RAADSINFORMATIEBRIEF met beantwoording artikel 42 vragen

Van
college van burgemeester en wethouders

Vergadering van
1 november 2022

Kenmerk
Z/22/053030 / D/22/079433

Portefeuillehouder
Mariette Pennarts

Portefeuille
Informatieveiligheid

Opsteller
Wolff, Sandra de

Onderwerp
Cyberweerbaarheid gemeente Woerden

Beantwoording van de vragen
1. Heeft de gemeente Woerden een informatiebeveiligingsbeleid?

Ja. De gemeente Woerden heeft een strategisch informatiebeveiligingsbeleid. In 2023 komt er een nieuw informatiebeveiligingsbeleid.

2. Is de gemeente bekend met dit dreigingsbeeld van de IBD? Zo ja, heeft de gemeente op basis hiervan al maatregelen genomen of worden deze binnenkort genomen?

Ja, het dreigingsbeeld van de IBD is bekend. Het is nog niet bekend of we naar aanleiding van dit dreigingsbeeld aanvullende maatregelen gaan nemen. De beschreven risico's en aanbevelingen zijn immers al langer bekend. De IBD schrijft maar één keer in de twee jaar een dreigingsbeeld. De IBD geeft de gemeenten wel voortdurend informatie over risico's en kwetsbaarheden. Op basis hiervan nemen wij gepaste aanvullende maatregelen.

3. De gemeente Buren werd op 1 april 2022 getroffen door een geavanceerde ransomware – aanval waarbij er onder meer 130GB aan gegevens door de cybercriminelen op het darkweb werd gedeeld. Heeft de gemeente naar aanleiding van dit incident en het eerder genoemde dreigingsbeeld onderzocht of zij ook getroffen kan worden door een dergelijke aanval?
De gemeente Buren deelt actief via www.buren.nl, maar ook vanuit de IBD, informatie over de ransomware aanval. Op basis van deze informatie nemen wij waar nodig gepaste aanvullende maatregelen.
In de raadsbijeenkomst van 8 september 2022 hebben wij aangegeven dat een ransomware aanval ook bij ons kan gebeuren. Maar dat wij door het nemen van maatregelen de kans daarop proberen te verkleinen en onze weerbaarheid proberen te vergroten.

4. Indien de gemeente wel getroffen zou worden door ransomware aanval, heeft de gemeente dan maatregelen genomen die de impact verminderen, bijvoorbeeld door het hebben van goede back-ups en Dataloss Prevention systemen (DLP)? Met andere woorden, in hoeverre komt de dienstverlening van de gemeente en de veiligheid – en privacy van de inwoners van Woerden in het geding?
Naar aanleiding van toenemende ransomware aanvallen, waaronder die bij de gemeente Buren en de gemeente Hof van Twente, heeft de gemeente aanvullende maatregelen genomen. Dit is aan uw raad toegelicht in een informatiebijeenkomst van 8 september 2022. Meer informatie is te vinden in de besloten raadsinformatiebrieven D/22/060735 (7 juni 2022) en D/21/023153 (8 juni 2021).

5. Is het informatiebeveiligingsbeleid aangepast naar aanleiding van dit dreigingsbeeld of wordt dit op korte termijn

gedaan?
Het informatiebeveiligingsbeleid is een strategisch beleid op hoofdlijnen. Daarin staat beschreven dat de gemeente steeds op basis van risico's maatregelen neemt. Zie ook de antwoorden op vraag 1 en 2.

6. De BIO (Baseline Informatiebeveiliging Overheid) is een huidige en belangrijke richtlijn voor overheden, zowel landelijk als lokaal. Is de gemeente bekend met de BIO en zo ja, in hoeverre voldoet de gemeente Woerden aan deze richtlijn?
De gemeente kent de BIO en gebruikt de BIO als uitgangspunt. Elk jaar kijken we door middel van een zelfevaluatie naar de normen en bijbehorende maatregelen.

