Schriftelijke vraag

Artikel 54 Reglement van orde voor de vergaderingen
en andere werkzaamheden van de Raad

Zaaknummer: **83852-2024**

Schriftelijke vraag aan	☒ het college van burgemeester en wethouders	☐ de burgemeester

Onderwerp: defensie storing op 28 augustus 2024 en de cyberweerbaarheid van de gemeente Maashorst

Naar aanleiding van de storing op 28 augustus 2024, die veroorzaakt werd door een softwarefout in het Netherlands Armed Forces Integrated Network (NAFIN) en gevolgen had voor diverse overheidsdiensten, waaronder DigiD, heeft het CDA zorgen over de cyberweerbaarheid van de gemeente.

De storing heeft laten zien dat overheidsdiensten kwetsbaar zijn voor IT-problemen. Verder kun je in het nieuws dagelijks verhalen lezen over storingen en datalekken in IT-systemen. Dit roept de vraag op of onze gemeentelijke IT-systemen voldoende beschermd zijn tegen vergelijkbare incidenten. De bescherming van persoonsgegevens van onze burgers is van essentieel belang. We moeten erop kunnen vertrouwen dat de gemeente adequaat beveiligd is tegen aanvallen die kunnen leiden tot datalekken of verstoring van essentiële diensten. Het CDA heeft signalen opgepakt dat deze storing invloed had op de dienstverlening van de gemeente Maashorst.

Gezien deze overwegingen heeft het CDA de volgende vragen over de impact van de storing op 28 augustus en de bredere cyberweerbaarheid van de gemeente Maashorst:

1. **Had de storing van 28 augustus 2024 invloed op de IT-systemen en essentiële diensten van de gemeente Maashorst, zoals de aanvraag van rijbewijzen en paspoorten?**
    - Zo ja, welke diensten waren getroffen, hoe lang duurde de verstoring en welke maatregelen zijn genomen om de continuïteit te waarborgen?
    - Indien nee, welke maatregelen zijn genomen om te voorkomen dat deze storing invloed had op onze systemen?
2. **Zijn er sinds het begin van de bestuursperiode andere incidenten geweest waarbij de IT-systemen van de gemeente getroffen zijn door storingen of cyberaanvallen?**
    - Zo ja, welke stappen zijn toen ondernomen om de dienstverlening te herstellen en toekomstige uitval te voorkomen?
    - Heeft dit ooit geleid tot datalekken van gegevens van burgers?
3. **Welke stappen onderneemt de gemeente Maashorst om haar weerbaarheid tegen cyberaanvallen te versterken, gezien de toenemende dreigingen die zijn aangetoond in verschillende onderzoeken, zoals het CloudFlare-rapport dat stelt dat 83% van de Nederlandse bedrijven verwacht slachtoffer te worden van een cyberaanval?**
    - Zijn er concrete maatregelen, zoals het implementeren van moderne veiligheidsarchitecturen (bijv. secure access service edge (SASE) of zero-trust-netwerken), die momenteel worden toegepast om de gemeentelijke systemen beter te beschermen?
    - Vindt het college dat de persoonsgegevens van onze burgers voldoende beschermd zijn tegen cyberaanvallen?

- Maakt de aanwezigheid van Vliegbasis Volkel, een strategische militaire locatie, onze gemeente extra kwetsbaar voor cyberdreigingen? Welke maatregelen worden er genomen om deze risico's te beperken?

4. **Maakt de gemeente Maashorst gebruik van audits of sociale hackers om de veiligheid van haar IT-systemen actief te testen en te verbeteren?**
   - Zo ja, welke bevindingen en verbeteracties zijn hieruit voortgekomen?
   - Indien nee, waarom wordt dit niet toegepast en overweegt de gemeente dit in de toekomst in te zetten?
5. **Is het college bereid de raad voortaan actief te informeren over aanvallen en storingen in de gemeentelijke IT-systemen wanneer deze invloed hebben op essentiële diensten of burgergegevens, inclusief de oorzaken, getroffen diensten en de genomen maatregelen om deze problemen te verhelpen en toekomstige uitval te voorkomen?**

Met de toenemende dreiging van cyberaanvallen en de groeiende afhankelijkheid van digitale systemen voor gemeentelijke dienstverlening, is het naar onze mening van groot belang dat de gemeente haar digitale weerbaarheid blijft versterken en de raad tijdig op de hoogte stelt van incidenten die invloed hebben op onze burgers.

