Gemeente Amstelveen

INITIATIEFVOORSTEL

Datum 20 november 2022

Nummer	83	**Afdeling**	OOV
Voorstel van	Goed voor Amstelveen	**Behandelend ambtenaar**	Frank Voorbij
Portefeuillehouder	Burgemeester		f.voorbij@amstelveen.nl

Onderwerp

Voorziening vergroten digitale veiligheid MKB

Gevraagd besluit

1. In te stemmen met het versterken van de lokale en regionale GCC (gedigitaliseerde criminaliteit en cybercrime) -aanpak, door het initiëren en faciliteren van een publiek-private samenwerking met het MKB Amstelveen voor het oprichten van een cybermeldpunt en 24/7 helpdesk voor expertise en zo nodig fysieke opvolging bij digitale aanvallen, hacks of andere zorgelijke incidenten, naar voorbeeld van Cybermeldpunt Havengebied IJmuiden.
2. In te stemmen met het hiertoe verrichten van een onderzoek in samenwerking met het MKB, onder regie van het regionaal Platform Veilig Ondernemen (PVO) en in nauwe betrokkenheid met gemeente Amstelveen, naar de exacte behoeften en wensen van het MKB en eventuele financieringsconstructies waar het gaat om adequate ondersteuning bij digitale calamiteiten en het voorkomen, bestrijden en beheersen van GCC.
3. In te stemmen met een budget van €15.000,- voor het faciliteren van dit nader onderzoek in de eerste helft van 2023 onder regie van het PVO, te dekken uit het veiligheidsbudget.
4. In te stemmen met een budget van €50.000,- als maximale bijdrage van Amstelveen voor het initiëren en faciliteren van een Cybermeldpunt MKB Amstelveen met 24/7 opvolging door IT security experts, om na een positief resultaat en uitwerking met het MKB in de tweede helft van 2023 te kunnen doorpakken. Te dekken uit het veiligheidsbudget.

WAT WILLEN WE BEREIKEN EN WAT GAAN WE DAARVOOR DOEN

Wat willen we bereiken (effectindicatoren)

1. Ondernemers en inwoners digitaal beter beschermen. Door het MKB te faciliteren met adequate en betrouwbare expertise worden niet alleen de ondernemingen zelf, maar ook hun klantenbestanden en daarmee onze inwoners beter beschermd.
2. De gevolgen van (ernstige)digitale incidenten te beperken. Bij een ernstig incident, zoals een lek met privacygevoelige gegevens van klanten kan de impact d.m.v. het direct treffen van de juiste interventies, aanzienlijk worden beperkt.
3. Voorkomen van onvoorziene uitgaven. De gemeente helpt bijdragen aan het voorkomen van onvoorziene uitgaven om de schade te herstellen na een hack of ransomware-aanval bijvoorbeeld bij een gewist of beschadigd systeem, of uitgelekte databestanden.
4. De kans op succesvolle opsporing en vervolging van daders te vergroten. Op dit moment is de pakkans bij online misdrijven relatief laag, vergeleken bij de pakkans van klassieke misdrijven. Het cybermeldpunt deelt bij incidenten, met instemming van de aangesloten bedrijven, relevante informatie met politie. Zo neemt de kans op succesvolle opsporing en vervolging toe en de kans op herhaling door dezelfde dader(s) af.
5. Een preventieve werking van een cybermeldpunt dat 24/7 bereikbaar is, monitort en waarschuwt, adequaat reageert en informatie deelt met de politie. Dit voorkomt mogelijk dat hackers kiezen voor deze doelgroep. En maakt dat ondernemers meer bewust worden van de risico's op het internet en bereid zijn te investeren in digitale veiligheid.

6. Een gevoel van rust en veiligheidsgevoel vergroten. Deze voorziening waarbij deskundigen direct geraadpleegd kunnen worden en zo nodig op locatie komen, draagt bij aan het veiligheidsgevoel onder ondernemers. Zij kunnen immers bij een betrouwbare partij terecht bij zorgen en calamiteiten. Dat stelt gerust.

Wat gaan we daarvoor doen (prestatie-indicatoren)

Om de aanpak van GCC te versterken gaat Amstelveen naast de reguliere preventie-, informatie- en bewustwordingscampagnes het MKB faciliteren in een adequate response, naar voorbeeld van het Cybermeldpunt Havengebied IJmuiden. Zeg maar een: 112 meldkamer voor digitale noodgevallen. Een dergelijke voorziening bestaat nog niet in onze regio.

Hiertoe laat Amstelveen onderzoek verrichten naar de exacte behoeften en wensen van het MKB om een dergelijke voorziening op te zetten in een publiek-private samenwerking en mogelijke co-financieringsconstructies.

