Gemeenteraad

Zaaknummer	Z/26/514110-ADV/26/1298477
Portefeuillehouder	A. Boone
Onderwerp	Schriftelijke vragen CDA over Cyberveiligheid

Beste raadsleden,

Op 06 mei 2026 zijn de volgende schriftelijke vragen gesteld, met kenmerk Z/26/514110. Ter beantwoording van deze schriftelijke vragen informeert het college u als volgt.

Vraag 1
Is het College bekend met de recente NCSC-waarschuwing (15 april 2026) over AI-gestuurde kwetsbaarheidsopsporing (Mythos van Antrophic), de verschillende ransomware-aanval zoals op Chipsoft en Odido en de cyberaanval op gemeente Epe?

a. *Zo ja: heeft het College naar aanleiding van deze incidenten al actie ondernomen of overwogen?*
b. *Zo nee: is het College bereid dit alsnog te doen?*

Antwoord vraag 1
Het college is bekend met de verschillende incidenten die de afgelopen tijd hebben plaatsgevonden en heeft naar aanleiding van deze gebeurtenissen diverse acties ondernomen.

Vraag 2

Heeft de gemeente een actueel en geoefend incidentresponsplan voor een cyberaanval of datalek, en wanneer is dit voor het laatst getest en eventueel bijgewerkt?

Antwoord vraag 2

Binnen de gemeente Zevenaar is geconstateerd dat het incident responsplan niet actueel is, momenteel wordt deze geactualiseerd voor verschillende scenario's. Een cyberaanval is één van deze scenario's.

Vraag 3

Zijn er naar aanleiding van de hack op gemeente Epe en andere organisaties of de NCSC-waarschuwing, intern controlestappen gezet om na te gaan of vergelijkbare kwetsbaarheden bij onze gemeente bestaan? Anders gesteld; is de dijkbewaking recent getoetst naar aanleiding van de publiek bekendgemaakte incidenten om te zien dat de gemeente geen vergelijkbaar risico loopt?

Antwoordt vraag 3

Er is gekeken of en welke maatregelen de gemeente heeft geïmplementeerd om weerbaar te zijn tegen de methodieken die gebruikt zijn bij de betreffende aanvallen. Hierbij is gekeken naar zowel technische als organisatorische maatregelen.
Analyse van de clickfix-aanval door het informatiebeveiligingspersoneel toont aan dat de bij de hack van Epe gebruikte aanvalspaden binnen onze omgeving niet direct toegankelijk zijn voor standaardgebruikers en aanvullende rechten of stappen vereisen.

Vraag 4

Op welke servers of systemen worden kopieën van identiteitsbewijzen en BSN-nummers van inwoners opgeslagen, en wie heeft hier toegang toe? (*Dit in het licht van de situatie in Epe, waar een server met bestanden van vóór 2022 de kwetsbaarheid bleek.)*

Antwoord vraag 4

Gegevens zoals BSN-nummers en kopieën van legitimatiebewijzen worden, indien hiervoor een wettelijke grondslag is om deze te bewaren of verwerken, opgeslagen in systemen en vak-applicaties. Zevenaar gebruikt, in het licht van de situatie in Epe, geen server van waaruit bestanden moeten worden opgeladen naar de vak-applicatie. Op systemen en applicaties wordt toegang- en autorisatiebeheer toegepast.

Vraag 5

Hanteert de gemeente een actief beleid van dataminimalisatie? Worden persoonsgegevens actief verwijderd zodra de bewaartermijn is verstreken en hoe wordt hierop gecontroleerd?

Antwoord vraag 5

We voeren dataminimalisatie niet als losstaand proces uit, maar borgen dit integraal via de volgende instrumenten:

- Informatiebeheerplannen: de informatiebeheerplannen geven inzicht in de omvang en het gebruik van data binnen de verschillende teams. Hierdoor hebben we inzicht in welke data aanwezig is en kunnen we waar nodig gerichte verbetermaatregelen opstellen.
- Documentair structuurplan (DSP): met behulp van het DSP worden de archiefbeherende informatiesystemen ingericht conform wet- en regelgeving (Archiefwet, AVG). Hiermee worden bewaartermijnen vastgesteld en ingericht waardoor we data niet langer bewaren dan noodzakelijk en voldoen we aan onze vernietigingsplicht door tijdige vernietiging, maar zijn we ook bewust van welke persoonsgegevens worden uitgevraagd en welke ook volgens wet- en regelgeving mogen worden uitgevraagd.
- Kwaliteitssysteem: met het kwaliteitssysteem meten we met de periodieke controles door de pdca-cyclus of we nog voldoen aan gestelde normen en regels. Zo borgen we dus ook dat tijdige vernietiging van de data wordt bewaakt en voorkomen we dat meer data beschikbaar blijft dan noodzakelijk.

