criminaliteit verdubbelen.
Jaarlijks zien we gedigitaliseerde criminaliteitsvormen met 20 tot 25 procent stijgen en het einde van deze stijging is voorlopig niet in zicht. De cijfers binnen de eenheid Rotterdam zijn opvallend hoog, de eenheid steekt m.b.t. vriend in noodfraude en zgn. geldezels met kop en schouder boven de andere eenheden uit.

Het werkaanbod en de opgave van politie, OM en gemeenten in de samenleving veranderen door digitalisering drastisch.
Ieder heeft hierin zijn eigen rol. De politie zorgt voor veiligheid in wijken en buurten en pakt criminaliteit aan. Het OM is verantwoordelijk voor het opsporen en vervolgen van strafbare feiten en vormt samen met de Rechtspraak de rechterlijke macht. Gemeenten dienen vanuit hun zorgplicht de samenleving weerbaar te maken tegen cybercrime en gedigitaliseerde criminaliteit. Digitale criminaliteit vraagt om een andere aanpak en brengt een verschuiving van werkzaamheden en competenties met zich mee. Dit vraagt naast een integrale aanpak ook om een krachtig antwoord van de keten op korte termijn.

Specifieke overwegingen

Aandacht voor cybercriminaliteit is niet nieuw
In 2017 heeft het Regionaal VeiligheidsOverleg (RVO) opdracht gegeven om binnen de regio via 5 sporen aandacht te besteden aan cybercriminaliteit. In de Uitwerking van de Veiligheidsagenda 2019-2022, zoals toegezonden aan de Tweede Kamer, is cybercrime één van de vijf landelijke beleidsdoelstellingen. In het Regionaal Veiligheidsplan eenheid Rotterdam (Strategische thema's veiligheid 2019 – 2022) is de aanpak van cybercriminaliteit benoemd als één van de zes veiligheidsthema's. Op 12 februari 2021 heeft de VNG de resolutie 'Digitale Veiligheid: kerntaak voor gemeenten' unaniem aangenomen. De resolutie komt voort uit de Agenda Digitale Veiligheid gemeenten 2020-2024
In het RVO van 12 juli 2021 is de urgentie onderschreven om extra prioriteit te geven aan digitale criminaliteit en is ingestemd met het oprichten van een werkgroep met vertegenwoordigers vanuit politie, OM, VAR en de gemeente Rotterdam. De werkgroep heeft de opdracht de mogelijkheden voor een gezamenlijke aanpak van digitale criminaliteit verder te onderzoeken. Met deze notitie wordt draagvlak gevraagd voor de gezamenlijke aanpak en worden het doel en de resultaten op hoofdlijnen beschreven.

Volgende >

Scope
Het gaat hier specifiek om veel voorkomende digitale criminaliteit met het doel zichzelf te bevoordelen ten koste van anderen. Deze vorm van veelvoorkomende digitale criminaliteit veroorzaakt veel slachtoffers en er is sprake van veelal jonge daders. Voorbeelden zijn vriend-in-nood-fraude, helpdeskfraude en aan- en verkoopfraude, veelal gepleegd met behulp van geldezels.
Onderstaande valt buiten scope:

- Cybercrime in enge zin: ransomware, DDoS-aanvallen, etc.
- Minder veelvoorkomende delicten met een digitale component zoals sextortion.
- Eigen huis op orde
- Cybergevolgbestrijding

Doel

De politie-eenheid Rotterdam, het Openbaar Ministerie en de 25 gemeenten in de eenheid Rotterdam werken in de periode tot en met 2024 samen met publieke en private partners aan een versnelde positieve ontwikkeling op het gebied van weerbaarheid en bewustzijn in het digitale domein. De focus ligt hierbij op de meest voorkomende vormen van digitale criminaliteit, het gaat hierbij veelal om online fraude.

Doel van het programma

- Als één overheid versneld een positieve ontwikkeling op het tegengaan van digitale criminaliteit teweeg te brengen.
- De aanpak van veel voorkomende digitale criminaliteit op te nemen in het meerjarenbeleidsplan voor de eenheid (2022-2026) en de beleids- en uitvoeringsplannen van de deelnemende organisaties.
- Komen tot een integraal plan van aanpak voor de korte en de lange termijn, waaraan alle partijen bijdragen. Deze plannen richten zich in elk geval op de aanpak van vriend-in-nood-fraude, helpdeskfraude, aan- en verkoopfraude (veelal gepleegd met behulp van geldezels) en digitale seniorenveiligheid. Hiermee ontstaat een integrale aanpak met een groot maatschappelijk effect voor inwoners en ondernemers, waardoor zij beter beschermd zijn tegen digitale criminaliteit.
- De aanpak van veelvoorkomende digitale criminaliteit wordt hiermee net zo normaal als de aanpak van bijvoorbeeld high impact crimes en andere veelvoorkomende criminaliteit.

