

RAADSINFORMATIEBRIEF

Zaaknummer: 690784
Documentnummer: 690785

Datum: 8-11-2024
Portefeuille(s): Informatiemanagement en Veiligheid
Portefeuillehouder(s): S.J. Lap en J.P. Gebben
Contactpersoon: M. Muizelaar
Te.nr: 691 **E-mail:** m.muizelaar@dronten.nl

Onderwerp: Art. 33 vragen fractie CDA omtrent Digitale Veiligheid gemeente Dronten.

Context

- ☐ Afdoening motie [naam / raadsvergadering d.d.]
- ☐ Afdoening toezegging [commissievergadering/raadsvergadering d.d.]
- ☒ Beantwoording raadsvragen
- ☐ Actuele bestuurlijke aangelegenheid
- ☐ Anders, [te weten...]

Aanleiding:

Naar aanleiding van gestelde vragen door raadslid Hermen van Eijken namens de fractie van het CDA, vindt u hierbij de schriftelijke beantwoording.

Beantwoording vragen:

Vraag 1: Kan het college aangeven welke maatregelen in de lokale driehoek (Gemeente, Politie, OM) zijn genomen of worden overwogen om inwoners te beschermen tegen cybercrime? Wordt de effectiviteit van de genomen maatregelen gemeten? Welke afwegingen moeten er nog gemaakt worden voordat een overwogen maatregel uitgevoerd kan worden?

De afgelopen jaren zien we een verschuiving van traditionele criminaliteit naar gedigitaliseerde criminaliteit. Delicten die buiten de digitale wereld ook plaatsvinden, kunnen door het gebruik van digitale middelen op grotere schaal en sneller gepleegd worden. Dit maakt het aanpakken van cybercriminelen ingewikkeld, aangezien hun methoden razendsnel kunnen veranderen.

Het college heeft in het dit jaar vastgestelde Integrale Veiligheidsbeleid 2024-2027 digitale veiligheid benoemd als een van de geprioriteerde thema's. Binnen dit thema wordt vooral ingezet op het versterken van de weerbaarheid en bewustwording van onze inwoners en ondernemers en het vergroten van het lokale netwerk van publieke en private (veiligheids-) partners. Hierbij werken we nauw samen met het Openbaar Ministerie, de politie en de gemeenten Urk en Noordoostpolder.

In de afgelopen periode zijn er in samenwerking met onze partners verschillende projecten uitgerold. Zo is samen met de Flevomeer Bibliotheek de training Laat je geen h@ck zetten ontwikkeld, gericht op het versterken van de weerbaarheid van senioren tegen digitale Bijlage(n):

oplichting. Vanuit het project Cyberchef heeft een succesvolle thema avond plaatsgevonden voor ondernemers en hebben studenten diverse bedrijven in de gemeente bezocht om hen te helpen bij het versterken van de digitale veiligheid van hun bedrijf. Momenteel wordt samen met de ondernemers en de onderwijsinstelling verkend hoe dit project een vervolg kan krijgen. Verder nemen we als gemeente al een aantal jaren deel aan Hackshield, een game die kinderen van de basisschool weerbaar maakt tegen cybercriminelen. Daarnaast komt er op landelijk en regionaal niveau steeds meer aandacht voor de verwevenheid van cybercrime met het thema ondermijning.

Het meten van de effectiviteit van de ingezette projecten is lastig omdat er nog weinig cijfers verzameld worden over gedigitaliseerde criminaliteit. Sinds kort registreert de politie slachtofferschap door gedigitaliseerde criminaliteit als aparte categorie. Deze cijfers geven echter een vertekenend beeld omdat veel mensen uit schaamte of onwetendheid geen melding of aangifte doen.

Ondanks de ingezette acties blijft het zoeken naar een effectieve en integrale aanpak. Veel wet- en regelgeving is gericht op onze fysieke leefwereld, waardoor de toepassing in de digitale wereld nog onbekend terrein is. Binnen de lokale driehoek is daarom ook aandacht voor kansrijke landelijke initiatieven die lokaal in Dronten ingezet zouden kunnen worden.

Vraag 2: Kan het college aangeven welk budget beschikbaar is om de weerbaarheid van inwoners tegen online criminaliteit te vergroten en hoe dit wordt uitgegeven(daders/slachtoffers, jongeren/senioren/ondernemers)?

Hoe is dit budget opgebouwd en vindt het college de hoogte van deze bedragen voldoende?

Er is op dit moment geen apart budget aangewezen voor het vergroten van de weerbaarheid van onze inwoners tegen online criminaliteit. Acties en maatregelen aangaande digitale veiligheid worden bekostigd vanuit het Integrale Veiligheidsbeleid (IVB). Voor het IVB is een jaarlijks budget beschikbaar van €112.500. Dit budget wordt verdeeld over de reguliere werkzaamheden en de zes geprioriteerd veiligheidsthema's, waaronder digitale veiligheid.

