Directie Veiligheid
Openbare Orde en Veiligheid

Postadres: Postbus 70012
3000 KP Rotterdam
Website: www.rotterdam.nl

Van: Luca Cox
E-mail: lm.cox@rotterdam.nl

Uw kenmerk: 22bb007469, 22bb007778, 22bb008232
Ons kenmerk: M2211-6124, M2211-7377, M2212-1731

Onderwerp: Moties "Het 'hack' is van de dam" en "Maak het digitale gevaar inzichtelijk", toezegging "Cyber-security"

Datum: B&W 20 juni 2023
Verzonden op 27 juni 2023

Aan de gemeenteraad

Op welke gronden deze brief?/Waarom nu voorgelegd?
Tijdens het commissiedebat over de begroting op 10 november 2022 is de motie "het 'hack' is van de Dam" (kenmerk 22bb007469) aangenomen, ingediend door R. G.C. Segers-Hoogendoorn (CDA Rotterdam), T. Kind (Volt) en A. Oostdijk (Forum voor Democratie). Tevens is een toezegging gedaan om de vragen die tijdens dit debat gesteld zijn over cybersecurity te beantwoorden in het afdoeningsvoorstel van de motie (kenmerk 22bb007778).
In aanvulling hierop werd bij het raadsdebat ter vaststelling van de Veiligheidskoers 2023-2027 op 1 december 2023 de motie "Maak het digitale gevaar inzichtelijk" (kenmerk 22bb008232), ingediend door D.A. van Groningen (VVD) en B. van Drunen (Leefbaar Rotterdam), aangenomen. Beide moties en toezegging worden met deze brief afgedaan.

Relatie met het coalitieakkoord/collegewerkprogramma/eerder aangenomen moties en gedane toezeggingen:
- Veiligheidskoers 2023 - 2027
- Programma Digitale Inclusie

Toelichting:

Motie 22bb8232 - Maak het digitale gevaar inzichtelijk
De motie vraagt om een analyse van de digitale criminaliteit in Rotterdam en in deze analyse mee te nemen hoe vaak Rotterdammers slachtoffer zijn van digitale criminaliteit en hoe Rotterdammers hun digitale veiligheid ervaren.

<u>Slachtofferschap Rotterdam</u>
Uit onderzoek blijkt dat in 2022 bij de politie 3.151 meldingen en aangiftes gedaan zijn van slachtofferschap van digitale criminaliteit in de gemeente Rotterdam. Dit betrof voornamelijk bankhelpdeskfraude (648), account take-over (539) en betaalverzoekfraude (447). Hierbij zijn aan- en verkoopfraude en vriend in nood-fraude niet meegenomen, terwijl dit twee veel voorkomende vormen van digitale criminaliteit in Rotterdam zijn. Dit komt omdat sinds eind 2022 de cyberbeelden jaarlijks worden opgeleverd vanuit de landelijke politie. Hiervoor werden er halfjaarlijkse beelden uitgebracht per eenheid. Door

deze verschuiving is er een informatiebron weg gevallen. Er wordt gelobbyd bij de politie om de ontbrekende data vanaf nu weer op te laten nemen in de jaarbeelden van de politie en daarmee vanaf 2024 een meer compleet beeld van slachtofferschap in Rotterdam te kunnen schetsen.
Het daadwerkelijke aantal meldingen en aangiftes van alle vormen van digitale criminaliteit, zal dus nog hoger liggen. Ter illustratie: in de eerste helft van 2022 werden deze vormen van digitale criminaliteit wel meegenomen en toen zijn al 3.420 registraties van slachtofferschap gedaan. Hier komt nog eens bovenop dat de aangiftebereidheid bij slachtofferschap van digitale criminaliteit heel laag is. Deels verklaarbaar omdat de schuld vaak bij de slachtoffers wordt gelegd. Dit gaat gepaard met een hoge mate van schaamte en dat terwijl de gevolgen voor slachtoffers enorm kunnen zijn. Zo heeft meer dan een kwart van de Rotterdamse slachtoffers financiële, emotionele dan wel psychische problemen ondervonden. De financiële schade van slachtoffers binnen de eenheid Rotterdam, wordt in totaal ingeschat op een schadebedrag van €8,7 miljoen over de periode jan-jun 2022. Dit omvat bijna 11% van de ingeschatte financiële schade voor Nederland (€88,9 miljoen) in deze periode.

