gemeente Deventer

Nota voor Burgemeester en Wethouders

Bestuursorgaan	:	Burgemeester en Wethouders
Onderwerp	:	Vragen ex art. 46 RvO-DENK-Cyberaanval gemeente Epe
Portefeuillehouder	:	Burgemeester
Notanummer	:	2026-362
Datum B&W-vergadering	:	12-05-2026
Team	:	Afdeling Concernstaf
Programma	:	01 - Burger en bestuur
Parafen voor akkoord nota	:	• 11-05-2026: Manager Digitalisering en Data • 07-05-2026: Burgemeester
Parafen voor agendering	:	• 07-05-2026: Gemeentesecretaris/algemeen directeur
Bijlagen bij deze nota	:	2026-04-25 Vragen art 46 RvO - DENK - Cyberaanval gem Epe.docx,Antwoordbrief vragen ex art 46 RvO-DENK-Cyberaanval gemeente Epe.docx
Datum definitieve akkoord	:	12-05-2026

Besluit

1. De beantwoording van de vragen ex art 46 RvO van de DENK-fractie vast te stellen
2. De beantwoording aan te bieden aan de raad

De nota en het besluit openbaar te maken

Inleiding

Per brief van 25 april 2026 heeft A. Kaya van de fractie van DENK uw college een aantal schriftelijke vragen ex art 46 RvO gesteld over Cyberaanval gemeente Epe. Bijgaand treft u de beantwoording aan.

Beoogd maatschappelijk resultaat

Kader

Betrokken partijen en participatie

Argumenten voor en tegen

Financiële consequenties en dekking

Openbaarmaking en communicatie

Aanpak en uitvoering

Deventer, 25 april 2026

Betreft: Schriftelijke vragen naar aanleiding van de cyberaanval op de gemeente Epe – Cybersecurity en informatiebeveiliging gemeente Deventer

Geacht college van B&W,

De recente, ernstige cyberaanval op de gemeente Epe heeft pijnlijk duidelijk gemaakt hoe kwetsbaar lokale overheden kunnen zijn voor digitale dreigingen en wat de verstrekkende gevolgen kunnen zijn voor de dienstverlening en de privacy van inwoners. Deze gebeurtenis onderstreept de noodzaak om ook in onze gemeente de digitale weerbaarheid continu tegen het licht te houden.

Namens de fractie van DENK Deventer legt ondergetekende, met een beroep op artikel 46 van het Reglement van Orde, de volgende vragen voor aan het College van Burgemeester en Wethouders:

1. In hoeverre voldoen de informatiesystemen van de gemeente Deventer aan de Baseline Informatiebeveiliging Overheid (BIO), op welke onderdelen wordt hier momenteel nog niet volledig aan voldaan, en wanneer heeft de laatste onafhankelijke audit plaatsgevonden inclusief de mogelijkheid voor de raad om de resultaten in te zien?

2. Laat de gemeente periodiek penetratietests uitvoeren en hoe wordt omgegaan met gevonden kwetsbaarheden, inclusief concrete opvolging en terugkoppeling aan de raad?

3. In welke mate is Deventer afhankelijk van externe IT-leveranciers, en hoe borgt het college dat deze partijen aantoonbaar voldoen aan dezelfde beveiligingseisen?

4. Heeft de gemeente de afgelopen jaren te maken gehad met datalekken of cyberincidenten, en beschikt zij over een actueel en aantoonbaar getest crisis- en herstelplan (bijvoorbeeld bij ransomware), mede gelet op de scenario's die zich in Epe hebben voorgedaan?

5. Hoe worden gevoelige persoonsgegevens (zoals BSN en gegevens binnen het sociaal domein) technisch beschermd binnen de gemeente Deventer (bijv. via versleuteling en toegangsbeheer), en binnen welke termijn worden inwoners concreet geïnformeerd bij een datalek?

6. Gelet op de recente cyberaanval bij de gemeente Epe en incidenten bij andere gemeenten, acht het college de digitale weerbaarheid van Deventer op dit moment voldoende, en welke concrete extra verbetermaatregelen met planning zijn voorzien om een vergelijkbaar scenario in Deventer te voorkomen?

In afwachting van uw beantwoording,

Fractie DENK Deventer

Ahmet Kaya

Grote Kerkhof 1
Postbus 5000
7400 GC Deventer

14 0570
telefoon

Aan de fractie van DENK
t.a.v.

direct telefoonnummer

A. Kaya

gemeente@deventer.nl
e-mail

Interne Post

2026-362		12 mei 2026
kenmerk	uw referentie	datum
S.B. van der Velden	Schriftelijke vragen ex art 46 RvO	

Geachte heer Kaya,

Naar aanleiding van uw schriftelijke vragen over de cyberaanval op de gemeente Epe en de digitale weerbaarheid van de gemeente Deventer informeren wij u als volgt.

Vraag 1
In hoeverre voldoen de informatiesystemen van de gemeente Deventer aan de Baseline Informatiebeveiliging Overheid (BIO), op welke onderdelen wordt hier momenteel nog niet volledig aan voldaan, en wanneer heeft de laatste onafhankelijke audit plaatsgevonden inclusief de mogelijkheid voor de raad om de resultaten in te zien?
Antwoord
De gemeente Deventer hanteert de Baseline Informatiebeveiliging Overheid (BIO) als normenkader voor haar informatiebeveiliging. In belangrijke mate voldoen onze informatiesystemen aan deze norm. Dit toetsen we periodiek met een BIO-gap-analyse. Ook wordt er gewerkt aan ISO 27001-certificeringen voor de domeinen IT, HR en FZ. Op onderdelen waar nog verbetering nodig is, gaat het met name om organisatorische en mensgerichte maatregelen. De gemeente Deventer laat periodiek onafhankelijke audits uitvoeren. In 2025 zijn er audits uitgevoerd voor DigiD en Suwinet. Deze voldeden aan de gestelde normen.
De gemeenteraad wordt via het CISO-jaarverslag geïnformeerd over de resultaten van deze audits. De uitkomsten worden verwerkt in verbeterplannen, waaronder het jaarplan voor informatiebeveiliging voor 2026, dat aan de raad beschikbaar wordt gesteld.