Vraag 6

Zijn er externe leveranciers of softwarebedrijven die namens de gemeente persoonsgegevens van inwoners verwerken of opslaan (vergelijkbaar met de rol van Chipsoft voor zorginstellingen), en hoe is de beveiliging en aansprakelijkheid in die contracten geregeld?

Antwoord vraag 6

Gemeente Zevenaar maakt gebruik van externe leveranciers en softwarebedrijven voor de verwerking en opslag van gegevens van haar inwoners. Hierbij wordt gewerkt met een uniforme set van inkoopvoorwaarden, kwaliteitsnormen en instrumenten die specifiek is ontwikkeld door de Vereniging van Nederlandse Gemeenten (VNG) voor de inkoop van IT-producten en -diensten (GIBIT) en de standaard verwerkersovereenkomst van de VNG om afspraken rondom beveiliging en aansprakelijkheid goed contractueel vast te leggen.

Vraag 7

Wat is de huidige gemiddelde doorlooptijd tussen het beschikbaar komen van een kritieke beveiligingsupdate (patch) en de daadwerkelijke implementatie daarvan in gemeentelijke systemen? (Het NCSC stelt dat reactietijden van weken niet meer passen bij het huidige dreigingslandschap.)

Antwoord vraag 7

Voor installeren van kritische beveiligingsupdates zijn binnen het daarvoor geldende vulnerability managementproces oplostijden vastgesteld die aansluiten bij de richtlijnen van het NCSC. In de praktijk worden deze doelstellingen momenteel niet structureel gehaald. De norm voor het implementeren van kritieke patches binnen 24 uur wordt niet gehaald; de daadwerkelijke doorlooptijd varieert sterk per systeem, afhankelijk van de complexiteit van de wijziging en de doorlooptijden bij interne en externe beheerpartijen.

Beperkingen in de huidige capaciteit binnen de IT-uitvoeringsorganisatie en de complexiteit van de huidige infrastructuur maken dat een volledig tijdige implementatie niet altijd haalbaar is. Om die reden wordt een risico gestuurde aanpak gehanteerd, waarbij prioriteit wordt gegeven aan kwetsbaarheden die actief worden misbruikt en systemen die direct zijn verbonden met het internet (internet-facing).

Vraag 8

Wanneer heeft de gemeente voor het laatst een externe pentest of security-audit laten uitvoeren op haar IT-infrastructuur, en wat waren de belangrijkste bevindingen?

Antwoord vraag 8

In de recente jaren zijn drie separate security-tests uitgevoerd op de IT-infrastructuur van de gemeente:

• Q2 2026: een geautomatiseerde vulnerability scan / security assessment
• Q3 2023: een externe black-box pentest
• Q2 2026: een interne/externe white-box pentest

Daarnaast vindt er 24/7/365 geautomatiseerde vulnerability scanning en external attack surface management[1] plaats als onderdeel van de continue beveiligingsmonitoring.

De belangrijkste bevindingen uit deze onderzoeken zijn:

• Verdere hardening [2]van systemen is noodzakelijk om het risico op misbruik te reduceren;
• Verbetering van interne netwerksegmentatie verdient prioriteit;
• Structurele en frequente controle van verouderde configuraties en systemen op kwetsbaarheden is noodzakelijk, met nadruk op continue en geautomatiseerde monitoring waar mogelijk.

Vraag 9

Is de gemeente aangesloten op de dreigingsanalyse van het NCSC en/of de Informatiebeveiligingsdienst (IBD) van de VNG, en wordt deze informatie actief benut?

