Gemeente Epe

INFORMATIE BEVEILIGINGS DIENST

# Evaluatie

## Datalek Gemeente Epe: evaluatie en verantwoording

| | |
|---|---|
| **Van** | College van burgemeester en wethouders in samenwerking met de Informatiebeveiligingsdienst voor gemeenten (IBD) |
| **Status** | DEFINITIEF |
| **Datum** | 4 juni 2026 |
| **Onderwerp** | Evaluatie datalek maart 2026: verantwoording en verbetermaatregelen |
| **Kenmerk** | 1428935 |
| **Bijlage:** | 1. Forensische Rapportage Eye Security |

## 1. Inleiding

Op 10 maart 2026 hebben hackers via een zogeheten ClickFix-aanval toegang gekregen tot het netwerk van Gemeente Epe. Daarbij zijn grote hoeveelheden gemeentelijke data gestolen, waaronder (persoons)gegevens van inwoners, medewerkers, contractpartners en leveranciers. Het college informeert de raad met deze brief over het verloop van het incident, de genomen maatregelen en de structurele verbeteringen die zijn of worden doorgevoerd.

Het technisch en forensisch onderzoek is volledig afgerond en het rapport is als bijlage bijgevoegd. Communicatie aan betrokkenen en autoriteiten vond parallel aan het onderzoek plaats en werd afgestemd op de beschikbare informatie over de aard en omvang van het datalek. De huidige nazorgfase bestaat uit de opvolging van de communicatie met betrokkenen, begeleiding bij vervanging van identiteitsbewijzen voor personen van wie een kopie is aangetroffen in de data, doorlopende monitoring op misbruik van de gegevens en implementatie van structurele verbeteringen in de informatiebeveiliging.

Deze evaluatie is opgesteld in samenwerking met de Informatiebeveiligingsdienst voor gemeenten (IBD), onderdeel van de Vereniging van Nederlandse Gemeenten (VNG). De IBD ondersteunt gemeenten op het gebied van informatiebeveiliging en privacy. De IBD is voor gemeenten het schakelpunt met het Nationaal Cyber Security Centrum (NCSC).

## 2. Wat is er gebeurd?

### 2.1 Het incident

Op 12 maart 2026 constateerde de IT-dienstverlener van de gemeente Epe een ongeautoriseerde toegang tot de ICT-omgeving van Gemeente Epe. Na direct forensisch onderzoek, uitgevoerd door Eye Security, een gespecialiseerde externe incidentresponspartij, is de aanval gereconstrueerd. Het betreft een professionele cyberaanval in drie fasen, waarbij de aanvaller meerdere technieken combineerde, legitieme hulpprogramma's inzette en gecoördineerd door het netwerk bewoog.

### Verloop van de aanval

**Stap 1: De aanvaller komt binnen**: Een medewerker bezocht een website en werd daar misleid om zonder het te weten een schadelijk programma te starten (ClickFix). Daarmee kreeg de aanvaller toegang tot de computer van die medewerker. Het account van de medewerker was beveiligd met multifactor authenticatie (MFA). MFA beschermt effectief tegen aanvallers die een wachtwoord hebben bemachtigd, maar biedt geen bescherming tegen een aanval waarbij de gebruiker zelf (onbewust) schadelijke code uitvoert op zijn eigen werkplek. De ClickFix-aanval is juist op die manier opgezet: de aanvaller omzeilt MFA structureel door de gebruiker te misleiden tot het zelf uitvoeren van de aanval.

**Stap 2: De aanvaller zorgt dat hij meer kan op het systeem**: Eenmaal binnen ging de aanvaller op zoek naar andere ingelogde gebruikers, die hebben voor een bepaalde tijd een toegangsticket voor het systeem (een kerberosticket) en dat ticket is te ontsleutelen met het wachtwoord. Het lukte de aanvaller om een wachtwoord van een ingelogde beheerder te kraken en zo op het ticket van de beheerder binnen te komen. Ook dit account had MFA ingesteld. Vervolgens kreeg de aanvaller ook toegang tot een noodaccount met ruime toegangsrechten op het systeem. Zo'n noodaccount kan worden gezien als een loper die op alle sloten van het systeem past. Een dergelijk account heeft in de regel geen MFA omdat deze wordt gebruikt als noodtoegang voor het geval een normale toegang niet meer mogelijk is.

