

GBO (Gemeentebelangen Overbetuwe)
Chanessa Wartes - de Boef

Uw brief van	Uw kenmerk	Ons kenmerk	Datum	Verzonden d.d.
		2022-021694	5 juli 2022	
Onderwerp:		Behandeld door	Telefoonnummer	Bijlage(n)
S-607 Schriftelijke vragen GBO over Datalek gemeente Buren		S. van Eldik-Giesbers	14 0481	

Geachte mevrouw Wartes – de Boef en overige leden van de gemeenteraad,

U heeft op 1 juni jongstleden schriftelijke vragen gesteld aan het college over het datalek bij de gemeente Buren. Hieronder de vragen met de daarbij behorende inleiding/ aanleiding van de fractie GBO:

Gemeentebelangen Overbetuwe hecht een zeer grote waarde aan een zorgvuldige verwerking van (persoons-)gegevens. Op 22 april jongstleden is de gemeente Buren getroffen door een ransomware-aanval waarbij kwaadwillenden 130 gigabyte aan gegevens van Gemeente Buren en van de gemeente Neder-Betuwe hebben ontvreemd en daarna op het darkweb aangeboden. Op 23 mei heeft staatssecretaris van Huffelen kamervragen in dit kader beantwoord.

- De Informatiebeveiligingsdienst heeft de beveiligingsfunctionarissen van Nederlandse gemeenten geïnformeerd over deze ransomware-aanval en de maatregelen die mogelijk zijn om dergelijke situaties te voorkomen;
- Eerder werden de gemeenten Lochem (2019) en Hof van Twente (2020) getroffen door een ransomware-aanval. Deze gemeenten hebben lessen transparant gedeeld;
- De Baseline Informatiebeveiliging Overheid (BIO) stelt eisen aan o.a. het afhandelen van informatiebeveiligingsincidenten met inbegrip van vastgestelde procedures;
- Medio Q1 2021 heeft DMC Group in opdracht van de rekenkamercommissie een volwassenheidsonderzoek informatiebeveiliging uitgevoerd. Het rapport van 1 maart 2021 maakt duidelijk dat Gemeente Overbetuwe geen overzicht heeft van de mate waarin zij momenteel (aantoonbaar) aan de eisen van de BIO voldoet;
- In de raad van 21 april 2021 is het besluit genomen om in te stemmen met de conclusies en aanbevelingen van dit rapport en aan het college een aantal aanbevelingen mee te geven;
- Op 16 juni 2021 is de raad middels een informatiememo geïnformeerd over het plan van aanpak en de activiteiten die gemeente Overbetuwe in haar bedrijfsvoering doorvoert om haar informatieveiligheid te versterken.

Uw vraag 1: Heeft het college opvolging aan het advies van de Informatiebeveiligingsdienst gegeven ter voorkoming van een vergelijkbaar incident bij andere gemeenten? Indien niet, waarom niet?



Ons antwoord:

Ja.

Deze adviezen worden ontvangen via de door de Gemeentesecretaris bij de IBD (Informatiebeveiligingsdienst) aangemelde Vertrouwde Contactpersonen Informatiebeveiliging, waaronder de CISO's van zowel Overbetuwe als van Lingewaard (CISO = Chief Information Security Officer). Aangezien het beheer van de IT Infrastructuur door de gemeente Lingewaard wordt uitgevoerd zijn deze adviezen in het reguliere overleg van de CISO Overbetuwe met de IT organisatie van Lingewaard besproken. De adviezen worden gebruikt om de voortgaande verbeteringsacties waar nodig anders te prioriteren.

Uw vraag 2: Heeft het college de communicatie van eerdere incidenten (Lochem & Hof van Twente) gevolgd? Indien ja, zijn de spreekwoordelijke 'lessen gevolgd'?

Ons antwoord:

Ja. Zie ook de beantwoording van vraag 1.

De lessen die van deze incidenten geleerd kunnen worden zijn onderdeel van de besprekingen in de IT samenwerking tussen de gemeentes Overbetuwe en Lingewaard, bijvoorbeeld in de eisen die vooraf gesteld worden aan nieuwe IT infrastructuur en applicaties en het prioriteren van geïdentificeerde verbeteracties.