ACHTERGROND EN OVERWEGINGEN

Programma (speerpunt)

Veiligheid en cybercrime

Aanleiding

De ongelooflijk sterke opmars van cybercrime, zoals hacks, DDos aanvallen en ransomware aanvallen is niet hand in hand gegaan met het treffen van veiligheidsmaatregelen. Deze laatste zijn achtergebleven. Volgens het CBS is afgelopen jaar 15% van alle Nederlanders geconfronteerd met een digitaal misdrijf ten opzichte van 17% dat in 2021 te maken heeft gehad met een klassiek misdrijf, zoals fietsendiefstal, woninginbraak, intimidatie en geweld op straat. Het aantal digitale misdrijven streeft de klassieke misdrijven in rap tempo voorbij. Waarbij tevens opgemerkt moet worden dat de meeste online misdrijven niet gemeld worden, uit schaamte of dat men denkt "het heeft toch geen zin".

Uit diverse onderzoeken blijkt dat het MKB vaak doelwit is van GCC. Ondernemers van het MKB zijn de meest kwetsbare groep die slachtoffer wordt van cybercrime. Cyber incidenten zijn binnen het MKB wijdverbreid. In de kamerbrief van Minister. D. Yesilguz-Zegerius d.d 6-7-2022 wordt gemeenten opgeroepen de weerbaarheid van ondernemingen te versterken en de digitale veiligheid te vergroten. De aanpak van gedigitaliseerde criminaliteit en cybercrime (GCC) heeft dan ook de volle aandacht van het college B&W. Regionaal Veiligheidsplan (RVP) en het Platform Veilig Ondernemen hebben GCC tot prioriteit benoemd. Ook in het concept van het nog door uw raad vast te stellen Integraal Veiligheidsplan Amstelveen (IVP) krijgt de aanpak van GCC prioriteit.

In de praktijk blijkt dat het MKB een extra kwetsbare groep is, omdat zij veelal niet de expertise en middelen heeft om zichzelf te beschermen, maar wel een groot gevaar loopt. Zo zijn de frequentie van aanvallen en de schade groot. Het kabinet merkt op dat in heel Nederland, dus ook Amstelveen, het MKB een kwetsbare groep is (kamerbrief d.d. 6 juli 2022).

In lijn hiermee is het van belang dat onze maatregelen en instrumenten, zoals informatiesessies en websites als Hack Helpdesk (waar ondernemers terecht kunnen voor informatie en trainingen), zich niet blijven beperken tot preventie, informatie en bewustwording. Gezien de urgentie, toenemende complexiteit en impact is meer nodig.

Alhoewel ondernemers allereerst zelf verantwoordelijk zijn voor de eigen (digitale) veiligheid, legitimeert de situatie volgens het Kabinet om hen daarin als overheid te faciliteren en de aanpak van

cybercrime te versterken. Zij stelt daarom subsidie beschikbaar via het PVO om op lokaal niveau publiek-private samenwerkingsverbanden aan te gaan om de digitale veiligheid voor het MKB te vergroten.

Wij zochten naar best practices. De circa 300 bedrijven in het Havengebied IJmuiden hebben samen met politie IJmond, gemeente Velsen, IT Security bedrijf Korper ICT, het Platform Veilig Ondernemen en ondernemingsverenigingen een formule opgezet die succesvol blijkt te werken: Een Cybermeldpunt met 24/7 expertise en opvolging. Zo kunnen ondernemers rekenen op een centraal nummer voor betrouwbare en hoge kwaliteit IT security expertise, wordt informatie met elkaar gedeeld bij een aanval of dreiging, worden situaties individueel en door IT security experts geanalyseerd en wordt een maatwerk respons toegepast. Daarnaast wordt relevante (opsporings)informatie gedeeld met de Politie, ontvangen bedrijven preventieve tips en kunnen zij trainingen volgen.

Argumenten

- Sterk toenemende dreiging en schade door cybercrime.
- MKB is een kwetsbare groep, ook in Amstelveen.
- Een digitale aanval op een onderneming kan het vermogen en de bestaanszekerheid van de onderneming aantasten.
- Een digitale aanval tast niet alleen de onderneming aan, maar ook de gezondheid van ondernemers.
- Ondernemers beheren gevoelige informatie, waaronder klantenbestanden met gegevens van onze inwoners die daardoor ook gevaar lopen
- Een cybermeldpunt met opvolging is een concept dat zich heeft bewezen in gemeente Velsen. De samenwerkende partners zijn tevreden, zo blijkt onder meer uit de tweede editie van Out of Business, het Cyber event van 2020-2022 van de Maritime Academie IJmuiden.
- De bijdrage van de gemeente richt zich op het initiëren en faciliteren van publiek-private samenwerking onder regie van het PVO.
- De Ondernemersvereniging Amstelveen geeft aan gebaat te zijn bij een dergelijke voorziening en geeft ook aan in dat verband een presentatie en training over cybercrime te willen organiseren.
- Een dergelijke voorziening geeft een stevige aanvulling op het huidige aanbod aan preventieve, informatieve en bewustwordingsmaatregelen en versterkt het digitale veiligheidsbeleid en bewustzijn.
- Een nader onderzoek naar de wensen en behoeften van het MKB borgt dat een dergelijke voorziening en samenwerking duurzaam en effectief is.
- Een pilot in Amstelveen voor de duur van een jaar geeft de mogelijkheid om hiermee te experimenteren en deze voorziening bij gebleken succes structureel te maken en regionaal uit te rollen.