Bronnen:
Storing 28 augustus:
https://nos.nl/liveblog/2534860-storing-kwam-door-fout-in-softwarecode-systemen-starten-weer-op
CloudFlare rapport:
https://www.computable.nl/2024/06/20/nederland-relatief-vaak-dupe-van-cyberaanvallen/

Ondertekening:

Datum indiening	:	24-10-2024
Fractie	:	CDA
Naam indiener	:	Niek Bongaerts
Einddatum	:	30-11-2024
Id. Nr. Ibabs	:	102

Antwoord op schriftelijke vraag

Artikel 54 Reglement van orde voor de vergaderingen
en andere werkzaamheden van de Raad

Antwoord door: ☒ college van burgemeester en wethouders	☐ burgemeester
Datum: 29-10-2024	

Vraag:
Onderwerp: defensie storing op 28 augustus 2024 en de cyberweerbaarheid van de gemeente Maashorst

Naar aanleiding van de storing op 28 augustus 2024, die veroorzaakt werd door een softwarefout in het Netherlands Armed Forces Integrated Network (NAFIN) en gevolgen had voor diverse overheidsdiensten, waaronder DigiD, heeft het CDA zorgen over de cyberweerbaarheid van de gemeente.

De storing heeft laten zien dat overheidsdiensten kwetsbaar zijn voor IT-problemen. Verder kun je in het nieuws dagelijks verhalen lezen over storingen en datalekken in IT-systemen. Dit roept de vraag op of onze gemeentelijke IT-systemen voldoende beschermd zijn tegen vergelijkbare incidenten. De bescherming van persoonsgegevens van onze burgers is van essentieel belang. We moeten erop kunnen vertrouwen dat de gemeente adequaat beveiligd is tegen aanvallen die kunnen leiden tot datalekken of verstoring van essentiële diensten. Het CDA heeft signalen opgepakt dat deze storing invloed had op de dienstverlening van de gemeente Maashorst.

Gezien deze overwegingen heeft het CDA de volgende vragen over de impact van de storing op 28 augustus en de bredere cyberweerbaarheid van de gemeente Maashorst:

1. **Had de storing van 28 augustus 2024 invloed op de IT-systemen en essentiële diensten van de gemeente Maashorst, zoals de aanvraag van rijbewijzen en paspoorten?**
    - Zo ja, welke diensten waren getroffen, hoe lang duurde de verstoring en welke maatregelen zijn genomen om de continuïteit te waarborgen?
    - Indien nee, welke maatregelen zijn genomen om te voorkomen dat deze storing invloed had op onze systemen?
2. **Zijn er sinds het begin van de bestuursperiode andere incidenten geweest waarbij de IT-systemen van de gemeente getroffen zijn door storingen of cyberaanvallen?**
    - Zo ja, welke stappen zijn toen ondernomen om de dienstverlening te herstellen en toekomstige uitval te voorkomen?
    - Heeft dit ooit geleid tot datalekken van gegevens van burgers?
3. **Welke stappen onderneemt de gemeente Maashorst om haar weerbaarheid tegen cyberaanvallen te versterken, gezien de toenemende dreigingen die zijn aangetoond in verschillende onderzoeken, zoals het CloudFlare-rapport dat stelt dat 83% van de Nederlandse bedrijven verwacht slachtoffer te worden van een cyberaanval?**
    - Zijn er concrete maatregelen, zoals het implementeren van moderne veiligheidsarchitecturen (bijv. secure access service edge (SASE) of zero-trust-netwerken), die momenteel worden toegepast om de gemeentelijke systemen beter te beschermen?
    - Vindt het college dat de persoonsgegevens van onze burgers voldoende beschermd zijn tegen cyberaanvallen?

- Maakt de aanwezigheid van Vliegbasis Volkel, een strategische militaire locatie, onze gemeente extra kwetsbaar voor cyberdreigingen? Welke maatregelen worden er genomen om deze risico's te beperken?