7.Indien de gemeente niet of slechts gedeeltelijk aan deze richtlijn voldoet, wat is hiervan de reden en welke maatregelen worden er genomen om alsnog aan de BIO te voldoen?
De BIO bestaat uit honderden normen en maatregelen. Elk jaar kijken we aan de hand van het dreigingsbeeld van de IBD en andere bronnen welke maatregelen voor ons het meeste bijdragen aan het verlagen van ons risicoprofiel.

8. De Cyber Security Raad hanteerde in 2017 reeds een ondergrens van 10 procent van het ICT budget als minimumbudget voor informatiebeveiliging en privacy6. Wat is het huidige ICT budget van de gemeente en welk percentage hiervan is gereserveerd voor informatiebeveiliging en privacy?
Er is geen vast percentage vastgelegd voor informatiebeveiliging en privacy. Dit omdat veel contracten gaan over zowel informatiebeveiliging, software als ondersteuning. Het is daarom niet mogelijk om dit percentage te berekenen. Een inschatting levert op dat de gemeente 10 procent als ondergrens haalt.

9. Door de corona-crisis is het thuis – en hybride werken sterk toegenomen. Het op afstand werken levert (mogelijk) extra risico's op cyberincidenten op, onder meer door de vaak minder goed beveiligde thuiswerkplekken. Heeft de gemeente hiervoor extra maatregelen genomen, zoals het verplichten van een VPN verbinding en 2-factor authenticatie (2FA) bij het inloggen op de IT-omgeving van de gemeente op afstand?
Ja.

10. Met de komst van NID2 (NIS2), de nieuwe Europese wetgeving op het gebied van cyberweerbaarheid worden beveiligingseisen aangescherpt, ook voor leveranciers, worden rapportageverplichtingen gestroomlijnd en komt er verscherpt toezicht. De verwachting is dat deze nieuwe richtlijn bovenop de BIO een grote impact gaat hebben op de eisen voor cyberweerbaarheid voor overheden en een groter aantal vitale organisaties. Is de gemeente Woerden bekend met de NID2 en is hiermee in het beleid en budget voor de komende jaren al rekening gehouden?
Wij zijn bekend met de NIS2 (NIB2). De staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties zegt hierover in de Kamerbrief van 29/09/2022) "Intussen is in Europa een voorlopig politiek akkoord bereikt over een herziening van Netwerk- en Informatiebeveiligingsrichtlijn (NIB2-richtlijn). Een belangrijke wijziging ten opzichte van de huidige richtlijn is dat overheidsdiensten binnen de reikwijdte van de richtlijn worden gebracht, en daarmee aan wettelijke verplichtingen voor de beveiliging van hun netwerk- en informatiesystemen moeten voldoen. Dit geldt in ieder geval voor de Rijksoverheid. De conceptrichtlijn stelt verder dat regionale en lokale overheden na een risicobeoordeling kunnen worden aangewezen. Ik wil de daarbij geldende criteria als uitgangspunt nemen, zoals de hierboven genoemde vitaal criteria. Eerder vermeldde ik dat het aantal processen dat hieraan voldoet, beperkt is. Ik verwacht daarom niet dat medeoverheden categoraal binnen de scope van NIB2 gaan komen."
Op basis van het bovenstaande zullen we nadat de richtlijn is omgezet in Nederlandse wetgeving een impactanalyse uitvoeren.

11.Vanuit de NID2 is er een verplichting op het zorgen voor zicht wat er binnen het IT – landschap (netwerk, devices en applicaties) van de gemeente gebeurt. In hoeverre is deze monitoring al aanwezig binnen de gemeente en bij welke partij is dit belegd?
In de raadsbijeenkomst van 8 september is dit geduid. Zoals aangegeven kunnen raadsleden altijd een afspraak maken met de teammanager ICT of Chief Information Security Officer (CISO) zodat zij kunnen laten zien op welke wijze zij de monitoring verzorgen. De gemeente doet een deel van de monitoring zelf en een deel is uitbesteed aan commerciële partijen. Dit om de continuïteit en deskundigheid te borgen.

