College van burgemeester en wethouders

Postbus 149

3840 AC Harderwijk

Betreft: Schriftelijke vragen ex artikel 32 Organisatieverordening van de gemeenteraad
Datum: 23 april 2026

Onderwerp: Informatieveiligheid, preventie van datalekken en ClickFix-risico's

Geacht college,

Er heerst grote maatschappelijke bezorgdheid omtrent dataveiligheid. Het voorkomen van datalekken is cruciaal om het enorme afbreukrisico voor de gemeente te beperken. Recente incidenten bij organisaties zoals Odido,Basic-Fit, maar in het bijzonder het ernstige datalek bij de gemeente Epe, onderstrepen de kwetsbaarheid van overheidsinstanties. De VVD heeft veiligheid in de breedste zin van het woord — en dus ook digitale veiligheid — altijd hoog op de agenda staan.

De gevolgen van dergelijke lekken zijn groot: van identiteitsfraude bij achteraf betaalmethoden tot misbruik bij het huren van voertuigen. Door dataverrijking op het *dark web* worden gegevens uit verschillende lekken gecombineerd, waarbij kwetsbare groepen doorgaans het hardst worden geraakt. Nu de Autoriteit Persoonsgegevens (AP) aangeeft onvoldoende middelen te hebben voor een sterke preventieve rol, is het credo "voorkomen is beter dan genezen" urgenter dan ooit.

Naar aanleiding hiervan stelt de fractie van de VVD Harderwijk-Hierden de volgende vragen:

Vraag 1: Heeft het college kennisgenomen van het grootschalige datalek bij de gemeente Epe, waarbij persoonsgegevens van nagenoeg alle inwoners zijn buitgemaakt?

Vraag 2: De gegevens in Epe zijn naar verluidt buitgemaakt via de zogenaamde ClickFix-methode (waarbij gebruikers worden verleid op kwaadaardige links te klikken onder het mom van browser-updates). Is de gemeente Harderwijk ook kwetsbaar voor een dergelijke methode? Zo ja, welke technische en procedurele maatregelen zijn er getroffen om dit specifiek te voorkomen?

Vraag 3: Wordt er binnen de ambtelijke organisatie gewerkt met 'lijstwerk' (zoals Excel-bestanden of exports) waarin kritieke persoonsgegevens zoals BSN, geboortedatum en naam gelijktijdig buiten de beveiligde kernsystemen worden opgeslagen?

Vraag 4: Middels workspace-accounts is het mogelijk om eigen hardware te gebruiken (Bring Your Own Device - BYOD). Hoewel dit voordelig is voor de hardwarekosten en prettig voor de eindgebruiker, brengt dit extra veiligheidsrisico's met zich mee. Wat is de visie van het college op het gebruik van eigen hardware in relatie tot de informatiebeveiliging?

Vraag 5: Wordt er conform de AVG met regelmaat een Data Protection Impact Assessment (DPIA) uitgevoerd op de meest kritieke processen? Zo ja, wat is de datum van de meest recent uitgevoerde DPIA en op welke processen had deze betrekking?

Vraag 6: Zijn er uit recente DPIA's of audits (zoals de ENSIA-audit) aanbevelingen voortgekomen die nog opvolging behoeven? Zo ja, om welke verbeterpunten gaat dit en op welke wijze wordt de raad over de voortgang hiervan geïnformeerd? (Vertrouwelijkheid ten aanzien van dit punt in acht genomen)

Vraag 7: Is het college van mening dat er momenteel voldoende financiële middelen en expertise beschikbaar zijn om de data van onze inwoners veilig te houden? Zo nee, welke aanvullende middelen of maatregelen zijn volgens het college noodzakelijk?

Met vriendelijke groet,

Namens de VVD Harderwijk-Hierden,

Jelle van Nieuwenhuizen

Aanvullende bronnen :

https://www.nu.nl/economie/6393546/hackers-stelen-data-van-bijna-alle-inwoners-epe-en-ook-zon-duizend-id-bewijzen.html?referrer=https%3A%2F%2Fwww.google.com%2F

https://eenvandaag.avrotros.nl/artikelen/ap-wil-strenger-optreden-bij-datalek-maar-kan-het-aantal-meldingen-niet-aan-door-te-weinig-capaciteit-163428