Hoe ervaren Rotterdammers hun digitale veiligheid?
Over het algemeen voelen Rotterdammers zich veilig online. Dit blijkt uit onze eigen veiligheidsmonitor. Wel schatten zij de kans groter in dat ze slachtoffer zullen worden van digitale criminaliteit dan van verschillende vormen traditionele criminaliteit. Dit komt overeen met het landelijk beeld van digitale veiligheidsgevoelens. Men maakt zich zorgen over de mogelijkheid om slachtoffer te worden van verschillende vormen van digitale criminaliteit, maar voelt zich online wel veilig. Deze tegenstrijdigheid kan er juist voor zorgen dat mensen minder geneigd zijn om preventief gedrag te tonen ten aanzien van digitale criminaliteit. Dit maakt hen kwetsbaarder voor slachtofferschap van digitale criminaliteit.
Omdat nog weinig bekend is over de mate waarin Rotterdamse inwoners digitaal veilig gedrag vertonen, wordt in de landelijke Veiligheidsmonitor van het CBS op een uitgebreidere manier het thema digitale criminaliteit uitgevraagd. De gemeente Rotterdam heeft voor de komende monitor extra vragen ingebracht. De resultaten daarvan zullen in het voorjaar 2024 beschikbaar zijn voor analyse. Deze analyse zal medio 2024 worden uitgevoerd en in het derde kwartaal van 2024 beschikbaar zijn.

Motie 22bb7469 – Het "hack" is van de dam
In de motie wordt gevraagd te komen met een uitwerking van plannen ten aanzien van cybersecurity vanaf 2024 en als daar middelen voor nodig zijn te onderzoeken of een heroverweging binnen het meerjarenperspectief mogelijk is.

De huidige aanpak op cyberveiligheid vanuit directie Veiligheid bestaat sinds 2019 en richt zich voornamelijk op weerbaarheid. De aanpak bestaat uit drie actielijnen:

1. Versterken van onze eigen kennispositie.
2. Openbare orde en veiligheid (OOV); specifiek crisisbeheersing en digitale criminaliteit.
3. Voorlichting aan burgers en ondernemers.

Op basis van beide moties en de uitgevoerde analyse hebben wij ons besluit om de middelen voor digitale criminaliteit met ingang van 2024 stop te zetten, heroverwogen. Bij de voorjaarsnota 2024 stellen wij voor om binnen het Programma Veilig de aanpak op digitale veiligheid deels te continueren. Gelet op de rol en taak van de gemeente omtrent veiligheid wordt er vanuit dit programma gekozen om ons vanaf 2024 zuiver te richten op de OOV-aspecten van digitale veiligheid. Het programma Digitale Inclusie zal zich in

2024-2025 gaan richten op bewustwording van de risico's van digitale criminaliteit bij Rotterdammers, daar waar dit eerder belegd was bij het Programma Veilig.
Het doel van de aanpak vanaf 2024 is het bestrijden van digitale criminaliteit en het weerbaar maken en houden van de stad. Digitale criminaliteit heeft in veel gevallen een grote impact op slachtoffers. Daarom is het van belang in te blijven zetten op de bestrijding hiervan. Dit sluit aan op de ambities van de Veiligheidskoers 2023-2027 waarin het bestrijden van cybercriminaliteit als een van de hoofddoelen wordt beschreven. Daarnaast blijven we onverminderd inzetten op het weerbaar maken van de stad tegen toekomstige cyberaanvallen. We blijven oefenen om de potentiële impact van een cybercrisis minimaal te houden en ervoor te zorgen dat wij als stad en bestuur voorbereid zijn. Het behouden van onze kennispositie en het op de hoogte blijven van trends en ontwikkelingen blijft hierin onderdeel van onze werkzaamheden, maar dit behoeft geen aparte actielijn meer te zijn.
Met de beschikbare middelen zullen wij de komende jaren inzetten op:

- Het zo klein mogelijk maken van de impact van mogelijke cyberaanvallen door bestuurlijke oefeningen op het gebied van cybergevolgbestrijding op te zetten.
- Het bestrijden van daders- en slachtofferschap van veelvoorkomende digitale criminaliteit in samenwerking met politie, OM en VeiligheidsAlliantie regio Rotterdam (VAR). Deze integrale aanpak richt zich op het opzetten van projecten ter voorkoming van slachtoffer- en daderschap, het aanpakken van daders en het opwerpen van barrières met behulp van publiek-private samenwerking.
- Het stimuleren van cybersecurity bij belangrijke stedelijke functies zoals de Rotterdamse ziekenhuizen via Stichting Rotterdamse Ziekenhuizen (SRZ) en het verhogen van de cybersecurity in de Rotterdamse haven door samen te werken en een bijdrage te leveren aan FERM. FERM zet zich in voor weerbaarheid tegen digitale criminaliteit in het Haven Industrieel Complex van Rotterdam door samenwerking tussen bedrijven in de Rotterdamse haven te stimuleren en het bewustzijn bij bedrijven over cyberrisico's te verhogen.