Uw vraag 3: Het bovenbedoelde plan van aanpak bevat een uitvoeringskalender met 41 onderwerpen. Wat is de actuele stand van zaken met betrekking tot deze (mn. #16) onderwerpen?

Ons antwoord:

De memo van 15 juni 2021 gaf aan dat op 3 terreinen, uitgewerkt in 41 acties / projecten prioriteit gegeven zou gaan worden aan de verbetering van de informatieveiligheid. Door de stuurgroep informatiebeveiliging wordt maandelijks bekeken hoe de voortgang is, en of de gestelde prioriteiten mogelijk aanpassing behoeven.

Belangrijkste resultaten voor de verschillende onderdelen, zoals ook genoemd in de eerdere beantwoording:

Voor het onderdeel **Governance** is door de indiensttreding per 1 juni van een nieuwe CISO voor Overbetuwe meer capaciteit beschikbaar gekomen om de activiteiten op te volgen en waar nodig te ondersteunen.

Voor het onderdeel **Risicomanagement** is in samenwerking met de Teammanagers een QuickScan gedaan, waarvan de resultaten meegenomen zijn in het bedrijfscontinuïteitsplan. Ook is een start gemaakt met het bijhouden van een intern risicoregister door de CISO en de PO (Privacy Officer).

Voor het onderdeel **Incident Management** (en met name #16) is door de nieuwe CISO gestart om het bestaande Beleid voor Incident Management en Respons aan te passen aan de actuele inzichten, en dit ook direct te koppelen aan nieuwe en duidelijke beschrijvingen voor het afhandelen van Datalekken zoals opgesteld door de Privacy Officer.



Uw vraag 4: Aan nieuwe (burger-)raadsleden is ten behoeve van de uitvoer van hun werkzaamheden recentelijk een nieuwe iPad in bruikleen gegeven. Technisch beheer over deze apparaten is niet (meer) centraal georganiseerd. De verantwoordelijkheid voor bijvoorbeeld patchmanagement (onderwerp #23 uitvoeringskalender) ligt daardoor bij de eindgebruiker.

- Hoe is dit te rijmen met de volgende uitspraak van het college: "informatieveiligheid is een cruciale randvoorwaarde voor een betrouwbare dienstverlening van gemeente Overbetuwe"?

Ons antwoord:

Vanuit het oogpunt van Informatiebeveiliging is er overleg geweest met de Griffier om te zien hoe de Raadsleden goed geïnformeerd kunnen worden over de aanwezige en gewenste maatregelen om zo veilig mogelijk met de verstrekte iPad en de daarop aanwezige informatie om te gaan. Er zal door de CISO en IT organisatie een presentatie worden gegeven die hierop ingaat, met daarna een sessie om overgebleven vragen te kunnen stellen.

Door de CISO is in overleg met de Stuurgroep Informatieveiligheid en de Griffier afgestemd dat de raadsleden ook uitgenodigd worden voor het volgen van de VNG training iBewustzijn Overheid. Deze training over informatiebeveiliging wordt ook gevolgd door alle gemeentelijke medewerkers.

Aan de leden van de nieuwe gemeenteraad van Overbetuwe is inderdaad een iPad ter beschikking gesteld om op een effectieve manier te kunnen vergaderen. Hierbij wordt gebruik gemaakt van een speciale applicatie (iBabs) om de stukken voor de vergaderingen in een veilige omgeving te kunnen delen. Deze applicatie is ontworpen om dit op een veilige manier te doen, waarbij de risico's van het mailen en lokaal bewaren van raadsstukken worden geminimaliseerd. Een andere belangrijke factor voor de veiligheid is het gedrag van de gebruikers, die er zorg voor moeten dragen dat er op een goede manier met vertrouwelijke informatie moet worden omgegaan.

Afsluitend:

We onderschrijven dat er doorlopend aandacht nodig is voor informatieveiligheid en zien dit als een belangrijk kwaliteitsaspect in de diensten en bedrijfsvoering van de gemeente Overbetuwe. Waar nodig wordt in samenwerking met de portefeuillehouder en de stuurgroep informatieveiligheid besloten welke acties hierbij prioriteit hebben.

Hoogachtend,

burgemeester en wethouders,
de gemeentesecretaris, de burgemeester,

P.J.E. Breukers

R.P. Hoytink-Roubos