Zo nee, heeft de gemeente plannen, eventueel in een samenwerkingsverband met andere gemeenten in het Groene Hart om dit te gaan regelen en zijn hiervoor al mogelijke dienstverleners in beeld?
Wij werken met omliggende gemeenten (Ronde Venen, Gouda, Stichtse Vecht, Montfoort, Diemen, Uithoorn, Ouder-Amstel, Alphen aan de Rijn en Wijdemeren) samen op het gebied van kennisdeling op het gebied van informatiebeveiliging.
Wij hebben dit voorlopig zelfstandig geregeld en staan open voor een samenwerking met andere gemeenten. We volgen de ontwikkelingen via de IBD.

12. Heeft de gemeente een draaiboek (een zogenoemd Incident Response plan) voor het geval er een cyberaanval of groot IT – incident plaatsvindt waardoor mogelijk de dienstverlening van de gemeente in het geding komt? Zo ja, oefent men binnen de gemeente periodiek aan de hand van dit plan?

Wij zijn bezig met een incident response plan. Dit wordt geïntegreerd met onze gemeente brede crisisplan Verder hebben we meegedaan met de overheidsbrede cyberoefening van 31 oktober jl. De deelnemers hebben ervaring op kunnen doen met hun rol, de samenwerking in het crisisteam en de crisisorganisatie als geheel, mocht er een soortgelijke calamiteit binnen onze organisatie spelen. We hebben meegedaan aan deze cyberoefening samen met Ferm Werk.

13. Zo nee, wat is de reden dat dit plan er niet is? Is de gemeente bereid hiervoor bijvoorbeeld de hulp van de IBD (VNG) in te roepen of een commerciële partij hiervoor in te schakelen?
De IBD heeft een handreiking gemaakt voor het incident response plan. Wij zijn nu bezig met een externe partij om aan de hand van deze handreiking dit plan op maat te maken voor de gemeenten Woerden en Oudewater.

14. Een belangrijke factor bij informatiebeveiliging en privacy is bewustzijn van medewerkers. Door informatiebeveiliging en gegevensbescherming te koppelen aan het werkproces zijn risico's herkenbaar voor medewerkers. Veel incidenten zijn terug te voeren op een gebrek aan digitaal bewustzijn. Hoe is het gesteld met het bewustzijn (awareness) van medewerkers van de gemeente als het gaat om cybersecurity en cybercrime? Is hiervoor door de gemeente voor de medewerkers een programma opgezet met bijvoorbeeld phishing testen of online trainingen? Zo nee, heeft de gemeente hier op korte termijn plannen voor en welke plannen zijn dit dan?
Wij hebben een awareness programma met oa phising testen, e-learning, nanolearning, acties in het bedrijfsrestaurant, pubquizen en binnenkort een escaperoom. De gemeenteraadsleden hebben sinds kort ook toegang tot de gemeentelijke ICT-omgeving. De gemeenteraadsleden zijn zelf verantwoordelijk voor veilig gedrag op het gebied van informatiebeveiliging. Zij kunnen in overleg met de griffie aansluiten bij een aantal onderdelen van het awareness programma.

15. Voorkomen is beter dan genezen, ook bij cybercrime. De politie heeft vanuit het Cyber Offender Prevention Squad8 een programma om cybercrime (onder jongeren en jongvolwassenen) te voorkomen en te ontmoedigen. Zijn de gemeente en/of de politie in Woerden hiermee bekend en zijn hieruit al concrete initiatieven gekomen?
Zie antwoord vraag 16

16. Staat de gemeente open voor partijen die samen met de politie dergelijke initiatieven zouden kunnen verzorgen?
De in het artikel genoemde programma's (hackright en hackshield) zijn bekend bij de politie en gemeente. Het programma/spel Hackshield is voor iedereen in Nederland speelbaar en heeft ook in Woerden al een aantal jonge inwoners bereikt.
De gemeente staat open om samen met de politie dergelijke initiatieven lokaal in te zetten. Bij het opstellen van het nieuw integraal veiligheidsplan 2023-2026 zal hier bij de uitwerking van het onderwerp cybercrime aandacht voor zijn. Hierbij kijken we concreet ook naar initiatieven die zich richten op preventie onder jeugd en jongvolwassen (zoals Hackshield).

