



Beantwoording schriftelijke vragen

Reg. Nr. 2026-Sv007

Datum:	24-06-2026
Van:	College
Aan:	Joost Dikker Hupkes
Onderwerp:	Informatiebeveiliging naar aanleiding van het datalek bij gemeente Epe
Datum beantwoording:	17-06-2026
Behandeld in college van:	23-06-2026

Inleiding

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 bestandserver 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 Phishing berichten, nepmeldingen en andere vormen van misleiding te maken, maar ook om aanvallen sneller, gericht en op grotere schaal voor te bereiden. Kwaadwillende 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.

Antwoord

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?

Antwoord: De hack bij gemeente Epe en de gevolgen daarvan zijn bekend. Gemeente Epe heeft samen met de Informatiebeveiligingsdienst (IBD) de gevolgen van het cyberincident uitgebreid geëvalueerd. Daarbij is gekeken naar de organisatorische, financiële en communicatieve impact. De evaluatie levert belangrijke lessen op voor andere gemeenten, zoals het belang van een projectmatige aanpak en open communicatie met inwoners tijdens een crisis. Ook geeft het rapport inzicht in de kosten die het incident heeft veroorzaakt.

Volgens de evaluatie van de Informatiebeveiligingsdienst voor gemeenten (IBD) ontstond de hack bij Gemeente Epe door een zogeheten ClickFix-aanval. Daarbij werd een medewerker via een nepbericht of misleidende melding verleid om handelingen uit te voeren waarmee hackers toegang kregen tot het gemeentelijke netwerk. Na de eerste toegang maakten de aanvallers gebruik van onvoldoende beveiligde accounts en legitieme beheertools om zich verder door het netwerk te bewegen. Hierdoor konden zij uiteindelijk ruim 552.000 bestanden downloaden van een interne bestandsserver, waaronder persoonsgegevens van vrijwel alle inwoners van Epe. De IBD concludeert dat het ging om een professionele en gecoördineerde cyberaanval waarbij meerdere technieken werden gecombineerd. De gemeente heeft na ontdekking de toegang direct geblokkeerd en extra beveiligingsmaatregelen ingevoerd'.

Op basis van deze informatie zal binnen de H2O-gemeenten gekeken worden of verdere maatregelen genomen moeten worden. Als het substantiële maatregelen zijn zal het college van B&W hierover worden geïnformeerd, zo nodig besloten of vertrouwelijk.

De volledige evaluatie van gemeente Epe is te vinden via <https://www.epe.nl/datalek>.

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?

Antwoord: Naar aanleiding van dit incident zijn er vooralsnog geen extra maatregelen genomen of acties uitgezet, één van de bestaande maatregelen is dat een standaardgebruikers binnen de H2O-omgeving geen rechten heeft voor PowerShell, Run-venster en Command Prompt [CMD]. Na een incident zoals in Epe controleren we extra goed of onze toegangsrechten, logging en bewustwordingsmaatregelen voldoende zijn. Waar nodig verbeteren we deze maatregelen verder.

In de basis nemen we al verschillende technische en organisatorische maatregelen om gegevens goed te beveiligen. Denk aan veilige inlogmethoden, het bijhouden en controleren van activiteiten, antivirussoftware, beveiliging van apparaten, het regelmatig uitvoeren van updates en het zoveel mogelijk scheiden van netwerken.

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?

Antwoord: Gemeente Epe heeft samen met de Informatiebeveiligingsdienst (IBD) de gevolgen van het cyberincident uitgebreid geëvalueerd en de resultaten gepubliceerd. Daarnaast zijn de CISO's van de omliggende gemeenten in Noord Oost Gelderland uitgenodigd voor een besloten kennissessie 'hack gemeente Epe'. Uit de beschikbare informatie en evaluatie blijkt dat, gelet op de huidige H2O IT-inrichting, vooralsnog geen extra maatregelen nodig zijn.

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?

Antwoord: Ja, het verdere onderzoek zal onze gemeente inzicht geven in de status van onze informatiebeveiliging. Afhankelijk van aard en omvang van deze inzichten zullen wij de raad daarover informeren.

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?

