Fractie POV

UW BRIEF VAN	UW KENMERK	ONS KENMERK	DATUM
24 april 2026		**2875784** / 2883032	12 mei 2026

BEHANDELD DOOR	BEZOEKADRES	TELEFOON	BIJLAGEN
	Paul Krugerstraat 1		

ONDERWERP
Beantwoording art 34 RvO vragen fractie Perspectief op Vlissingen - Cyberveiligheid gemeente Vlissingen naar aanleiding van de hack bij gemeente Epe

Geachte fractie.

Naar aanleiding van de door uw fractie ingediende vragen ex artikel 34 RvO informeren wij u als volgt.

Uw inleiding
De fractie van Perspectief op Vlissingen, POV maakt zich grote zorgen over de recente hack bij gemeente Epe, waarbij volgens berichtgeving circa 800 gigabyte aan data en ongeveer 600.000 bestanden zijn buitgemaakt, waaronder persoonsgegevens en ID-bewijzen van inwoners. De aanval werd uitgevoerd via een phishingmethode, bekend als ClickFix.

De gemeente Vlissingen noemt in haar begroting zelf al het risico op een hack of cryptolocker als reëel, met mogelijke gevolgen voor dienstverlening, herstelkosten en dataverlies.

Naar aanleiding hiervan stellen wij het college de volgende vragen:

<u>Vraag 1</u>
Bent u bekend met de hack bij de gemeente Epe en heeft u naar aanleiding daarvan de eigen cyberweerbaarheid opnieuw beoordeeld?

<u>Ons antwoord</u>
Ja, de hack is bekend. Deze heeft niet geleid tot een separate herbeoordeling, omdat onze cyberweerbaarheid al structureel en continu wordt geëvalueerd binnen de PDCA-cyclus (conform informatiebeveiligingsnormen Baseline Informatiebeveiliging Overheid (BIO) en de internationale norm ISO27001). Dreigingsontwikkelingen, zoals het incident in Epe, worden hierin doorlopend meegenomen.

Op basis van deze werkwijze hebben wij geen signalen dat onze huidige maatregelen tekortschieten. Tegelijk blijven wij alert en worden relevante ontwikkelingen direct vertaald naar aanscherpingen waar nodig.

<u>Vraag 2</u>

Wat is op dit moment de stand van zaken rondom de cyberveiligheid van uw gemeente, met name op het gebied van phishingaanvallen?

Ons antwoord
De cyberveiligheid is ingericht conform BIO, ISO27001 en de Europese Network and Information Security richtlijn (NIS2) welke zijn vertaling zal vinden in de aanstaande Cyberbeveiligingswet. Maatregelen zoals Multi-Factor-Authenticatie, e-mailbeveiliging, monitoring en awareness zijn geïmplementeerd. Phishing blijft een actueel risico, waarin we met bewustwordingscampagnes de medewerkers op blijven attenderen.

Vraag 3
Zijn er in 2025 en/of 2026 cyberincidenten of verdachte signalen geweest binnen uw organisatie?

Ons antwoord
Er hebben zich geen grootschalige incidenten voorgedaan. Wel zijn er phishingpogingen en verdachte inlogactiviteiten waargenomen. In enkele gevallen hadden accounts tijdelijk te maken met ongeautoriseerde toegang; deze accounts zijn direct geblokkeerd en volgens de geldende procedure weer veilig gemaakt, zonder datalekken of gevolgen voor gegevens.

Vraag 4
Welke technische en organisatorische maatregelen zijn momenteel genomen om cyberaanvallen te voorkomen en de impact ervan te beperken?

Ons antwoord
Technisch: Multi-Factor-Authenticatie, End-Point Detectie en Respons, back-ups, patchmanagement en monitoring.
Organisatorisch: Incident Reponse Plan, risicoanalyses, leveranciersafspraken en awarenessprogramma's.

Vraag 5
Is uw gemeente voorbereid op het melden van datalekken conform de AVG (artikel 33 en 34)?

Ons antwoord
Ja. Er is een datalekprocedure ingericht conform AVG, inclusief meldproces en rolverdeling.

Vraag 6
Zijn medewerkers in de afgelopen 12 maanden getraind op het herkennen van phishing en andere cyberdreigingen?

Ons antwoord
Ja. Medewerkers worden structureel en doorlopend bewust gemaakt via wekelijkse awarenessvragen, waarmee kennis actief wordt getoetst. Daarnaast worden zij via het intranet regelmatig voorzien van aanvullende informatie en actuele dreigingsbeelden. In het jaarlijkse awarenessprogramma heeft phishing een prominente en terugkerende rol.

Vraag 7
Zijn er afspraken gemaakt met externe leveranciers over cyberveiligheid en de bescherming van gegevens?

Ons antwoord
Ja. Met kritieke leveranciers zijn afspraken gemaakt over beveiliging en het melden van incidenten. Daarnaast houdt een externe partij onze omgeving continu in de gaten, zodat verdachte activiteiten snel worden opgemerkt en afgehandeld.

Vraag 8
Heeft uw gemeente afspraken over detectie, logging en respons bij cyberincidenten?

Ons antwoord
Ja. Deze zijn vastgelegd in het Incident Respons Plan, procedures en leveranciersafspraken.

Vraag 9
Bent u bereid het college op korte termijn te informeren over de cyberweerbaarheid van uw gemeente?

Ons antwoord
Ja, wij nemen dit mee in het introductieprogramma voor een nieuw college.

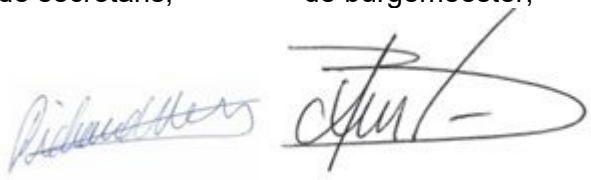
Vraag 10
Zijn er aanvullende maatregelen nodig om de continuïteit van de dienstverlening te waarborgen bij een cyberincident?

Ons antwoord
Ja. Focus ligt op versterking van phishingweerbaarheid, monitoring, back-up/restore en het oefenen van crisisscenario's.

Wij gaan ervan uit u hiermee in voldoende mate te hebben ingelicht.

Hoogachtend,

burgemeester en wethouders van Vlissingen,
de secretaris, de burgemeester,



drs. R.D.A. Wiskerke drs. A.R.B. van den Tillaar