17. Onze maatschappij is steeds meer afhankelijk van digitale middelen en digitale communicatie. Dat begint ook op steeds jongere leeftijd, waarbij ook zaken als sexting en cyberpesten al binnen het primair onderwijs voorkomen. Wat doet de gemeente om op scholen bij zowel leerkrachten, ouders als leerlingen het bewustzijn en daarmee de digitale weerbaarheid van inwoners te vergroten, ook uit oogpunt van eerdergenoemde preventie en ontmoediging van cybercrime?
De gemeente zet een de adviseur 'Gezonde School' in die de scholen actief adviseert en begeleidt bij de uitvoering van de Gezonde School aanpak. Mediawijsheid is één van de gezondheidsthema's van de gezonde school aanpak.

De gemeente heeft ook een maatschappelijke partner (Pretty Woman/Best Man) die voorlichting (o.a. sexting en sociale media) , hulpverlening, consultatie en deskundigheidsbevordering biedt over relaties, intimiteit, wensen & grenzen en seksualiteit.
Ondanks inspanningen van zowel Pretty Woman als de gemeente, lukt het niet voldoende om hun kennis en ervaring in te zetten voor het voortgezet onderwijs. Zij willen hier op investeren in 2023 en zijn in samenwerking met de gemeente, Hart voor Woerden en andere maatschappelijke partners in overleg om met een gezamenlijke aanpak de VO-scholen beter te gaan bereiken. De VO-scholen zijn er overigens vrij in om lesprogramma's of voorlichting al dan niet in te zetten in hun lesprogramma's.

18.Een recent gelanceerd initiatief vanuit het Ministerie van Justitie en Veiligheid is het Cyberrijbewijs10 dat zich specifiek richt op leerlingen van groep 7/8 in het PO. Is de gemeente hiermee bekend?
De gemeente is hiermee bekend. Het Cyberrijbewijs is een gratis lesprogramma dat bijdraagt aan de digitale weerbaarheid van leerlingen uit groep 7 en 8 van het primair onderwijs. Het programma wordt aangeboden via verschillende onderwijsplatforms. Scholen kunnen hier zelfstandig mee aan de slag gaan.

19. Staat de gemeente open voor partijen die een dergelijk programma samen met leerkrachten op de Woerdense basisscholen eventueel willen gaan verzorgen om zo de digitale geletterdheid en weerbaarheid van kinderen te vergroten?
Dit is niet van toepassing. Het Cyberrijbewijs is een gratis lesprogramma. Scholen kunnen hier zelfstandig mee aan de slag gaan.

Bijlagen
D/22/079432 Artikel 42 vragen Splinter Cyberweerbaarheid

Schriftelijke vragen – Cyberweerbaarheid gemeente Woerden

Inleiding
Het aantal cyberaanvallen op Nederlandse gemeenten is het afgelopen jaar verdubbeld en in de afgelopen twee jaar waren er vijf grote cyberincidenten in ons land[1]. Dat blijkt uit het nieuwe tweejaarlijkse Dreigingsbeeld van de Informatiebeveiligingsdienst (IBD) van de Vereniging Nederlandse Gemeenten (VNG)[2].

Het aantal incidenten neemt dus toe, het wordt steeds complexer om ze het hoofd te bieden en de impact is steeds ernstiger. Hierbij gaat het vooral om een toenemende dreiging van ransomware aanvallen waarbij cybercriminelen niet alleen bestanden versleutelen maar ook niet aarzelen om privacygevoelige gegevens van inwoners, bedrijven en medewerkers online te publiceren.

