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