Op dit moment is het budget voldoende om diverse cyberprojecten gericht op inwoners, ondernemers en senioren uit te voeren. Wel ziet het college dat de dreiging van cybercriminelen een permanent karakter heeft gekregen en dat er binnen het veiligheidsdomein steeds meer aandacht komt voor het ontwikkelen van nieuwe maatregelen, projecten en instrumenten. Dit kan mogelijk betekenen dat het budget in de toekomst niet meer toereikend is.

Vraag 3: Kan het college aangeven welke kaders worden gebruikt voor het gebruik van AI binnen de gemeente/ gemeentelijke organisatie en afdelingen van Dronten?

Vorig jaar heeft de toenmalige CISO enkele kaders naar de interne organisatie gecommuniceerd. Dit betreft:

- a. Check altijd het antwoord van AI. AI kan schadelijke instructies, onjuiste informatie of bevooroordeelde inhoud opleveren. Ook is er vaak beperkte kennis van de wereld na 2021.
- b. Ook bij de toepassing van AI bijvoorbeeld objectherkenning en Robotic Process Automation (RPA) geldt dat alle uitkomsten gecontroleerd moeten worden.
- c. Vermeldt het gebruik van de AI bron (bijvoorbeeld Microsoft Copilot of



ChatGPT)

- d. Voer geen persoonsgegevens of andere gevoelige gegevens in bij het gebruik van AI. Alle informatie die ingevoerd wordt zal door het systeem gebruikt worden om verder te leren en te verbeteren.

Verder beleid omtrent AI wordt in 2025 vormgegeven.

Vraag 4: Kan het college (op hoofdlijnen) aangeven hoe de gemeente / gemeentelijke organisatie en afdelingen worden beschermd tegen kwaadwillende cyberacties van buiten de eigen organisatie?

De organisatie wordt ondersteund middels een SOC (security operations Centre) dienst via een commerciële partner waarbij diverse cybersecurity-technieken worden ingezet. Deze technieken worden doorlopend ontwikkeld en geïmplementeerd.

Vraag 5: Kan het college aangeven hoe de gemeente Dronten zich voorbereid op nieuwe Europese regelgeving zoals de AI Act en Cyber Beveiligingswet?

Er is een planning gemaakt die zich conformeert aan de planning die de AI Act als leidraad heeft. Daarnaast is Dronten bezig met kennissessies en het in beeld brengen van de juiste informatie, zodat er in 2025 begonnen kan worden met de uitvoering van verschillende facetten van deze wet.

Vraag 6: Kan het college aangeven hoe de bedrijfscontinuïteit binnen de gemeente Dronten is gewaarborgd bij digitale verstoringen. Worden hiervoor ook oefeningen gehouden. Zo nee, waarom niet?

De bedrijfscontinuïteit is deels geborgd door technische voorzieningen in uitwijk, welke jaarlijks worden getest. Tevens wordt (wettelijke verplicht) er een jaarlijkse uitwijktest gehouden vanuit burgerzaken. In 2025 wordt er verder doorontwikkeld op de voorzieningen en zullen meerdere processen vanuit continuïteitsmanagement worden aangesloten en bestaande voorzieningen worden verbeterd dan wel aangescherpt.

De focus ligt hierbij in eerste instantie op het waarborgen van de continuïteit van de primaire kritische bedrijfsprocessen. We volgen daarbij de aanwijzingen van de IBD bij het ontwikkelen van bedrijfscontinuïteitsbeheer (BCM) voor de top 13 gemeentelijke kritische processen en de belangrijkste ondersteunende bedrijfsprocessen. De prioriteit voor BCM is geadresseerd bij en geprioriteerd door de gemeentesecretaris en chief information officer op basis waarvan een aanpak volgens de richtlijnen van de IBD in ontwikkeling is.

Vraag 7: Kan het college aangeven of er binnen de eigen organisatie een crisisteam bestaat (of in ontwikkeling is) dat voorbereid is op cyberaanvallen? Zo nee, is het college voornemens zo'n team op te richten?

Vanuit de lokale crisisorganisatie heeft onze organisatie een crisisteam met diverse opgeleide medewerkers die zowel bij een fysieke crisis als een crisis met digitale componenten ingezet kan worden. Door te trainen met verschillende scenario's wordt het crisisteam voorbereid op een breed scala van crises. In navolging van de landelijke trends en ontwikkelingen wordt intern gewerkt aan het ontwikkelen van mogelijke scenario's gericht op cyberaanvallen.



Vraag 8: Kan het college aangeven in hoeverre de gemeente Dronten samenwerkt met ketenpartners / buurgemeenten om lokaal cyberveiligheid te waarborgen?

Is er bijvoorbeeld een periodiek overleg tussen betrokken functionarissen?