Vraag 2
Laat de gemeente periodiek penetratietests uitvoeren en hoe wordt omgegaan met gevonden kwetsbaarheden, inclusief concrete opvolging en terugkoppeling aan de raad?
Antwoord
De gemeente Deventer laat periodiek penetratietests en zogeheten ‘Red Teaming’-acties uitvoeren op kritische systemen, infrastructuur en op de organisatie. Daarnaast worden alle IT-systemen doorlopend gescand op nieuwe of aanwezige kwetsbaarheden met behulp van gespecialiseerde tooling. Geconstateerde kwetsbaarheden worden geprioriteerd op basis van risico en vervolgens verholpen. Hiervoor zijn processen ingericht.

Vraag 3
In welke mate is de gemeente Deventer afhankelijk van externe IT-leveranciers, en hoe borgt het college dat deze partijen aantoonbaar voldoen aan dezelfde beveiligingseisen?
Antwoord
De gemeente Deventer maakt, net als andere organisaties, gebruik van externe IT-leveranciers voor systemen en applicaties die de bedrijfsvoering en dienstverlening ondersteunen. Bij aanbestedingen en contracten gelden strikte aansluitvoorwaarden, welke gebaseerd zijn op de BIO en relevante wet- en regelgeving. Het naleven van deze beveiligingseisen door leveranciers wordt gevalideerd via onafhankelijke toetsingen, zoals ISO 27001- en SOC 2-certificeringen. Nieuwe applicaties en leveranciers worden daarnaast vooraf onderworpen aan een risicoanalyse.

Vraag 4
Heeft de gemeente de afgelopen jaren te maken gehad met datalekken of cyberincidenten, en beschikt zij over een actueel en aantoonbaar getest crisis- en herstelplan (bijvoorbeeld bij ransomware), mede gelet op de scenario's die zich in Epe hebben voorgedaan?
Antwoord
De gemeente Deventer heeft de afgelopen jaren, zoals veel organisaties, te maken gehad met datalekken. Waar nodig zijn deze gemeld bij de Autoriteit Persoonsgegevens. Er hebben zich geen incidenten voorgedaan zoals bij de gemeente Epe. De gemeente Deventer beschikt over een actueel cybercrisis- en herstelplan. Deze plannen worden periodiek geactualiseerd, mede op basis van actuele dreigingen en ervaringen van andere organisaties. Lessen uit incidenten bij andere overheden en organisaties worden gebruikt om de eigen IT-inrichting en cybercrisisaanpak te toetsen en waar nodig aan te scherpen. Het herstelplan van de gemeente bevat een uitgewerkt scenario voor logisch verlies, zoals ransomware-aanvallen.

Vraag 5
Hoe worden gevoelige persoonsgegevens (zoals BSN en gegevens binnen het sociaal domein) technisch beschermd binnen de gemeente Deventer (bijv. via versleuteling en toegangsbeheer), en binnen welke termijn worden inwoners concreet geïnformeerd bij een datalek?
Antwoord
Voor het beschermen van gevoelige persoonsgegevens wordt een breed scala aan passende technische en organisatorische maatregelen toegepast. Dit is een doorlopend proces.
De specifieke beheersmaatregelen (bepaalde versleuteling of toegangsbeheer) zijn per situatie of systeem verschillend. De toepassing van de BIO is hierin leidend. Wanneer een datalek mogelijk een hoog risico voor de betrokkenen oplevert, worden zij hierover geïnformeerd conform de Algemene Verordening Gegevensbescherming (AVG). Betrokkenen worden zo spoedig mogelijk geïnformeerd. Daarnaast wordt binnen 72 uur na ontdekking van het incident een (voorlopige) melding gedaan bij de Autoriteit Persoonsgegevens.

Vraag 6
Gelet op de recente cyberaanval bij de gemeente Epe en incidenten bij andere gemeenten, acht het college de digitale weerbaarheid van Deventer op dit moment voldoende, en welke concrete extra verbetermaatregelen met planning zijn voorzien om een vergelijkbaar scenario in Deventer te voorkomen?
Antwoord
Het college acht de digitale weerbaarheid van de gemeente Deventer op dit moment adequaat, maar benadrukt dat voortdurende verbetering noodzakelijk is. Absolute weerbaarheid bestaat niet. De menselijke factor speelt daarin een cruciale rol, zoals ook is gebleken bij de gemeente Epe. De werkwijze bij de aanval op de gemeente is daarom behandeld in ons bewustwordingsprogramma voor medewerkers. Daarnaast is een analyse uitgevoerd op basis van de beschikbare informatie over dit incident. De hieruit voortgekomen aandachtspunten zijn beoordeeld en waar nodig zijn passende maatregelen genomen.

Wij vertrouwen erop u hiermee voldoende te hebben geïnformeerd.

Met vriendelijke groet,

Burgemeester en wethouders van de gemeente Deventer,

de secretaris,	de burgemeester,
J.P. Wassens	R.C. König