Onderwerp: Cyberveiligheid gemeente Vlissingen naar aanleiding van de hack bij gemeente Epe

Geacht college,

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:

1. Is het college bekend met de hack bij gemeente Epe van vandaag, en heeft deze gebeurtenis aanleiding gegeven om de eigen digitale weerbaarheid van gemeente Vlissingen opnieuw te toetsen?
2. Kan het college aangeven hoe het staat met de cyberveiligheid van de gemeente Vlissingen, in het bijzonder tegen phishing-aanvallen zoals ClickFix of vergelijkbare aanvalsvormen?
3. Zijn er op dit moment binnen de gemeente Vlissingen signalen van verdachte inlogpogingen, ongeautoriseerde toegang, datadiefstal of andere cyberincidenten geweest in 2025 en 2026?
4. Welke technische en organisatorische maatregelen zijn op dit moment getroffen om te voorkomen dat gevoelige gemeentelijke gegevens worden buitgemaakt of versleuteld, zoals ook bij gemeenten elders is gebeurd?
5. Is de gemeente Vlissingen voorbereid op een scenario waarin persoonsgegevens betrokken zijn bij een inbreuk in de zin van artikel 33 en 34 van de AVG, waaronder de verplichting tot melding aan betrokkenen bij een hoog risico?
6. Hoe vaak zijn medewerkers in de afgelopen 12 maanden getraind of getest op phishing, social engineering en veilig digitaal werken?
7. Zijn de belangrijkste systemen, back-ups en kritieke leveranciers van de gemeente Vlissingen op voldoende wijze gesegmenteerd en beschermd tegen ransomware en datadiefstal?
8. Welke afspraken zijn er met ICT-leveranciers over detectie, logging, incidentrespons en directe opschaling bij een beveiligingsincident?
9. Is het college bereid om de raad op korte termijn te informeren over de actuele stand van zaken rond cyberweerbaarheid, inclusief verbeterpunten en eventuele resterende risico's?
10. Welke aanvullende maatregelen acht het college nodig om de continuïteit van de gemeentelijke dienstverlening bij een cyberaanval te borgen?

In afwachting van uw schriftelijke beantwoording en met vriendelijke groet,

POV Fractie