Dit dreigingsbeeld en de grote impact die ransomware aanvallen op onder meer de gemeente Buren[3] hebben gehad vraagt om een duidelijk beeld over de cyberweerbaarheid van de gemeente Woerden zeker ook gezien de komende Europese NID2 richtlijn die strengere eisen stelt aan de cyberweerbaarheid van organisaties en overheden.[4]

Schriftelijke vragen aan het college:
1. Heeft de gemeente Woerden een informatiebeveiligingsbeleid?
2. Is de gemeente bekend met dit dreigingsbeeld van de IBD? Zo ja, heeft de gemeente op basis hiervan al maatregelen genomen of worden deze binnenkort genomen?
3. De gemeente Buren werd op 1 april 2022 getroffen door een geavanceerde ransomware – aanval waarbij er onder meer 130GB aan gegevens door de cybercriminelen op het darkweb werd gedeeld. Heeft de gemeente naar aanleiding van dit incident en het eerder genoemde dreigingsbeeld onderzocht of zij ook getroffen kan worden door een dergelijke aanval?
4. Indien de gemeente wel getroffen zou worden door ransomware aanval, heeft de gemeente dan maatregelen genomen die de impact verminderen, bijvoorbeeld door het hebben van goede back-ups en Dataloss Prevention systemen (DLP)? Met andere woorden, in hoeverre komt de dienstverlening van de gemeente en de veiligheid – en privacy van de inwoners van Woerden in het geding?
5. Is het informatiebeveiligingsbeleid aangepast naar aanleiding van dit dreigingsbeeld of wordt dit op korte termijn gedaan?
6. De BIO (Baseline Informatiebeveiliging Overheid)[5] is een huidige en belangrijke richtlijn voor overheden, zowel landelijk als lokaal. Is de gemeente bekend met de BIO en zo ja, in hoeverre voldoet de gemeente Woerden aan deze richtlijn?
7. Indien de gemeente niet of slechts gedeeltelijk aan deze richtlijn voldoet, wat is hiervan de reden en welke maatregelen worden er genomen om alsnog aan de BIO te voldoen?
8. De Cyber Security Raad hanteerde in 2017 reeds een ondergrens van 10 procent van het ICT budget als minimumbudget voor informatiebeveiliging en privacy[6]. Wat is het huidige ICT budget van de gemeente en welk percentage hiervan is gereserveerd voor informatiebeveiliging en privacy?

[1] https://www.informatiebeveiligingsdienst.nl/nieuws/ibd-dreigingsbeeld-groeiende-dreiging-ransomware-aanvallen/
[2] https://www.informatiebeveiligingsdienst.nl/product/dreigingsbeeld-informatiebeveiliging-nederlandse-gemeenten-2023-2024/
[3] https://www.buren.nl/nieuws/datalek-gemeente-buren/7399/
[4] https://www.binnenlandsbestuur.nl/digitaal/omvang-en-impact-nis2-potentieel-enorm-voor-overheden

[5] https://www.informatiebeveiligingsdienst.nl/project/baseline-informatiebeveiliging-overheid/
[6] https://www.cybersecurityraad.nl/documenten/jaarplannen/2018/04/01/csr-meerjarenstrategie-2018-2021

