gemeente NOORDOOSTPOLDER RAAD

Fractie:	ChristenUnie-SGP
Naam:	Sjoerd de Boer
Onderwerp:	Informatiebeveiliging en digitale veiligheid
Datum indiening vragen:	3 april 2025

De ChristenUnie-SGP-fractie hecht groot belang aan digitale veiligheid. Hackaanvallen en datalekken kunnen grote gevolgen hebben, en onze gemeente moet hierop voorbereid zijn. Hoewel de gemeente Noordoostpolder geen grote incidenten heeft gekend en wij de indruk hebben dat informatiebeveiliging serieus wordt genomen, roept de recente beoordeling op basisbeveiliging.nl bij ons zorgen op.

Uit deze beoordeling blijkt dat Noordoostpolder binnen Flevoland de meeste highrisk-beveiligingsproblemen heeft. Dit is zorgwekkend, zeker nu deze informatie openbaar is. De website toetst weliswaar niet het volledige informatiebeveiligingsbeleid, maar geeft wel een indicatie van verbeterpunten. Dit brengt ons tot de volgende vragen:

Vragen:

1. Hoe duidt het college de uitkomst van de beoordeling op **basisbeveiliging.nl** en welke concrete maatregelen worden genomen om de geconstateerde risico's te verminderen?
   Antwoord:
   De website basisbeveiliging toetst niet op ons informatiebeveiligingsbeleid. Ze voeren een check uit op beveiligingsstandaarden die voor websites zijn afgesproken. Ze controleren op basis van domeinnamen die namens de gemeente Noordoostpolder geregistreerd zijn. Vanwege strategische redenen hebben we soms wel de domeinnamen in eigendom, maar is de website niet in ons eigendom. Denk bijvoorbeeld aan de websites van de verschillende dorpen.

   De websites die door ons worden beheerd en een belangrijke rol spelen in onze digitale dienstverlening naar onze inwoners en ondernemers bevatten geen high risk beveiligingsproblemen. Hierop wordt continue door onze functioneel beheerders in samenspraak met de leverancier op gemonitord. Jaarlijks wordt door onze onafhankelijke auditpartij een verklaring opgesteld die informatie bevat over de beveiligingsrisico's en de privacyrisico's die verbonden zijn aan onze interne ICT Systemen. Wij sturen de gemeenteraad hiervan altijd een collegeverklaring als onderdeel van de ENSIA-audits. U kunt in mei deze verklaring wederom tegemoet zien.

   Redirects zijn een belangrijk onderdeel van ons websitebeheer. Op deze wijze zorgen we er voor dat bezoekers en zoekmachines altijd bij de juiste en veilige pagina uitkomen. Dat is voor de genoemde domeinnamen op basisbeveiliging ook het geval. Websites die niet actief gebruikt worden of waarbij sprake is van een verouderde URL zijn geredirect naar een website die in (mede)beheer is van de gemeente Noordoostpolder en die wel voldoet aan de beveiligingsnormen.

2. Is het college bereid om, waar mogelijk, eenvoudig op te lossen **highrisk-problemen** (zoals verkeerde DNS-instellingen) binnen één maand op te lossen en de risico's tot nul terug te brengen?
   Zoals al aangegeven als antwoord op vraag 1: de websites die bij ons in beheer staan hebben geen highrisks. Naar aanleiding van uw vragen zullen we de lijst met domeinnamen nog eens kritisch doorlopen en beoordelen of deze moeten blijven bestaan. Er zijn diverse websites voor specifieke doeleinden die door externen beheerd worden. We zullen hen (of de interne opdrachtgevers) attenderen op het blijvend voldoen aan de beveiligingsstandaarden. We onderzoeken of en op welke wijze we hier in de toekomst meer regie op kunnen voeren.

3. In hoeverre voldoet de gemeente op dit moment volledig aan de **Baseline Informatiebeveiliging Overheid (BIO)**? Zo nee, welke stappen worden gezet om hieraan te voldoen?
   Antwoord:
   De vigerende versie van de BIO is al vele jaren de maatstaf voor onze informatieveiligheid. Dat is ook zo opgenomen in het strategisch beleid. We hebben een Information Security Systeem waarin we de normen hebben opgenomen. Jaarlijks wordt een zelfaudit uitgevoerd. We zijn in die zin in control. Niets geeft immers 100% zekerheid, maar er is veel aandacht voor het behouden van onze informatieveiligheid.

   De raad heeft vorig jaar geld beschikbaar gesteld voor de verbetering van onze cyberweerbaarheid. Er is nu sprake van 24/7 monitoring en response op mogelijke informatiebeveiligingsincidenten. Voor de invoering hiervan is een nulmeting gedaan om eventuele bestaande informatieveiligheidsrisico's op te lossen. Er is daarnaast zeer recent nog een penetratietest uitgevoerd, waarbij een ethische hacker op diverse manieren heeft getracht 'in te breken". Hoewel het rapport nog niet is opgeleverd, is kunnen we wel melden dat het niet gelukt is.

4. Is de gemeente Noordoostpolder volledig voorbereid op de invoering van de **Cyberbeveiligingswet** later dit jaar? Welke acties worden ondernomen om te voldoen aan de wettelijke verplichtingen?
   Antwoord:
   De raad heeft in september 2024 een memo ontvangen over de nieuwe wetgeving en hoe we ons hier op voorbereiden. We hebben ons al aangemeld als essentiële entiteit conform verplichting. De BIO 2.0 dient als normenkader voor de zorgplicht die de overheid heeft op het gebied van informatiebeveiliging. Het eerder genoemde monitoring en response past bij de eisen van de Cyberbeveiligingswet en BIO 2.0. We willen enerzijds zeer snel kunnen reageren op incidenten om grote(re) schade te voorkomen en moeten dit ook binnen 24 uur melden wanneer het significante incidenten betreft. We sluiten aan bij al bestaande interne procedures voor het melden van beveiligingsincidenten en datalekken.

Datum beantwoording vragen:	
Contactpersoon:	
E-mail adres:	
Tel:	