**Stap 3: De gegevens worden gestolen:** Met die ruime toegang kopieerde de aanvaller met behulp van een normaal hulpprogramma (AzCopy) circa 871 GB aan data, ruim 550.000 bestanden, naar externe cloudopslag (Azure Blob Storage).

## 2.2 Welke gegevens zijn getroffen?

De gelekte data stond op een interne bestandsserver die zou worden uitgefaseerd vanwege de geplande migratie naar SharePoint en Microsoft Teams. De server stond op de planning voor uitfasering in 2026. De volgende categorieën gegevens zijn getroffen:

- Een export uit de Basisregistratie Personen (BRP) met persoonsgegevens van inwoners, waaronder naam, adres, geslacht, woonplaats, geboortedatum en BSN.
- Persoonsgegevens van medewerkers, waaronder namen, e-mailadressen, zakelijke telefoonnummers, datum indiensttreding en profielfoto's.
- Financiële gegevens van de gemeente en haar relaties.
- Bedrijfsgegevens en contractinformatie van contractrelaties.
- Aanvragen voor gemeentelijke voorzieningen, meldingen van overlast of verstoring van de openbare orde, waarbij niet in alle gevallen nauwkeurig is te achterhalen over welke personen het gaat.
- Kopieën van 1.022 identiteitsbewijzen, waarvan er na verder onderzoek 845 nog geldig waren.

De gemeente heeft vastgesteld dat de data tot op moment van schrijven niet is gepubliceerd op bekende leksites of marktplaatsen. De gemeente heeft opdracht gegeven tot het monitoren van het dark web. Het datalek is niet opgeëist en er is geen losgeld geëist. Er zijn tot op heden geen indicaties van misbruik van de data.

# 3. Hoe heeft de gemeente gehandeld?

## 3.1 Eerste crisisfase (week 11-12, maart 2026)

- Direct na ontdekking heeft de IT-dienstverlener van de gemeente Epe de ICT-omgeving geïsoleerd en is Eye Security ingeschakeld voor forensisch onderzoek en het veilig herstel van de IT-omgeving.
- Alle gebruikers-, service- en beheerdersaccounts zijn gereset, inclusief het break-glass account.
- Persistentiemechanismen (kwaadaardige scheduled tasks) zijn verwijderd en systemen zijn gecontroleerd.
- De Gemeente Epe heeft het incident op 13 maart, binnen de wettelijke termijn van 72 uur, voorlopig gemeld bij de Autoriteit Persoonsgegevens (AP). Op 18 maart is de melding aangevuld met aanvullende bevindingen. Op 8 mei is de melding verder aangevuld en definitief gemaakt.
- De gemeente heeft direct melding gemaakt bij de politie en het OM en alle informatie uit de technische onderzoeken is gedeeld. Het apparaat van waaruit de ClickFix is gestart is voor onderzoek aan de politie beschikbaar gesteld. De gemeente heeft ook formeel aangifte gedaan.
- De gemeente heeft een melding gedaan bij de Informatiebeveiligingsdienst voor gemeenten (IBD) die ook het Nationaal Cyber Security Centrum (NCSC) heeft betrokken. De IBD heeft de gemeente doorlopend geadviseerd bij de incidentrespons.
- College, gemeenteraad en medewerkers, ketenpartners en de pers zijn geïnformeerd.
- Inwoners zijn en worden geïnformeerd via de website, sociale media, de speciale projectpagina www.epe.nl/datalek en via een huis-aan-huis-brief.

## 3.2 Projectmatige aanpak (week 13-21, april-mei 2026)

Direct na de initiële crisisfase is een projectstructuur ingericht onder leiding van een externe projectleider met ervaring bij eerdere gemeentelijke digitale incidenten. De burgemeester en gemeentesecretaris zijn bestuurlijk en ambtelijk opdrachtgever en een stuurgroep bestaande uit leden van het managementteam van de gemeente zorgt voor de operationele aansturing.

