



Schriftelijke vragen

Reg. Nr. 2026-Sv007

Datum: 12-05-2026
Van: Joost Dikker Hupkes
Aan: College via gemeentesecretaris
Onderwerp: Informatiebeveiliging naar
aanleiding van het datalek bij
gemeente Epe
[xx]-[xx]-20[xx]

Datum beantwoording:
Behandeld in college van:

[in te vullen door de organisatie]
[in te vullen door de organisatie]

Toelichting

Recent is onze buurgemeente Epe getroffen door een ernstig datalek. Volgens de berichtgeving van de gemeente Epe kregen hackers op 10 maart 2026 via de zogeheten ClickFix-methode toegang tot het gemeentelijke netwerk. Er zijn vervolgens bijna 552.000 bestanden van een interne bestandsserver gedownload. Uit onderzoek blijkt dat waarschijnlijk persoonsgegevens van bijna alle inwoners van Epe zijn gestolen, waaronder naam, adres, geboortedatum, geboorteplaats/-land, geslacht en BSN. In sommige gevallen ging het ook om aanvullende gegevens, zoals bankrekeningnummers of kopieën van identiteitsbewijzen.

De gemeente Heerde maakt voor ICT-diensten gebruik van H2O/i-Dienst, samen met de gemeenten Hattem en Oldebroek. Het incident in Epe roept de vraag op of vergelijkbare risico's ook bij ons kunnen spelen bij onze ICT-dienst (bedrijfsvoeringsorganisatie H2O/i-Dienst) en welke maatregelen zijn genomen of kunnen worden genomen om een vergelijkbaar incident te voorkomen.

Aanvullende context

De risico's rond digitale veiligheid nemen toe. Nieuwe AI-toepassingen maken het niet alleen eenvoudiger om overtuigende phishingberichten, nepmeldingen en andere vormen van misleiding te maken, maar ook om aanvallen sneller, gericht en op grotere schaal voor te bereiden. Kwaadwillenden kunnen op geautomatiseerde wijze informatie verzamelen over meerdere gemeenten, per organisatie mogelijke kwetsbaarheden inschatten en vervolgens de meest kansrijke methode kiezen. Daardoor is niet alleen technische beveiliging van belang, maar ook de inrichting van werkprocessen, toegangsrechten, opslag van bestanden, logging en het tijdig signaleren van afwijkend gedrag.

Inwoners moeten erop kunnen vertrouwen dat de gemeente zorgvuldig omgaat met hun gegevens. Zij zijn in veel gevallen verplicht om persoonsgegevens, BSN's, financiële gegevens of kopieën van identiteitsbewijzen aan de gemeente te verstrekken. Juist omdat inwoners die keuze vaak niet vrij hebben, rust op de gemeente een extra verantwoordelijkheid om deze gegevens veilig te verwerken, niet langer te bewaren dan nodig is en alleen toegankelijk te maken voor medewerkers die deze gegevens daadwerkelijk nodig hebben.

Graag de volgende vragen schriftelijk beantwoorden:

1. Is het college bekend met de aard en omvang van het datalek bij onze buurgemeente Epe, en welke concrete lessen heeft het college hieruit tot nu toe getrokken voor de gemeente Heerde?
2. Welke stappen zijn ondernomen of welke acties zijn uitgezet, naar aanleiding van dit incident binnen de gemeente Heerde en/of binnen H2O/i-Dienst?
3. Hoe worden de uitkomsten van het verdere onderzoek in Epe gevolgd en beoordeeld op mogelijke relevantie voor de gemeente Heerde en H2O/i-Dienst?
4. Wordt de gemeenteraad geïnformeerd wanneer uit dit verdere onderzoek nieuwe inzichten of maatregelen voortkomen die relevant zijn voor de informatiebeveiliging van de gemeente Heerde, zo nodig besloten of vertrouwelijk?
5. Is het college bereid een gerichte risicoanalyse of quickscan uit te voeren naar opslag, toegang, logging en beveiliging van persoonsgegevens binnen de gemeente Heerde, en de raad daarover — zo nodig besloten of vertrouwelijk — te informeren?
6. Kan het college aangeven of binnen de gemeente Heerde grote hoeveelheden persoonsgegevens, BSN's, aanvragen, bezwaarschriften, kopieën van identiteitsbewijzen of andere gevoelige documenten op één plek of in gedeelde opslagomgevingen worden bewaard?
7. Hoe is geregeld waar tijdelijke bestanden met persoonsgegevens mogen worden opgeslagen, en hoe wordt geborgd dat deze bestanden tijdig worden verwijderd of verplaatst naar daarvoor bedoelde systemen?
8. Wordt binnen de ICT-omgeving van Heerde onderscheid gemaakt in toegang tot gegevens op basis van functie, rol en noodzaak voor de werkzaamheden?
9. Zijn extra gevoelige gegevens, zoals BSN's, kopieën van identiteitsbewijzen, gegevens rond voorzieningen, bezwaarprocedures of het sociaal domein, afgeschermd van algemene werkmappen en algemene medewerkersaccounts?
10. Is onderzocht wat het maximale schadebereik zou zijn wanneer één reguliere gemeentelijke werkplek of één regulier medewerkersaccount wordt gecompromitteerd?
11. Worden ongebruikelijke activiteiten, zoals bulkdownload, bulkexport of toegang tot grote hoeveelheden persoonsgegevens, automatisch gesignaleerd? Zo ja, wie ontvangt deze meldingen en hoe snel wordt daarop gereageerd? Zo nee, is het college bereid te onderzoeken of dergelijke signalering kan worden ingericht?
12. Welke procedure volgt het college bij een vergelijkbaar datalek of cyberincident, en is daarin vastgelegd wanneer en hoe inwoners en de gemeenteraad worden geïnformeerd, zo nodig besloten of vertrouwelijk?