Ja, er is een twee maandelijks CISO (Chief Information Security Officer) overleg met buurgemeenten. Ook zijn we betrokken bij regionale kennisbijeenkomsten en zijn we betrokken bij de werkgroep BIO2 (Baseline Informatiebeveiliging Overheid) van de VNG.

Bijlage(n) bij deze raadsinformatiebrief

SV CDA Digitale Veiligheid gemeente Dronten



De Secretaris,
R. Hammenga MA



De Burgemeester,
drs. J.P. Gebben





schriftelijke vragen

Fractie:	CDA
Naam:	Hermen Van Eijken
Onderwerp:	Digitale veiligheid gemeente Dronten
Type vraag:	☐ informatieve/technische vraag ☒ politieke schriftelijke vraag (ex. art. 33 RvO)
Beantwoording (<i>alléén bij informatieve/technische vragen</i>)	☐ Ja, kan verspreid via mail / app ☐ Nee, alleen antwoord aan mij zelf

Inleiding/aanleiding:

Afgelopen jaren heeft cybercrime, waaronder online criminaliteit, in Nederland een enorme sprong genomen. Waar vroeger ICT-kennis nodig was om cybercrime te plegen is dat tegenwoordig niet meer nodig. Online criminaliteit neemt toe in het hele land. Zo waren er in 2023 in Midden-Nederland (onze regio) meer slachtoffers van online criminaliteit dan van woninginbraken, autokraken, (brom)fietsdiefstal en geweldsincidenten bij elkaar. (CBS, Veiligheidsmonitor 2023)

Bovendien kan één dader online snel veel slachtoffers maken. Dat vraagt om een andere aanpak dan bij traditionele criminaliteit.

Het is daarom cruciaal dat daders niet alleen (reactief) daders worden opgespoord, maar dat ook preventief en integraal online criminaliteit wordt voorkomen en verstoord. Dit vereist samenwerking tussen OM, gemeenten, politie en ketenpartners. Gemeenten kunnen zo actief bijdragen aan het verminderen van online criminaliteit.

Het CDA heeft hierover de volgende vragen:

1. Kan het college aangeven welke maatregelen in de lokale driehoek (Gemeente, Politie, OM) zijn genomen of worden overwogen om inwoners te beschermen tegen cybercrime? Wordt de effectiviteit van de genomen maatregelen gemeten? Welke afwegingen moeten er nog gemaakt worden voordat een overwogen maatregel uitgevoerd kan worden?
2. Kan het college aangeven welk budget beschikbaar is om de weerbaarheid van inwoners tegen online criminaliteit te vergroten en hoe dit wordt uitgegeven (daders/slachtoffers, jongeren/senioren/ondernemers)? Hoe is dit budget opgebouwd en vindt het college de hoogte van deze bedragen voldoende?

Digitalisering biedt kansen voor gemeenten, maar kent ook grote risico's binnen gemeentelijke organisaties.

Zo speelt Artificial Intelligence (AI) een steeds grotere rol in onze samenleving, ook binnen gemeentelijke organisaties. AI is aanwezig in alledaagse systemen en kan voordelen bieden. Maar de kans bestaat ook dat cruciale processen binnen afdelingen van de gemeente in ernstige mate verstoord raken of worden lam gelegd. Er zal dus veel nagedacht en overlegd moeten worden hoe een gemeente digitaal veilig kan (blijven) functioneren.

Dat vereist naast nieuwe kennis ook steeds meer samenwerking tussen gemeentes, onderling, maar ook intern tussen afdelingen en medewerk(st)ers.

Daarnaast moeten we ook kritisch blijven kijken naar de ethische en maatschappelijke gevolgen van AI.

Het CDA heeft hierover de volgende vragen:

3. Kan het college aangeven welke kaders worden gebruikt voor het gebruik van AI binnen de gemeente/ gemeentelijke organisatie en afdelingen van Dronten?
4. Kan het college (op hoofdlijnen) aangeven hoe de gemeente / gemeentelijke organisatie en afdelingen worden beschermd tegen kwaadwillende cyberacties van buiten de eigen organisatie?
5. Kan het college aangeven hoe de gemeente Dronten zich voorbereid op nieuwe Europese regelgeving zoals de AI Act en Cyber Beveiligingswet?
6. Kan het college aangeven hoe de bedrijfscontinuïteit binnen de gemeente Dronten is gewaarborgd bij digitale verstoringen. Worden hiervoor ook oefeningen gehouden. Zo nee, waarom niet?
7. Kan het college aangeven of er binnen de eigen organisatie een crisisteam bestaat (of in ontwikkeling is) dat voorbereid is op cyberaanvallen? Zo nee, is het college voornemens zo'n team op te richten?
8. Kan het college aangeven in hoeverre de gemeente Dronten samenwerkt met ketenpartners / buurgemeenten om lokaal cyberveiligheid te waarborgen? Is er bijvoorbeeld een periodiek overleg tussen betrokken functionarissen?