4. **Maakt de gemeente Maashorst gebruik van audits of sociale hackers om de veiligheid van haar IT-systemen actief te testen en te verbeteren?**
   - Zo ja, welke bevindingen en verbeteracties zijn hieruit voortgekomen?
   - Indien nee, waarom wordt dit niet toegepast en overweegt de gemeente dit in de toekomst in te zetten?
5. **Is het college bereid de raad voortaan actief te informeren over aanvallen en storingen in de gemeentelijke IT-systemen wanneer deze invloed hebben op essentiële diensten of burgergegevens, inclusief de oorzaken, getroffen diensten en de genomen maatregelen om deze problemen te verhelpen en toekomstige uitval te voorkomen?**

Met de toenemende dreiging van cyberaanvallen en de groeiende afhankelijkheid van digitale systemen voor gemeentelijke dienstverlening, is het naar onze mening van groot belang dat de gemeente haar digitale weerbaarheid blijft versterken en de raad tijdig op de hoogte stelt van incidenten die invloed hebben op onze burgers.

Bronnen:
Storing 28 augustus:
https://nos.nl/liveblog/2534860-storing-kwam-door-fout-in-softwarecode-systemen-starten-weer-op
CloudFlare rapport:
https://www.computable.nl/2024/06/20/nederland-relatief-vaak-dupe-van-cyberaanvallen/

Antwoord:

1. **Had de storing van 28 augustus 2024 invloed op de IT-systemen en essentiële diensten van de gemeente Maashorst, zoals de aanvraag van rijbewijzen en paspoorten?**

Ja, de storing had invloed op primaire diensten van nagenoeg alle Nederlandse gemeenten.
De storing heeft van 27 augustus in de avond tot 28 augustus in de middag geduurd en betrof alle diensten die van het landelijke beveiligde Diginetwerk gebruik maken. De getroffen diensten waren met name: DigiD inloggen, aanvragen/uitgifte van identiteitsdocumenten en buiten gemeentelijke BRP bevragingen. Het Diginetwerk biedt beveiligde verbindingen naar landelijke voorzieningen. Diverse primaire diensten kunnen niet opereren zonder deze landelijke voorzieningen omdat benodigde brongegevens daarin beheerd worden.

2. **Zijn er sinds het begin van de bestuursperiode andere incidenten geweest waarbij de IT-systemen van de gemeente getroffen zijn door storingen of cyberaanvallen?**

<u>Verstoringen</u>
Zoals u zelf aangeeft is iedere dag wel een verstoring in het nieuws. Vaak halen alleen grote en langdurige verstoringen het nieuws. In de praktijk komen kleine verstoringen nog veel vaker voor. De meeste verstoringen hebben geen invloed op onze dienstverlening. Wanneer de gemeente gebruik maakt van de betreffende specifieke dienst of netwerk kunnen wij ook worden getroffen. Wij nemen hier waar mogelijk mitigerende (risico beperkende) maatregelen tegen, echter blijven we in bepaalde mate afhankelijk van externe partijen. De meeste verstoringen worden door externe partijen veroorzaakt. Om dit geheel in perspectief te plaatsen: Onze diensten zijn ondanks deze afhankelijkheden in 2024 voor 99,998% operationeel.

Cyberaanvallen
Cyberaanvallen vinden continu plaats. Iedere paar seconden wordt er wel een poging gedaan. Daarom gaat ook veel aandacht uit naar de beveiliging van onze systemen. Tot op heden hebben onze systemen alle aanvallen afgeslagen en zijn er géén verstoringen veroorzaakt door een cyberaanval. Datalekken als gevolg van een cyberaanval zijn dan ook nog niet voorgekomen.

3. **Welke stappen onderneemt de gemeente Maashorst om haar weerbaarheid tegen cyberaanvallen te versterken, gezien de toenemende dreigingen die zijn aangetoond in verschillende onderzoeken, zoals het CloudFlare-rapport dat stelt dat 83% van de Nederlandse bedrijven verwacht slachtoffer te worden van een cyberaanval?**

Beveiligingssystemen en technieken
Wij zorgen dat onze systemen up-to-date zijn. Daarnaast blijven wij onze beveiligingsmaatregelen ontwikkelen en investeren we geregeld in nieuwe systemen of technieken. Wij worden hierbij ondersteund door externe partijen. De gemeente past bepaalde onderdelen van SASE toe en is bezig met de opbouw van een ZTNA (interne segmentatie en beveiliging op basis van rollen).