Het project kent drie deelprojecten:

- Deelproject 1: Onderzoek, Data & Techniek: volledige technische reconstructie, inventarisatie van gelekte data en risico-inschatting.
- Deelproject 2: Communicatie & Informatievoorziening: gerichte communicatie naar alle doelgroepen op basis van risicoprofiel.
- Deelproject 3: Nazorg & Verbetering: maatregelen ter verlaging van het risico (zoals vervangen identiteitsbewijzen voor personen van wie een kopie is aangetroffen in de data), evaluatie, aanbevelingen en borging van verbeteringen in de organisatie.

## 3.3 Communicatie naar betrokkenen

De gemeente heeft alle betrokkenen zo specifiek mogelijk geïnformeerd, afgestemd op het risicoprofiel en de beschikbare informatie. Daarbij is specialistisch advies ingewonnen over communicatiewijzen en handelingsperspectief:

- Inwoners: via een nieuwsbericht, een speciale projectpagina op de gemeentelijke website, en een huis-aan-huis-brief zodra voldoende duidelijkheid was over de aard van de gelekte data en het handelingsperspectief.
- Pers: via persberichten en een persgesprek om het informatiebereik verder te vergroten.
- Medewerkers: bericht via intranet en nadere informatie via teamleiders, inclusief handelingsperspectief.
- Betrokkenen met bijzondere persoonsgegevens: persoonlijk contact.
- Contractrelaties: via een informatiebrief met het verzoek om alert te zijn op signalen uit de samenleving.
- Betrokkenen van wie een kopie van een geldig identiteitsbewijs is aangetroffen: via een persoonlijke brief met aanbod om het document op kosten van de Gemeente Epe te vervangen.

## 3.4 Timing van de communicatie

De relevante momenten rondom de communicatie zijn weergegeven in onderstaande tabel.

| Datum | Gebeurtenis |
|---|---|
| **12 maart 2026**<br>*Donderdag* | **Ontdekking inbraak**<br>De inbraak wordt ontdekt. Er is op dit moment nog onvoldoende zekerheid over de aard en omvang van het incident om verantwoord extern te communiceren. |
| **13 maart 2026**<br>*Vrijdagavond* | **Bevestiging diefstal bestanden**<br>Gemeente Epe constateert dat er daadwerkelijk bestanden zijn gestolen en stelt vast over welke delen van het systeem het gaat. |
| **14 maart 2026** | **Nieuwsbericht op website en persbericht**<br>Gemeente Epe plaatst een nieuwsbericht over het datalek op de website en verstuurt een persbericht om het bereik verder te vergroten. |
| **16 maart 2026**<br>*Zaterdag* | **Projectpagina website live + bezetting geregeld**<br>Gemeente Epe richt een speciale projectpagina in op de website en regelt de bezetting om vragen van inwoners te beantwoorden. Op de website wordt ook handelingsperspectief geboden. |
| **14 maart - 30 maart 2026** | **Onderzoeksperiode: website bijgewerkt**<br>De gemeente werkt na 14 maart op 23 en op 30 maart de website bij met informatie over de voortgang van het onderzoek naar oorzaak en betrokken data. Het betreft ongestructureerde data, waardoor het complex is uit te zoeken wat er precies van wie in de gestolen data zit. |
| **27 maart 2026**<br>*Vrijdag* | **Eerste dataprofilering gereed**<br>Een eerste analyse van de gestolen data is beschikbaar. Op basis daarvan zijn bestanden zonder persoonsgegevens uitgesloten en is bepaald welke categorieën data nader onderzoek vereisen. |