Financiële en juridische consequenties/aspecten:
De aanpak op digitale criminaliteit wordt gefinancierd uit de intensivering van het vorige college en loopt tot 1 januari 2024. Tijdens de behandeling van de begroting op 8 en 10 november 2022 heeft uw raad aan het college verzocht om te komen met plannen ten aanzien van cybersecurity vanaf 2024. Uw raad heeft tevens verzocht om als daar middelen voor nodig zijn te onderzoeken of een heroverweging binnen het meerjarenperspectief mogelijk is.
Bij de voorjaarsnota 2023 stellen wij voor om binnen het Programma Veilig de aanpak op digitale criminaliteit deels te continueren. Daartoe is met ingang van 2024 tot en met 2027 € 250.000 beschikbaar, indien uw raad instemt met de voorjaarsnota. Daarnaast is in het budget van het programma Digitale Inclusie €125.000 gereserveerd voor 2024-2025 om in te zetten op bewustwording van de risico's op digitale criminaliteit bij Rotterdammers.

<u>Subsidies</u>
Ook is toegezegd om uit te zoeken of er landelijke middelen beschikbaar zijn voor inzet op dit thema. Onlangs hebben wij vernomen dat vanuit het ministerie van Justitie en Veiligheid in totaal €150.000 is toegekend voor het jaar 2024:

- €100.000 voor campagnes ter voorkoming van slachtofferschap op digitale criminaliteit.
- €50.000 om in gezamenlijkheid met politie, OM en VAR te besteden.

Toezegging 22bb007778 – beantwoording vragen omtrent cyberveiligheid

1. **Wat is de waarde van de Veiligheidsindex in het licht van de veranderende criminaliteit en kan digitale criminaliteit hierin worden opgenomen?**

De Veiligheidsindex geeft - als onderdeel van het wijkprofiel – weer hoe de staat is van de veiligheid in Rotterdam en in de wijken en richt zich daarbij op de thema's diefstal, geweld, inbraak, vandalisme en overlast. Deze thema's hebben betrekking op de directe leefomgeving van de Rotterdammer in de wijk en zijn op die manier relevant voor de monitoring van de ontwikkeling van wijken.

De vraag of Rotterdammers slachtoffer zijn van digitale (of cyber-) criminaliteit is momenteel wel onderdeel van de Veiligheidsmonitor (de enquête), maar maakt geen deel uit van de Veiligheidsindex. Dit omdat deze vorm van criminaliteit weliswaar grote gevolgen kan hebben voor het individu, maar weinig zegt over de veiligheid in de directe leefomgeving van de Rotterdammer.

Daarnaast zorgt het eventueel opnemen van 'nieuwe' veiligheidsthema's in de Veiligheidsindex (de berekende score op het Wijkprofiel) voor een aanpassing in de methodiek die maakt dat vergelijkingen met eerdere jaargangen niet of op een beperkte manier kunnen worden uitgevoerd. Aanpassing zou het onmogelijk maken om het collegetarget inzake veiligheid consistent en 'rekenkamerproof' te monitoren. Juist in de consistentie van monitoring ligt de waarde van de Veiligheidsindex. Over de vragen met betrekking tot digitale criminaliteit zal daarom apart van de Veiligheidsindex worden gerapporteerd.

2. **Hebben we zicht op welke vormen van digitale criminaliteit in Rotterdam aanwezig zijn? Wat is er nodig voor een effectieve aanpak? Zijn er barrières opgeworpen?**

Ja, er is voldoende zicht op de aanwezige vormen van digitale criminaliteit in Rotterdam. Een effectieve aanpak wordt voornamelijk bepaald door een nauwe samenwerking met onze partners. Voor inzicht zijn wij afhankelijk van deze samenwerkingspartners voor uitwisseling van data. Zo rapporteert de politie via cyberbeelden over politieregistraties die betrekking hebben op digitale criminaliteit. De data uit deze beelden vertalen wij naar beleid en interventies. Om deze aanpak vanaf 2024 te kunnen continueren, waren middelen nodig. Zoals besproken in de afdoening van motie "het 'hack' is van de dam" zijn deze inmiddels toegekend.

