Schriftelijke vragen.

Aandacht-LV

Schriftelijke politieke vragen ex artikel 32 van het Reglement van orde voor vergaderingen en andere werkzaamheden van de raad Leidschendam-Voorburg 2024.

Datum: **28-4-2026**
Steller: **Lieke Muller (Aandacht-LV), Chantal Brakus (PRO)**
Onderwerp: **Toezicht digitale veiligheid gemeentelijke domeinen/websites**

In maart 2024 heeft Lieke Muller (Aandacht-LV, destijds CDA) vragen gesteld[1] over "Digitale zaken op orde: verouderde websites" (ID 1843). In de beantwoording gaf het college aan:

> "We hebben 21 websites actueel en in gebruik. Daarvan voldoen 16 websites volledig, 2 websites voldoen voor 80% en 3 websites voldoen niet. De websites die niet voldoen worden actief opgepakt."

Recent verscheen op Vlietnieuws het artikel "Domeinen gemeente vormen risico"[2], waarin wordt verwezen naar data van Basisbeveiliging.nl. Daaruit blijkt dat de gemeente circa 110 domeinen heeft, waarvan 34 hoofddomeinen. Daarvan worden 10 domeinen aangemerkt als hoog risico, 36 als middenrisico, 30 als laag risico en 44 zonder vastgesteld risico.

In een tijd waarin digitale en geopolitieke dreigingen zich steeds vaker ook op gemeenten richten, zoals recent zichtbaar werd bij de cyberincidenten in Epe, vraagt digitale veiligheid om extra aandacht. Daarbij komt dat op Europees niveau, onder meer via analyses en richtlijnen van ENISA, al langer wordt gewezen op de risico's van versnipperd domeinbeheer en verouderde webomgevingen.

De recente beantwoording van vragen van Aandacht-LV over het gebruik van Google Forms door een extern bureau laat zien dat extra alertheid op digitale/dataveiligheid geen overbodige luxe is. In het huidige landschap van digitale middelen, publieke data, externe leveranciers, en geopolitieke spanningen ligt een verhoogd risico.

Tegen deze achtergrond zien Aandacht-LV en PRO aanleiding tot de volgende vragen:

1. Welke directe maatregelen zijn/worden genomen naar aanleiding van de berichtgeving over de risico's rond deze (sub)domeinen?

2. Is er binnen de organisatie één centraal register voor (aan de gemeente gelieerde) domeinen?

---

[1] https://lv.bestuurlijkeinformatie.nl/Reports/Document/6d5f847d-4ba4-4492-87a7-004fa821e657?documentId=a0f39de5-e816-4832-b095-826cb75ebe07

[2] https://vlietnieuws.nl/2026/04/27/domeinen-gemeente-vormen-risico/

a. Wordt dit periodiek extern gevalideerd?
b. Wie (functietitel) is/zijn eindverantwoordelijk voor domeinbeheer en cybersecurity binnen de organisatie?
c. Hoe is in de organisatie geborgd dat de aanschaf en het beheer van nieuwe (sub)domeinen via de juiste afdeling/persoon loopt?

3. Is het college bekend met het CIO-stelsel van het Rijk (incl. CIO-rol, CIO-beraad en stelselverantwoordelijkheid)?
    a. In hoeverre acht het college dit stelsel of onderdelen daarvan (zoals centrale regie, verplichte kaders en onafhankelijke toetsing) toepasbaar op gemeentelijk niveau?
    b. Welke ambitie heeft het college om de regie op digitale veiligheid, domeinbeheer en (web)kanalen te versterken, en hoe vertaalt zich dat in rollen, mandaat en governance (bijv. positie van CIO/CDO/CISO)?
    c. Indien deze ambitie er (nog) niet is: welke overwegingen liggen daaraan ten grondslag?

4. Hoe wordt voorkomen dat er “shadow IT” ontstaat, waarbij afdelingen of leveranciers zelfstandig domeinen registreren?

5. Worden medewerkers en leveranciers actief getraind op veilig domeingebruik en risico’s van shadow IT?

6. Hoe vaak wordt actief gecontroleerd op ongebruikte domeinen, verlopen certificaten en versleuteling, en verouderde (CMS-)systemen?

7. Kan het college bevestigen hoeveel (sub)domeinen:
    a. verouderde software draaien
    b. geen HTTPS of zwakke TLS-configuraties gebruiken
    c. kwetsbaar zijn voor bekende exploits (zoals gemeld door Basisbeveiliging.nl)

    En wanneer bovenstaande wordt opgelost?

8. Welke concrete risico’s lopen inwoners als zij gebruikmaken van kwetsbare of verouderde gemeentelijke websites?

9. Zijn deze risico’s formeel vastgelegd in een risicoanalyse (bijv. binnen BIO- of ISO27001-kaders)?

10. In hoeverre ligt het beheer van websites en domeinen bij externe leveranciers, welke beveiligingseisen gelden daarbij, en welke (schriftelijke én mondelinge) afspraken zijn hierover gemaakt?

11. Acht het college de huidige situatie NIS2-proof? Zo ja, waarop is dat gebaseerd?