| Datum | Gebeurtenis |
|---|---|
| **3 april 2026**<br>*Vrijdag* | **Opdracht vervolgonderzoek ID-bewijzen**<br>Gelet op het verhoogde risico op identiteitsfraude bij kopieën van identiteitsbewijzen geeft de gemeente opdracht tot gericht vervolgonderzoek naar de aanwezigheid daarvan in de gestolen bestanden. Gedurende de onderzoeksperiode wordt intensief overleg gevoerd met de IBD over het handelingsperspectief. |
| **20 april 2026**<br>*Maandag* | **Overzicht gevonden kopieën ID-bewijzen ontvangen**<br>De gemeente ontvangt het overzicht van de gevonden kopieën van ID-bewijzen.<br><br>De documenten in deze lijst zijn door de gemeente verder onderzocht en waar mogelijk is het huisadres van de betrokkene gematcht. |
| **22 april 2026**<br>*Woensdag* | **Forensisch onderzoeksrapport definitief**<br>Het forensisch onderzoeksrapport is gefinaliseerd. |
| **23 april 2026**<br>*Donderdag* | **Huis-aan-huis-brief verzonden + publicatie**<br>Inwoners ontvangen een huis-aan-huis-brief met informatie over de hack, de mogelijke gevolgen en het handelingsperspectief. De brief wordt op dezelfde dag gepubliceerd op de website en ter beschikking gesteld aan de media.<br><br>Medewerkers ontvangen een bericht over hun gegevens, de gemeenteraad is geïnformeerd.<br><br>De gemeente heeft de pers uitgenodigd voor een gesprek en een toelichting gegeven. |
| **Vanaf 23 april** | **Samenwerkingspartners geïnformeerd**<br>Contractrelaties en samenwerkingspartners krijgen, wanneer relevant, bericht over de betekenis van het datalek met handelingsperspectief. Partners zijn gevraagd om alert te zijn op signalen van misbruik van de data of zorgen hierover. |
| **Voor 8 mei 2026** | **Persoonlijk bericht aan betrokkenen met kopie-ID**<br>Betrokkenen van wie een kopie van een geldig ID-bewijs is gevonden, ontvangen bericht van de gemeente met instructies om het document op kosten van de gemeente te vervangen. |

## 4. Oorzaken en lessen

Het forensisch onderzoek (zie bijlage) wijst op een combinatie van technische en organisatorische factoren die de impact van het incident hebben vergroot:

- De aanval begon via social engineering, niet via een technisch lek in software. Technische maatregelen alleen zijn dus niet genoeg: medewerkers moeten verdachte situaties ook herkennen en melden.
- Een verhoging van rechten was mogelijk doordat een beheerderswachtwoord kon worden gekraakt.
- Een break-glass account, bedoeld als noodtoegang, had onvoldoende aanvullende beveiligingsmaatregelen, waardoor de aanvaller hiermee vergaande rechten kon verkrijgen.
- Afspraken over incidentrespons met leveranciers en ketenpartners bleken niet eenduidig vastgelegd, dit had kunnen leiden tot vertraging of extra schade. Dat is bij dit incident evenwel niet het geval geweest.

# 5. Genomen en geplande verbetermaatregelen

Op basis van het forensisch onderzoek en de evaluatie zijn concrete verbetermaatregelen vastgesteld. Een deel is al doorgevoerd; een deel wordt opgepakt via het projectplan voor implementatie van de Cyberbeveiligingswet (Cbw/NIS2). De gemeente stelt hiervoor een projectleider aan.

| Belangrijkste maatregelen | Status |
|---|---|
| 24x7 SOC monitoring op servers en endpoints (CrowdStrike) | Uitgevoerd |
| Langetermijn-SOC-monitoring op servers en endpoints (MS Defender); migratie gestart | In uitvoering |
| Isolatie getroffen omgeving en verwijdering persistentiemechanismen (scheduled tasks, DLL-bestanden) | Uitgevoerd |
| Reset van alle accounts, inclusief break-glass account en serviceaccounts | Uitgevoerd |
| Beperking van PowerShell en Run-venster voor standaardgebruikers | Uitgevoerd |
| Uitfasering bestandsserver versneld doorgezet - migratie naar SharePoint/Teams | In uitvoering |
| Netwerksegmentatie aangescherpt: laterale beweging van werkpleknetwerk naar servernetwerk bemoeilijkt | Uitgevoerd |
| Retentiebeleid aanscherpen | Gepland |
| Het bewustwordingsprogramma voor medewerkers vernieuwen | In uitvoering |
| Werkprocessen aanpassen zodat gevoelige gegevens (data-exports, kopieën van identiteitsbewijzen) niet meer worden opgeslagen | Gepland |
| Periodieke incidentresponsoefening (tabletop) | Gepland |