Antwoord vraag 9

---

[1] External Attack Surface Management (EASM) is een continu cybersecurity-proces dat alle internetgerichte digitale bedrijfsmiddelen ontdekt, analyseert en beveiligt die een aanvaller vanaf de buitenkant kan misbruiken

[2] Hardening van systemen is het proces waarbij de beveiliging van IT-systemen wordt gemaximaliseerd door het aanvalsoppervlak te verkleinen. Dit wordt bereikt door onnodige functies, services, poorten en applicaties uit te schakelen of te verwijderen, waardoor kwetsbaarheden worden geëlimineerd.

De gemeente is aangesloten op de dreigingsanalyse via de IBD en ontvang dan ook de analyses en kwetsbaarheidswaarschuwingen van de NCSC. De analyses en waarschuwingen worden actief benut en beoordeeld maken onderdeel uit van het bij vraag 7 genoemde vulnerability managementproces.

Vraag 10

Hoeveel fte is er binnen de gemeente specifiek belast met informatiebeveiliging, en acht het College dit voldoende gezien de toenemende dreiging?

Antwoord vraag 10

Binnen de gemeente Zevenaar is 0,5 fte specifiek belast met informatiebeveiliging in de rol van Chief Information Security Officer (CISO). Overige specifieke rollen voor informatiebeveiliging zijn ondergebracht bij het Regionaal ICT en Inkoop de Liemers (RID).

Binnen de RID is informatiebeveiliging belegd bij een team met een omvang van 3 FTE. Deze capaciteit is primair gericht op het identificeren, analyseren en rapporteren van risico's en kwetsbaarheden, evenals het adviseren van de directie op het gebied van informatiebeveiliging, compliance en organisatorische beheersing.

De RID acht deze capaciteit toereikend voor de genoemde taken binnen de informatiebeveiligingsfunctie. Tegelijkertijd wordt onderkend dat de huidige inrichting kwetsbaarheden kent in de vorm van een beperkte bezetting van kritieke functies, te weten één security analist, één TISO en één CISO. Deze beperkte bezetting leidt tot een verhoogd continuïteitsrisico bij (tijdelijke) uitval, aangezien er sprake is van een beperkte mate van vervangbaarheid en kennisredundantie binnen deze rollen.

Het belangrijkste risico ligt niet zozeer binnen de informatiebeveiligingsfunctie zelf, maar in de beschikbare capaciteit binnen de IT-uitvoeringsorganisatie voor de opvolging van geïdentificeerde risico's. Dit betreft met name de capaciteit om tijdig en proactief patchmanagement uit te voeren in lijn met de releasecycli van belangrijke softwareleveranciers en platformen.

Hierdoor ontstaat een afhankelijkheid in de doorvertaling van geconstateerde risico's naar tijdige technische maatregelen binnen de beheerorganisatie.

Vraag 11

Worden medewerkers structureel getraind op cyberbewustzijn (zoals phishing-herkenning), en hoe frequent?

Antwoord vraag 11

Cyberbewustzijn is onderdeel van de onboarding van nieuwe medewerkers, daarnaast worden er op ad-hoc basis andere bewustwordingscampagnes uitgevoerd. De gemeente heeft in april 2026 meegedaan aan een Phishathon om de weerbaarheid van medewerkers voor phishing te testen. In de maand mei heeft er een mystery guest onderzoek plaatsgevonden binnen het gemeentehuis om medewerkers bewust te maken op de risico's van meelopers (tailgaiting).

Vraag 12

Heeft de gemeente een communicatieplan klaarliggen voor het geval er een datalek of cyberaanval plaatsvindt die inwoners raakt, en voldoet dit aan de wettelijke meldplicht van de AVG (melding binnen 72 uur bij de Autoriteit Persoonsgegevens)?

Antwoord vraag 12

De gemeente heeft een standaard proces voor het afwikkelen van datalekken, dit voldoet aan de wettelijke verplichtingen zoals beschreven in de AVG. Onderdeel van de proces is onder ander het bepalen van de impact voor- en de communicatie richting betrokkenen.

Met vriendelijke groet,
burgemeester en wethouders van Zevenaar,

Danielle Jansen
Secretaris

Digitaal ondertekend door:
Daniëlle Jansen
Datum: 02-06-2026

Lucien van Riswijk
Burgemeester

Digitaal ondertekend door:
Lucien van Riswijk
Datum: 02-06-2026