9. Door de corona-crisis is het thuis – en hybride werken sterk toegenomen. Het op afstand werken levert (mogelijk) extra risico's op cyberincidenten op, onder meer door de vaak minder goed beveiligde thuiswerkplekken. Heeft de gemeente hiervoor extra maatregelen genomen, zoals het verplichten van een VPN verbinding en 2-factor authenticatie (2FA) bij het inloggen op de IT-omgeving van de gemeente op afstand?
10. Met de komst van NID2 (NIS2), de nieuwe Europese wetgeving op het gebied van cyberweerbaarheid worden beveiligingseisen aangescherpt, ook voor leveranciers, worden rapportageverplichtingen gestroomlijnd en komt er verscherpt toezicht. De verwachting is dat deze nieuwe richtlijn bovenop de BIO een grote impact gaat hebben op de eisen voor cyberweerbaarheid voor overheden en een groter aantal vitale organisaties. Is de gemeente Woerden bekend met de NID2 en is hiermee in het beleid en budget voor de komende jaren al rekening gehouden?
11. Vanuit de NID2 is er een verplichting op het zorgen voor zicht wat er binnen het IT – landschap (netwerk, devices en applicaties) van de gemeente gebeurt. In hoeverre is deze monitoring al aanwezig binnen de gemeente en bij welke partij is dit belegd?
12. Zo nee, heeft de gemeente plannen, eventueel in een samenwerkingsverband met andere gemeenten in het Groene Hart om dit te gaan regelen en zijn hiervoor al mogelijke dienstverleners in beeld?
13. Heeft de gemeente een draaiboek (een zogenoemd Incident Response plan) voor het geval er een cyberaanval of groot IT – incident plaatsvindt waardoor mogelijk de dienstverlening van de gemeente in het geding komt? Zo ja, oefent men binnen de gemeente periodiek aan de hand van dit plan?
14. Zo nee, wat is de reden dat dit plan er niet is? Is de gemeente bereid hiervoor bijvoorbeeld de hulp van de IBD (VNG) in te roepen of een commerciële partij hiervoor in te schakelen?
15. Een belangrijke factor bij informatiebeveiliging en privacy is bewustzijn van medewerkers. Door informatiebeveiliging en gegevensbescherming te koppelen aan het werkproces zijn risico's herkenbaar voor medewerkers. Veel incidenten zijn terug te voeren op een gebrek aan digitaal bewustzijn. Hoe is het gesteld met het bewustzijn (awareness) van medewerkers van de gemeente als het gaat om cybersecurity en cybercrime? Is hiervoor door de gemeente voor de medewerkers een programma opgezet met bijvoorbeeld phishing testen of online trainingen? Zo nee, heeft de gemeente hier op korte termijn plannen voor en welke plannen zijn dit dan?
16. Voorkomen is beter dan genezen, ook bij cybercrime. De politie heeft vanuit het Cyber Offender Prevention Squad[7] een programma om cybercrime (onder jongeren en jongvolwassenen) te voorkomen en te ontmoedigen. Zijn de gemeente en/of de politie in Woerden hiermee bekend en zijn hieruit al concrete initiatieven gekomen?
17. Staat de gemeente open voor partijen die samen met de politie dergelijke initiatieven zouden kunnen verzorgen?
18. Onze maatschappij is steeds meer afhankelijk van digitale middelen en digitale communicatie. Dat begint ook op steeds jongere leeftijd, waarbij ook zaken als sexting en cyberpesten al binnen het primair onderwijs voorkomen[8]. Wat doet de gemeente om op scholen bij zowel leerkrachten, ouders als leerlingen het bewustzijn en daarmee de digitale weerbaarheid van inwoners te vergroten, ook uit oogpunt van eerdergenoemde preventie en ontmoediging van cybercrime?

[7] https://magazines.cybersecurityraad.nl/csrmagazine/2022/01/16.-waarom-wachten-tot-het-fout-gaat-ook-daderpreventie-is-cybersecurity

[8] https://www.rtlnieuws.nl/nieuws/nederland/artikel/5279337/online-shaming-kinderen-basisschool-groep7-groep8-naaktfoto-webcam

19. Een recent gelanceerd initiatief vanuit het Ministerie van Justitie en Veiligheid is het Cyberrijbewijs[9] dat zich specifiek richt op leerlingen van groep 7/8 in het PO. Is de gemeente hiermee bekend?
20. Staat de gemeente open voor partijen die een dergelijk programma samen met leerkrachten op de Woerdense basisscholen eventueel willen gaan verzorgen om zo de digitale geletterdheid en weerbaarheid van kinderen te vergroten?

Femke Merel van Kooten
Splinter

[9] https://mijncyberrijbewijs.nl