# 6. Juridisch en financieel

## 6.1 Autoriteit Persoonsgegevens

De gemeente heeft het datalek gemeld bij de Autoriteit Persoonsgegevens (AP) conform de AVG, en heeft maximale transparantie betracht over de oorzaak, de omvang en de aanpak. Een formele reactie of aankondiging van verder onderzoek is op dit moment nog niet ontvangen. Indien onderzoek of handhaving volgt, werkt de gemeente volledig mee met de AP.

## 6.2 Aansprakelijkheid

De gemeente heeft een beperkt aantal voorlopige aansprakelijkheidsstellingen van betrokkenen ontvangen. Of een claim wordt gehonoreerd is afhankelijk van de feitelijke schade die als gevolg van dit datalek is of wordt geleden. Op dit moment zijn er geen signalen van daadwerkelijke schade. Betrokkenen van wie een kopie van een geldig identiteitsbewijs is gestolen, kunnen hun document gratis laten vervangen. De gemeente draagt daarvoor de kosten.

### 6.3 Woo-verzoeken

De gemeente heeft twee verzoeken gehad in het kader van de Wet open overheid (Woo). Een verzoek gaat over de eerste periode na de hack en een ander verzoek vraagt ook breder naar de informatiebeveiliging bij de gemeente. Omdat het gaat over zaken die mogelijk niet-openbaar zijn vanwege het belang van intern beraad, de persoonlijke levenssfeer van betrokkenen, het financiële belang van de gemeente, en/of impact op de beveiliging van onze gegevens en systemen wordt per document een afweging gemaakt tussen het belang van openbaarheid en de bescherming van andere belangen.

### 6.4 Financiële impact

De onderstaande tabel geeft een overzicht van de kosten van het incident. Een deel van de kosten is vastgesteld op basis van ontvangen facturen; een deel betreft stelposten voor werkzaamheden die nog lopen of waarvoor nog geen factuur is ontvangen. Het huidige totaal bedraagt € 345.258. De definitieve financiële afronding wordt verwacht in juli 2026; de raad wordt daarover in de voortgangsrapportage nader geïnformeerd.

| **Kosten** | **Bedrag (vastgesteld / stelpost)** | **Toelichting** |
|---|---|---|
| Technisch onderzoek & maatregelen | € 120.896 | *Forensisch en dataonderzoek, technische maatregelen en monitoring; incl. stelpost afronding* |
| Projectleiding & advies incidentrespons | € 79.815 | *Externe projectleiding en advies bij incidentrespons; incl. stelpost afronding* |
| Ondersteuning & communicatie | € 80.000 | *Ondersteuning Woo- en AVG-verzoeken, inhuur communicatie; incl. stelpost vervolg* |
| Post en repro | € 20.440 | *Verzending brieven aan betrokkenen en stelpost porto- en werkzaamheden* |
| Nazorg & vervanging identiteitsbewijzen | € 44.107 | *Vervanging reisdocumenten en rijbewijzen; inhuur KCC-medewerker* |
| **Totaal** | **€ 345.258** | |
| **Geschat eindtotaal (juli 2026)** | **p.m.** | **Definitieve afrekening na afronding resterende werkzaamheden** |

## 7. Tot slot

De gemeente beseft dat dit incident de privacy van inwoners, medewerkers en andere betrokkenen heeft geraakt. De gemeente heeft de verantwoordelijkheid om hier zorgvuldig mee om te gaan. Dit doet de gemeente door openheid over wat er is gebeurd, door betrokkenen adequaat te informeren en ondersteunen, en door te zorgen dat de informatiebeveiliging structureel verbetert. Deze evaluatie moet eraan bijdragen dat ook andere organisaties, zowel publiek als privaat, zich kunnen beschermen tegen vergelijkbare incidenten.