Kanttekeningen

Veel mensen zijn nog te weinig bewust van de gevaren van cybercrime. Het is een minder tastbare vorm van criminaliteit, maar de impact kan groot zijn.
Als Raad kunnen wij de weerbaarheid tegen de snelle opmars van cybercrime helpen vergroten.
Zoals het gezegde: Als het kalf verdronken is dempt men de put, kunnen we voor zijn.

Financiën

1. Te dekken vanuit het budget veiligheid van maximaal € 15.000,- voor het nader onderzoeken van het oprichten en beheren van een Cybermeldpunt MKB Amstelveen, in combinatie met andere in Nederland effectief gebleken maatregelen
2. Aan te vragen Rijkssubsidie bij en samenwerking met het regionaal Platform Veilig Ondernemen.
3. Ondernemersvereniging Amstelveen en gemeente Amstelveen nauw te betrekken bij dit onderzoek, uitwerking van dit voorstel en mogelijke co-financieringsconstructies. .

4. Te dekken vanuit het budget veiligheid van maximaal €50.000,- voor het (co-)financieren van deze voorziening gedurende de pilotperiode.

Communicatie

In samenwerking met de betrokken partijen in het publiek private samenwerkingsverband wordt een communicatieplan uitgewerkt hoe het initiatief voor een publiek-private samenwerking, nader onderzoek, uitwerking en oprichting van een Cybermeldpunt MKB Amstelveen bekend worden gemaakt.

Procedure

1. Na een positief besluit van de raad, college verzoeken in contact te treden met PVO voor het initiëren van een publiek-privaat samenwerkingsverband met het MKB, Politie, PVO, gemeente(n) en IT security leverancier, voor het opzetten van een cybermeldpunt met 24/7 opvolging naar voorbeeld van het Cybermeldpunt Havengebied IJmuiden.
2. Hiertoe onder regie van het PVO een nader onderzoek uit te laten voeren voor het in kaart brengen van nadere wensen en behoeften om het voorstel zo duurzaam en effectief mogelijk uit te kunnen werken, inclusief mogelijke co-financieringsconstructies.
3. Bij een positieve afronding van het onderzoek en nadere uitwerking samen met het MKB, uitschrijven van een (onderhandse) aanbestedingsprocedure voor het aantrekken van een IT security leverancier die voldoet aan hoge eisen van betrouwbaarheid, geschiktheid en niveau van dienstverlening.
4. Zo dienen IT security leveranciers op zijn minst te voldoen aan de (inter)nationaal erkende ISO 27001 norm (eigen informatieveiligheid op orde), is het een pré als het bedrijf ervaring heeft met het opzetten van een meldpunt voor MKB en heeft relevante referenties. Politie wordt in dit verband gevraagd of zij het bedrijf kunnen screenen.
5. Onder regie van het PVO wordt voor de duur van de pilot een publiek-private samenwerking aangegaan en stemt de co-financieringsconstructie af met partijen.
6. Amstelveen vraagt voor dit doel door het Kabinet vrijgemaakte Rijkssubsidie aan bij het PVO.
7. Gezamenlijk met betrokken partijen wordt een datum bepaald wanneer het cybermeldpunt officieel van start gaat, de Raad wordt hierover geïnformeerd.
8. Na de pilotperiode wordt met betrokken partners geëvalueerd en wordt de voorziening bij gebleken succes structureel gemaakt.

Bijlagen

https://open.overheid.nl/repository/ronl-cfe6a43ba7cb72d8968f7001a68ea5751aef3e8e/1/pdf/tk-preventie-cybercrime-voor-het-midden-en-kleinbedrijf.pdf

https://www.ijmuiden.nl/kickstart-meldpunt-cybersecurity-haven-ijmuiden/

https://www.ioresearch.nl/actueel/veiligheidsmonitor-2021-meer-online-minder-traditionele-criminaliteit/

https://veiligheidscoalitie.nl/action/?action=download&id=1824

https://www.rpcnh.nl/nieuws/nieuws-item/er-zijn-kapers-op-de-kust-maar-we-zien-ze-niet/

https://hetccv.nl/onderwerpen/cybercrime/

Jacqueline Höcker
Raadslid Goed voor Amstelveen

Dit document wordt elektronisch ondertekend. Zie de elektronische handtekening(en) rechtsboven op pagina 1.