Monitoren en verantwoorden

Het is de ambitie om de uitvoering van de aanpak van veelvoorkomende digitale criminaliteit gezamenlijk aan te pakken. Hoewel elke organisatie zelfstandig aan zijn bestuur verantwoording aflegt, zal de aansturing plaats vinden door een stuurgroep en zal ook gezamenlijk verantwoording afgelegd worden aan het RVO. De stuurgroep wordt voorgezeten door de regionale portefeuillehouder cybercrime, de stuurgroep wordt gevormd door de portefeuillehouder cyber van de politie eenheid Rotterdam, de cyberofficier van het OM, de adviseur regioburgemeester, het afdelingshoofd staf, ondermijning en strategie (Directie Veiligheid) Gemeente Rotterdam en het hoofd VAR.

Het monitoren en verantwoorden is gekoppeld aan het hoofddoel en de beoogde resultaten. Hiervoor worden indicatoren opgesteld. Het betreft vooral indicatoren die iets zeggen over de geleverde inspanningen. Effectindicatoren zijn lastig op te stellen omdat een causaal verband tussen veiligheidsinterventies en maatschappelijk effect moeilijk aantoonbaar is gezien de vele variabelen die een rol kunnen spelen.

De aanpak behelst de periode tot en met 2024. De resultaten en effecten van het programma worden jaarlijks en na afloop van de programmaperiode geëvalueerd.

In de periode tot en met 2024 worden de volgende resultaten behaald en aanpak gevolgd:

Commitment op gezamenlijk uitvoeren

• Inspanning te leveren op het thema digitale criminaliteit.
• Capaciteit en budget vrij te maken voor de integrale aanpak, waarbij ook ruimte is voor publiek-private samenwerking.

AANPAK

Elke deelnemende organisatie levert inspanning op het thema digitale criminaliteit.

Hierbij wordt rekening gehouden met elkaars interne opgaven.

Gedeelde visie

• Een gezamenlijke strategische visie op te stellen, zowel voor de korte als de lange termijn.
• Deze visie is beleidsmatig sterk en goed uit te voeren in de praktijk.

AANPAK

Door de werkgroep wordt een gezamenlijke strategische visie opgesteld, waaraan alle deelnemers zich confirmeren.

Deze visie wordt vastgesteld in het RVO.

Borging strategische visie

• De strategische visie te borgen in de individuele beleidsplannen van de eigen organisaties.
• Hierbij wordt in het bijzonder aan de gemeentes gevraagd om de samenwerking tussen het college van burgemeester en wethouders en de gemeenteraad op het dit onderwerp te verstevigen.

AANPAK

In de beleidsplannen van de politie en het OM en in de integrale veiligheidsplannen (IVP's) van alle 25 regiogemeenten wordt veel voorkomende digitale criminaliteit als prioriteit benoemd.

Betrouwbaar cyberbeeld

• Inzicht in de cijfers van de diverse delicten is noodzakelijk om de juiste (preventieve en repressieve) interventies te kunnen doen. We zorgen voor een goede geregistratie en maken een maandelijks cyberbeeld.

AANPAK

De aangifte- en meldingsbereidheid binnen de eenheid Rotterdam wordt gestimuleerd door het inzetten van gerichte communicatiecampagnes.

Maandelijks wordt door de politie en het OM een betrouwbaar regionaal cyberbeeld opgesteld.

Aangiften worden standaard gescreend op digitale componenten.

Gemeenten ontvangen informatie over typen delicten op wijkniveau en over de slachtoffer- en dadergroepen.

Aansluiting bij regionale en landelijke initiatieven

• Landelijk, regionaal en lokaal worden al veel initiatieven ontplooid, hierbij wordt aansluiting gezocht. Denk hierbij aan PVO, Centurion, de City Deal Lokale Weerbaarheid Cybercrime, het RAAK Consortium Cyberweerbaarheid, een gemeentelijk offensief ter preventie van slachtofferschap van cybercrime.

AANPAK

Gemeenten maken gebruik van de kennis, middelen en bijeenkomsten van de VAR, het CCV, PVO en de VNG op het gebied van online criminaliteit om zo de digitale weerbaarheid te verhogen.

Er wordt gebruik gemaakt van landelijke subsidies voor het doen van onder andere wetenschappelijk onderzoek en het opzetten van awareness campagnes.

Vermindering slachtoffer- en daderschap

• Slachtoffer- en daderschap binnen de eenheid Rotterdamwordt teruggebracht naar het gemiddelde van Nederland.

AANPAK

Gemeenten zetten ter voorkoming van herhaald slachtoffer- en daderschap gericht campagnes in op basis van het regionale en lokale cyberbeeld.

Veroordeelde verdachten worden zo mogelijk financieel 'geplukt' en er vinden lokaal en regionaal interventies plaats om zgn. geldezelschap tegen te gaan.

Er vindt structureel terugkoppeling over de voortgang van zaken plaats naar slachtoffers in combinatie met handelingsperspectief.