32761	Verwerking en bescherming persoonsgegevens
26643	Informatie- en communicatietechnologie (ICT)
Nr. 341	Brief van de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 16 juni 2026

Met deze kamerbrief bied ik u de reactie aan op het nieuwsbericht van NOS Nieuws op 23 april 2026 inzake ‘Persoonsgegevens van vrijwel alle inwoners Epe gestolen bij cyberaanval.[1]’

De gemeente Epe heeft via haar website aangegeven dat er op 10 maart 2026 via een zogeheten ClickFix-methode een cyberaanval heeft plaatsgevonden bij de gemeente Epe. Een ClickFix-methode is een vorm van een cyberaanval waarbij medewerkers door middel van misleidende berichten of instructies worden aangezet tot het uitvoeren van handelingen die de beveiliging omzeilen. Hierbij hebben hackers toegang verkregen tot een bestandsserver op het gemeentelijk netwerk. De gemeente Epe heeft aangegeven dat de inbraak op 10 maart plaatsvond en op 12 maart is ontdekt, waarna zij de toegang tot systemen heeft geblokkeerd en de beveiliging van de systemen is opgeschaald. Uit het forensisch onderzoek blijkt dat er geen aanwijzingen zijn dat kernsystemen, zoals belasting- en vergunningensystemen en/of landelijke voorzieningen, zijn geraakt.

De gemeente heeft naar aanleiding van dit incident een melding gemaakt bij de Autoriteit Persoonsgegevens, aangifte gedaan bij de politie en aanvullend onderzoek verricht. Vanaf 14 maart heeft zij haar inwoners hierover via de website epe.nl/datalek geïnformeerd. In berichtgeving van 23 april 2026 heeft de gemeente aangegeven dat vrijwel alle inwoners van Epe door dit zogenoemde datalek[2] zijn getroffen. Het betreft onder meer basisgegevens zoals naam, adres, woonplaats, geboortedatum, geboorteplaats en het Burgerservicenummer (BSN)[3]. In een deel van de gevallen zijn ook aanvullende gegevens gelekt, waaronder contactgegevens, bankrekeningnummers en/of kopieën van identiteitsbewijzen. De gemeente Epe houdt via verschillende communicatiewegen, onder meer via haar website, inwoners op de hoogte van ontwikkelingen

[1] https://nos.nl/artikel/2611660-persoonsgegevens-van-vrijwel-alle-inwoners-epe-gestolen-bij-cyberaanval
[2] Zoals bedoeld in art. 33 en art. 34 AVG
[3] “Meer duidelijkheid over gestolen persoonsgegevens bij Gemeente Epe” – 23 april 2026

en geeft hier tips over hoe om te gaan met de risico’s als gevolg van dit datalek.

Ik heb de ontwikkelingen rondom de cyberaanval in Epe nauwlettend gevolgd en betreur de gevolgen van dit datalek. Het is aan een betrokken gemeente om te onderzoeken wat er precies is gebeurd en zich hierover te verantwoorden aan haar gemeenteraad. Decentrale bestuursorganen hebben hierin een eigen bestuurlijke verantwoordelijkheid en verantwoorden zich hierover binnen hun eigen democratische en bestuurlijke verantwoordingsprocessen. Daarom is het ook aan de gemeente om te bepalen welke maatregelen nodig zijn om herhaling in de toekomst te voorkomen. Omdat dergelijke datalekken risico’s als fraude en gerichte phishing met zich mee kunnen brengen, onderschrijf ik van harte de oproep van de gemeente Epe aan haar inwoners om alert te zijn op mogelijk misbruik wanneer gebruikte gegevens zijn buitgemaakt.

Incidenten zoals bij de gemeente Epe zijn helaas niet uniek. Vanuit mijn verantwoordelijkheid voor de digitale weerbaarheid voor de overheid zet ik mij in om dergelijke incidenten zoveel mogelijk te voorkomen. Onder meer via de Cyberbeveiligingswet geef ik invulling aan deze verantwoordelijkheid. De gemeente Epe heeft forensisch onderzoek laten uitvoeren. De uitkomsten van dit onderzoek, en de zogeheten indicators of compromise, zijn gedeeld met de Informatiebeveiligingsdienst voor gemeenten (IBD) en via hen met het Nationaal Cyber Security Centrum (NCSC).

De gemeente Epe heeft daarnaast recent haar evaluatierapport over het datalek openbaar gemaakt[4]. Daarin geeft zij een weergave van de gebeurtenissen, deelt zij de oorzaken van het incident en geeft aan welke lessen hieruit zijn getrokken. De onderzoeken naar het incident in Epe laten zien dat de impact van een cyberaanval vaak wordt bepaald door een combinatie van technische, organisatorische en menselijke factoren. Dit onderstreept het belang van een integrale aanpak van digitale weerbaarheid, waarbij niet alleen wordt geïnvesteerd in technische beveiligingsmaatregelen maar ook in bewustwording, opleiding, monitoring en het regelmatig oefenen van incidentrespons.

Het is positief dat de gemeente Epe gekozen heeft om het evaluatierapport openbaar te maken. Zo kunnen overheidsorganisaties van elkaar leren en versterken we

[4] Het evaluatierapport is te raadplegen op https://www.epe.nl/datalek-gemeente-epe

gezamenlijk onze digitale weerbaarheid. Digitale weerbaarheid vraagt namelijk voortdurende inzet vanuit ons allemaal. Hiervoor is het noodzakelijk om onderling gebruik te maken van elkaars kennis, expertise en ervaring, onder andere door aansluiting te zoeken bij het Centrum voor Informatiebeveiliging en Privacybescherming (CIP).

Ons doel is en blijft om gezamenlijk te werken aan een veilige en betrouwbare omgang van digitale systemen met daarin persoonsgegevens. Zodat de overheid op een veilige manier met de gegevens van haar inwoners omgaat.

De staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,
E. van der Burg