De effectieve aanpak is op dit moment beschreven in de notitie "Aanpak veel voorkomende digitale criminaliteit regio Rotterdam"[1]. De notitie omschrijft de gezamenlijke aanpak van politie, OM, VAR (namens de overige gemeenten in de regio) en gemeente Rotterdam op digitale criminaliteit in de regio Rotterdam. Deze aanpak vormt zich rondom zes pijlers: commitment op gezamenlijk uitvoeren, gedeelde visie, borging strategische visie, betrouwbaar cyberbeeld. Aansluiting bij regionale en landelijke initiatieven en vermindering slachtoffer- en daderschap. De eerste vijf pijlers beschrijven dat wat nodig is voor een effectieve aanpak om slachtoffer- en daderschap in de regio te verminderen.

[1] Notitie Aanpak veelvoorkomende digitale criminaliteit in de regio Rotterdam

In de gedeelde visie is beschreven hoe we op de lange termijn vanuit publiek-private samenwerking barrières op willen werpen om het crimineel proces te verstoren[2]. Inmiddels is deze aanpak bij het Rijk komen te liggen. Vanuit de regio sluiten we aan op een traject vanuit J&V. Hierin wordt met partijen zoals het bankenwezen, de telecomsector, en sociale media platformen toegewerkt naar barrières en interventies om inwoners en bedrijven beter te beschermen, fraude te voorkomen en tegelijkertijd het verdienmodel van criminele netwerken te verstoren en potentiële daders te weren[3].

3. **De impact van cybercrime is groot, zoals sextortion. Is cybercriminaliteit een onderdeel van High Impact Crimes?**

In de Veiligheidskoers wordt de link tussen cybercriminaliteit en High Impact Crimes gelegd. Verder wordt landelijk onderzocht hoe de aanpakken mogelijk meer samen kunnen komen. Wij volgen de ontwikkelingen op dit vlak.

Bij de politie en OM is cybercrime geen onderdeel van de aanpak High Impact Crimes. De delicten kunnen wel een grote impact hebben. Bij de politie zijn programma's ingesteld en aparte rechercheteams opgericht in de aanpak van cybercrime en gedigitaliseerde criminaliteit.

4. **Waarom is cybercriminaliteit geen aparte pijler? (Van de Veiligheidskoers 2023-2027)**

Cybercriminaliteit is een van de pijlers van de Veiligheidskoers 2023-2027: hoofdstuk 7 "Bestrijden van cybercriminaliteit en criminaliteit met impact".

5. **Hoe kunnen we organisaties in de stad meer weerbaar maken naar aanleiding van de cyberaanval bij Bibliotheek Rotterdam?**

Cyberweerbaarheid kent vele facetten, zowel in de wijze waarop de digitale infrastructuur is ingericht, als op gedragscomponenten van de gebruikers van deze infrastructuur. Dit is in eerste instantie een taak van de organisatie zelf, waar nodig met steun van private partijen zoals verzekeraars.

Vanuit de gemeente organiseren we diverse projecten en campagnes waarbij we een handelingsperspectief aanreiken om onze burgers en ondernemers meer weerbaar te maken tegen digitale criminaliteit. Cyberveiligheid is echter niet 100% te garanderen, daarom proberen we ook te communiceren wat te doen bij slachtofferschap om de impact zo laag mogelijk te houden.

De stad veiliger maken: daar ligt onze kerntaak. Cyberincidenten kunnen een grote impact hebben op de openbare orde en veiligheid van onze stad. Rotterdam schenkt daarom veel aandacht aan het weerbaar maken van de stad tegen toekomstige cyberaanvallen op haar stedelijke functies. Stedelijke functies betreffen onderdelen van de maatschappij die essentieel zijn om een regio als geheel goed te laten functioneren. Een cyberaanval op deze functies kan daarom een grote impact op de maatschappij hebben en grote economische schade met zich meebrengen. De haven is een van deze stedelijke functies. Daarom investeren we in FERM dat zich inzet op weerbaarheid bij bedrijven in het Haven

[2] Visie Aanpak gedigitaliseerde criminaliteit (rotterdam.local)
[3] Actieplan integrale aanpak online fraude (overheid.nl)

Industrieel Complex. Daarnaast stimuleren we de cyberveiligheid van stedelijke functies zoals Rotterdamse ziekenhuizen via Stichting Rotterdamse Ziekenhuizen (SRZ).

Naast stedelijke functies, is er ook aandacht voor het cyberweerbaar maken van overige ondernemingen. Zo faciliteert de overheid lokale netwerken zoals het Platvorm Veilig Ondernemen (PVO). Hierin werken politie, justitie, gemeenten, brancheorganisaties en ondernemers samen aan oplossingen voor veiligheidsproblemen. Een van de thema's waarop wordt ingezet is cybercriminaliteit. Er wordt onder andere gewerkt aan het vergroten van bewustzijn door het geven van voorlichting en advies aan bedrijven en instellingen. Ook worden er trainingen en bijeenkomsten georganiseerd. Hierin wordt nauw samengewerkt met de gemeente Rotterdam. De politie kan kennis inbrengen in dergelijke netwerken en doet dat ook door regelmatig als gastspreker op te treden. Het OM deelt kennis in de ketenaanpak ten behoeve van preventie.

