



Schriftelijke vragen

Reg. Nr. 2025-11

Datum:	14-05-2025
Van:	Joost Dikker Hupkes (D66 voor Heerde)
Aan:	College
Onderwerp:	Informatiebeveiliging
Datum beantwoording:	04-06-2025
Behandeld in college van:	03-06-2025

Toelichting

Wij willen inzicht verkrijgen in de situatie t.a.v. informatiebeveiliging in de gemeente Heerde. Niet alleen vanuit een risicoperspectief, maar ook om te toetsen of wij als gemeente voldoende voorbereid zijn op incidenten die – helaas – andere vergelijkbare gemeenten niet bespaard zijn gebleven.

Context:

De digitale veiligheid van overheden staat steeds vaker onder druk. Gemeenten verwerken grote hoeveelheden gevoelige informatie, waaronder persoonsgegevens van inwoners, gegevens over sociale voorzieningen en interne beleidsdocumenten. De gevolgen van een beveiligingsincident kunnen groot zijn, zowel financieel als in termen van vertrouwen in het openbaar bestuur.

Daarnaast is het belangrijk om te realiseren dat sommige van de hieronder genoemde gemeenten voldeden aan alle geldende eisen t.a.v. informatiebeveiliging en desalniettemin getroffen werden.

Voorbeelden uit de praktijk zijn:

- Hof van Twente (2020): Volledige gemeentelijke infrastructuur platgelegd door een ransomware-aanval, schade >€4 miljoen.
- Lochem (2022): Gevoelige persoonsgegevens via de website openbaar toegankelijk, reputatieschade en melding bij de Autoriteit Persoonsgegevens.
- Zutphen (2023): Phishing-aanval leidde tot toegang tot interne e-mails en gegevens.

Geleerde lessen in deze gemeenten:

- noodzaak van offsite back-ups en herstelplannen
- investering in bewustwording en training van medewerkers
- invoering van meervoudige authenticatie
- toename van samenwerking met o.a. de Informatiebeveiligingsdienst (IBD)
- regelmatige uitvoering van penetratietests en risicoanalyses

Graag de volgende vraag/vragen schriftelijk beantwoorden

1. Is in kaart gebracht welke systemen en processen nooit mogen stilvallen in onze gemeente? Welke maatregelen nemen we om deze risico's te 'managen'? Volstaan deze maatregelen?
2. Kunnen we in het geval van een calamiteit uitwijken naar of samenwerken met een andere gemeente?

3. Hoe staat het college er tegenover aandacht te besteden aan informatiebeveiliging en eventueel de CISO daarvoor uit te nodigen, op een (eventueel besloten) themaraad of op een ander geschikte manier?

Antwoord

1. Is in kaart gebracht welke systemen en processen nooit mogen stilvallen in onze gemeente?

Welke maatregelen nemen we om deze risico's te 'managen'? Volstaan deze maatregelen?

De H2O gemeenten hanteren een breed scala aan beveiligingsmaatregelen. Toch is niet uit te sluiten dat één of meerdere processen stilvallen. Om in een dergelijk geval gericht te kunnen handelen is een Bedrijfscontinuïteitsplan opgesteld. Hierin zijn onder andere verantwoordelijkheden, communicatielijnen en prioriteiten (welke processen zo belangrijk dat ze eigenlijk niet stil mogen vallen en moeten als eerste hersteld worden) vastgelegd. Aan de verdieping van dit plan wordt op dit moment nog gewerkt. Voor de gemeente Heerde wordt hierin per proces uitgewerkt; welke systemen gebruikt worden, hoe deze hersteld moeten worden, met welke prioriteit en hoe eventueel zonder systeem verder gewerkt kan worden.

2. Kunnen we in het geval van een calamiteit uitwijken naar of samenwerken met een andere gemeente?

Fysiek uitwijken naar een andere H2O gemeente is geregeld. Dit scenario treedt in werking bij bijvoorbeeld een lokale stroomstoring of calamiteit in Heerde waardoor niet op de kantoren van gemeente Heerde gewerkt kan worden. Verder kennen we binnen H2O twee datacentra (in Zwolle en in Oldebroek) die elkaar kunnen overnemen. De uitwijk bestaat in dat geval uit het overschakelen naar het tweede datacentrum.

3. Hoe staat het college er tegenover aandacht te besteden aan informatiebeveiliging en eventueel de CISO daarvoor uit te nodigen, op een (eventueel besloten) themaraad of op een ander geschikte manier?

In de 3-raden bijeenkomst op 4 juni zijn de raden onder andere bijgepraat over de ontwikkelingen op het gebied van informatieveiligheid. Wanneer hier nog een verdieping op gewenst is, zouden we uiteraard graag in een themaraad aandacht besteden aan Informatieveiligheid. We kunnen hierin onder andere een toelichting op de door u aangegeven geleerde lessen voor gemeenten geven en de laatste resultaten van de ENSIA zelfevaluatie toelichten.