Mitigerende maatregelen
Wij passen netwerksegmentatie toe om te voorkomen dat een breuk in de beveiliging van één systeem zou leiden tot toegang tot alle systemen. Wij hebben voor onze back-up en uitwijk maatregelen getroffen om een eventuele infectie van onze gegevens te weren uit back-up data.
Wij voeren een strikt toegangsbeleid waarbij we gebruik maken van twee-staps verificatie met gebruikersinteractie (nummer matching) waarmee het bemoeilijkt wordt onterecht toegang te verkrijgen.
Om het risico op malafide websites en phishing te verkleinen passen we link scanning toe op onze omgeving waarmee links voordat deze gevolgd worden eerst gecontroleerd worden. Binnen het gemeentehuis is er daarnaast ook sprake van webfiltering waarmee ongewenste en malafide websites geblokkeerd worden.
Voor de continuïteit van onze eigen diensten hebben we, waar mogelijk, redundantie (dubbele uitvoering) toegepast. Zo hebben we verschillende internetlijnen in de gemeente, kunnen ICT systemen uitwijken naar de gemeentewerf en maken we concrete afspraken met (cloud)leveranciers over beschikbaarheid en veiligheid van hun systemen.
De systemen die we inzetten genereren ook zogeheten log- en monitoring informatie. Deze informatie volgen wij (samen met externe dienstverleners) actief op om vroegtijdig zwakheden te signaleren en op te lossen.

Audits en pentesten
Wij worden jaarlijks ge-audit op onze beveiliging. Dit betreft de Eenduidige Normatiek Single Information Audit (ENSIA) en een IT audit bij de accountantscontrole. Daarnaast laten we jaarlijks een zogenaamde penetratietest uitvoeren door een ethische hacker. Verder hebben wij Cyberoefeningen in de planning staan en zijn we bezig met het verbeteren van risicoanalyses.
De regelgeving waar wij aan moeten voldoen op dit vlak wordt ook ieder jaar verder aangescherpt.

Bewustwording
Het meest oncontroleerbare veiligheidsrisico in IT beveiliging blijft de mens. Op het moment dat de deur niet op slot wordt gemaakt is het makkelijk inbreken. Er worden daarom geregeld bewustwordingscampagnes gehouden. Ook moeten alle medewerkers een online training volgen.

Slag om de arm

Goede beveiligingsmaatregelen en bewustwording zijn essentieel. Een organisatie blijft enigszins ook afhankelijk van de mate waarop de aanvalskracht wordt uitgevoerd.

Wij moeten meebewegen met de situatie in de wereld. Onderwerpen als AI en Kwantumcomputers gaan nieuwe bedreigingen vormen. Ook geopolitieke situaties en ondermijning hebben invloed. Zo ook de aanwezigheid van de vliegbasis. Risico's worden in kaart gebracht en zullen waar nodig leiden tot de inzet van extra beveiligingsmaatregelen. Verhoogde beveiligingsrisico's worden door het Nationaal Cyber Security Centrum (NCSC) en Informatie Beveiligingsdienst (IBD) aan ons gemeld.
Eerder heeft u ingestemd met additionele middelen om de beveiligingsmaatregelen uit te breiden. Ook in de toekomst zullen wij moeten blijven meebewegen met ontwikkelingen.

4. **Maakt de gemeente Maashorst gebruik van audits of sociale hackers om de veiligheid van haar IT-systemen actief te testen en te verbeteren?**

Ja, zie ook antwoord op vraag 2, onderdeel audits en pentesten.
Bevindingen uit audits worden gerapporteerd en mitigerende maatregelen worden genomen dan wel opgenomen in de jaarplanning.
Verder heeft de Gemeente Maashorst een Responsible Disclosure op de website staan, dit stelt ethische hackers in staat om zelf fouten te melden die zij vinden. Uit deze hoek krijgen wij tot nu toe geen meldingen.

5. **Is het college bereid de raad voortaan actief te informeren over aanvallen en storingen in de gemeentelijke IT-systemen wanneer deze invloed hebben op essentiële diensten of burgergegevens, inclusief de oorzaken, getroffen diensten en de genomen maatregelen om deze problemen te verhelpen en toekomstige uitval te voorkomen?**

Wanneer onze dienstverlening wordt geraakt zullen wij allereerst de direct betrokkenen informeren. Ook rapporteert het college jaarlijks de resultaten van de audits aan de gemeenteraad, welke u bij jaarrekening vaststelt.

Het college is aanvullend bereid de raad te informeren bij meerdaagse verstoringen die de primaire dienstverlening richting inwoners, bedrijven en maatschappelijke instellingen raken en zal hier verantwoording over af leggen.