6. Is er voldoende aandacht voor sextortion en seksuele uitbuiting, desinformatie, en hoe gaat het met de opsporing en aanpak?

<u>Sextortion en seksuele uitbuiting</u>
Vanuit de aanpak seksueel geweld wordt ook aandacht geschonken aan het online aspect van seksueel geweld. Preventief wordt middels het lespakket 'Vrijheden' en de campagne 'Oordeel Niet' ingezet op de problematiek rondom (ongewenste) sexting en shaming, waarbij oog is voor samenhang met sextortion. Binnen het netwerk aanpak seksueel geweld wordt verder samengewerkt met partners die hulp bieden bij verschillende vormen van online seksueel geweld/seksuele uitbuiting, waaronder Slachtofferhulp Nederland en het Centrum Seksueel Geweld.

De gemeente zet in op preventie op seksuele uitbuiting, onder andere door het verzorgen van voorlichting op seksuele uitbuiting en seksueel grensoverschrijdend gedrag aan jongeren. In opdracht van de gemeente heeft het Expertisecentrum Seksualiteit Sekswerk en Mensenhandel (ESSM) gewerkt aan het vernieuwen van de voorlichting op deze thema's, waarin ook aandacht is voor thema's als sexting, shaming, het creëren van deepfake beelden en sextortion. Deze lessen worden (wanneer aangevraagd) gefaciliteerd door het ESSM op middelbare scholen en MBO-scholen. Er zijn voorlichtingen beschikbaar gericht op jongeren, maar er zijn ook modules gericht op (onderwijs)professionals die op deze manier beter worden uitgerust om zorgelijk gedrag bij jongeren te signaleren. Sinds de lancering in oktober 2022 is er veel interesse in deze voorlichtingen getoond en er worden goede reacties op ontvangen.

<u>Opsporing en aanpak</u>
Elk slachtoffer is er één te veel, de meldingsbereidheid is laag en daders zijn niet altijd identificeerbaar. Een kenmerk van het internet is dat het internationaal is en je eenvoudig je identiteit kan afschermen. Maar daar waar het kan, wordt opgespoord en vervolgd. Er zijn in de Veiligheidsagenda van de politie voor het eerst doelstellingen voor de politie opgenomen over de aanpak. Later dit jaar kan de politie zien of zij in de buurt komt van deze doelstellingen.

<u>Desinformatie</u>
Het verspreiden van desinformatie valt onder de vrijheid van meningsuiting en is daarmee op zich niet strafbaar, tenzij het aanzet tot geweld, discriminatie of haat, of iemand nodeloos beledigt. Echter, desinformatie kan leiden tot gevoelens van angst, onzekerheid, onvrede, of miskenning als gevolg van ongrijpbare fenomenen, zoals globalisering, klimaatverandering, migratie en ongelijkheid. Desinformatie kan hierdoor bijdragen aan

polarisatie en maatschappelijk ongenoegen. Er is daarom binnen de aanpak radicalisering, extremisme en polarisatie aandacht voor de rol van desinformatie bij maatschappelijke onrust. Zo 'lezen we de stad' zodat we weten wat er speelt in Rotterdam en adviseren we professionals als zij te maken krijgen met gepolariseerde situaties.

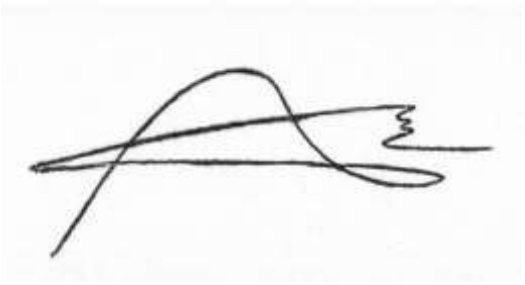
Wij stellen voor hiermee motie "Maak het digitale gevaar inzichtelijk" (kenmerk 22bb008232) en motie "het 'hack' is van de Dam" (kenmerk 22bb007469) en toezegging "Cyber-security" (kenmerk 22bb007778) als afgedaan te beschouwen.

Burgemeester en wethouders van Rotterdam,

De secretaris,

V.J.M. Roozen

De burgemeester,



A. Aboutaleb