Antwoord: Gezien de hierna genoemde periodieke testen en auditing lijkt een dergelijke risicoanalyse of quickscan niet van toegevoegde waarde: jaarlijks wordt de PEN-test op de IT-omgeving uitgevoerd in opdracht van de Bedrijfsvoeringsorganisatie en daarnaast wordt de Raad jaarlijks geïnformeerd, d.m.v. de ENSIA¹ verantwoording, over de resultaten van jaarlijkse [verplichte] DigiD-audit en ENSIA-onderwerpen. De toezichthouder Logius stelt de ICT-beveiligingsassessment verplicht om de veiligheid van DigiD-koppelingen² te borgen, om aan te tonen dat de gevoelige persoonsgegevens van burgers optimaal beschermd zijn, en om het vertrouwen in de digitale overheid te garanderen. De audits worden uitgevoerd door een externe gecertificeerde auditor.

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?

Antwoord: We maken geen gebruik van gedeelde opslagomgevingen, alle data moet worden opgeslagen in de daarvoor bestemde/aangewezen Taak Specifieke Applicaties [TSA], denk hierbij aan het Zaaksysteem (Verseon en Djuma), de Basis Registratie Persoonsgegevens, i-Participatie, i-Sam/c-Sam, YouForce. Desondanks dienen we rekening te houden met het 'gedrag' van medewerkers, wat het belang van bewustwording benadrukt.

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?

Antwoord: Onderdeel Bewustwording en gedrag van medewerkers. Alle medewerkers hebben een beveiligde persoonlijke map waar ze tijdelijk een bestand kunnen opslaan. Informatie die centraal binnenkomt wordt op basis van werkinstructies bewaard en verwijderd.

8. Wordt binnen de ICT-omgeving van Heerde onderscheid gemaakt in toegang tot gegevens op basis van functie, rol en noodzaak voor de werkzaamheden?

Antwoord: Ja Gebruikers krijgen alleen toegang tot informatie, netwerken en de systemen of delen van systemen waarvoor zij specifiek bevoegd zijn. Uitgangspunt voor het verlenen van toegang tot systemen is het "need-to-know" en/of "need-to-use" principe. Afhankelijk van de rol of taak van de gebruiker worden autorisaties voor toegang tot informatie en/of systemen toegekend door of namens de proceseigenaar.

De principes "need-to-know" en "need-to-use" gelden voor alle gebruikers en typen gebruikersaccounts. Op dit moment wordt de autorisatieverlening nog per individu vastgesteld. We bekijken de mogelijkheden om toe te werken naar standaard profielen.

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 medewerker accounts?

¹ Eenduidige Normatiek Single Information Audit

² de technische verbinding tussen een website van de gemeente en het DigiD-systeem van de overheid. Hierdoor kunnen burgers veilig inloggen met hun DigiD om online zaken te regelen. Denk hierbij o.a. aan Burgerzaken en belastingen.

Antwoord: Ja, de gewenste betrouwbaarheid van informatie en informatiesystemen wordt bepaald met behulp van een BIV-classificatie. BIV staat voor Beschikbaarheid, Integriteit en Vertrouwelijkheid. Bij een BIV-classificatie wordt door middel van een risicoanalyse het gewenste betrouwbaarheidsniveau van informatie en informatiesystemen vastgesteld. Hierbij worden de indicaties Laag, Midden, Hoog en Zeer Hoog (of alleen de beginletters ervan) gehanteerd. Die indicaties geven richting aan de maatregelen die genomen moeten worden waaronder de authenticatie methode. Zie ook antwoord vraag 8.

10. Is onderzocht wat het maximale schadebereik zou zijn wanneer één reguliere gemeentelijke werkplek of één regulier medewerkers account wordt gecompromitteerd?

Antwoord: Nee. Het [maximale] schadebereik is niet alleen afhankelijk van de type gebruiker/medewerker maar ook van veel andere [directe en indirecte] factoren. Zie:

Schade bepalen van een cyberincident | NCSC [veilige koppeling]

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?

Antwoord: Bepaalde ongebruikelijke activiteiten worden gesignaleerd en notificaties worden verstuurd naar de systeembeheerder. Het is zijn of haar taak om bij dergelijke meldingen direct actie te ondernemen.

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?

Antwoord: Deze onderwerpen (procedure, communicatieplan etc.) staan beschreven in het Strategisch Continuïteitsplan Informatievoorziening H2O.