

Aan de gemeenteraadsfractie van de BSD
T.a.v. de heer L.H. van der Kallen
Nieuwstraat 4
4611 RS Bergen op Zoom



28 JULI 2016

Uw kenmerk:	LVDKMM/15025	Ons kenmerk:	U16-013395
Uw brief:	22-07-2016	Beh. door:	F.L.W. Meijer
Onderwerp:	Digitale veiligheid gemeentelijke website	Afdeling:	Middelen, Informatie en Processen

Datum:
Doorkiesnr.: 0154-277658
Bijlage(n):

Geachte heer Van der Kallen,

In uw brief van 22 juli 2016 stelt u ons vragen over Digitale veiligheid gemeentelijke website. Graag beantwoorden wij hieronder uw vragen als volgt.

Vragen

1. Is uw College op de hoogte van het onderzoek waarnaar in het BN artikel wordt verwezen?

Antwoord:

Ja, daar zijn wij van op de hoogte.

2. Zo ja, wat is de reactie van uw college op de daarin vermelde positie van de gemeenten Bergen op Zoom?

Antwoord:

Aangezien wij achter het gebruik van open standaarden staan en informatiebeveiliging een belangrijk onderwerp vinden, zijn wij niet tevreden met die positie. Deze positie is bepaald aan de hand van een gegeven percentage voor toepassing van drie open standaarden "IPv6", "DNSSEC" en "TLS". Hoe dit percentage tot stand komt is niet te herleiden. Feit blijft dat wij als gemeente, maar ook vele andere gemeenten, deze standaarden nog niet volledig toepassen.

3. Acht uw college de Bergse reactie adequaat?

Antwoord:

In onze reactie hadden wij de indruk dat het artikel van BNDeStem gebaseerd was op het eerdere artikel in Binnenlands Bestuur. Als reactie hebben wij toen hetzelfde antwoord doorgestuurd dat ook al naar de raads werkgroep ICT was gestuurd. Vervolgens heeft BNDeStem de mening van de IBD (Informatiebeveiligingsdienst voor gemeenten) als onze mening weergegeven, zonder de conclusie dat we hierop al actie hadden ondernomen om samen met de GR ICT West Brabant West dit projectmatig op te pakken.

4. Waarom houdt de gemeente Bergen op Zoom zich tot het heden niet aan de veiligheidsnormen zoals vastgesteld in de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)?

Antwoord:

Informatiebeveiliging vinden wij een belangrijk onderwerp. Informatiebeveiliging is ook altijd een afweging tussen de inspanning (geld en menskracht), het gebruiksgemak en het risico wat je loopt als gemeente. Hierin moeten steeds bewuste keuzes worden gemaakt. Wij laten ons hierbij leiden door adviezen vanuit de IBD en de Baseline Informatiebeveiliging Gemeenten (BIG). De baseline informatiebeveiliging bestaat uit zeer vele richtlijnen, die soms verplicht en dan weer optioneel zijn. Het is nooit mogelijk om alles in één keer op te pakken, vandaar dat wij planmatig steeds verdere stappen ondernemen om onze informatiebeveiliging op een adequaat niveau te houden.

5. Is uw college bereid op korte termijn een moderne standaard voor veilig internetgebruik, zoals IPv6, voor de beveiliging van de gemeentelijke website in te voeren?

Antwoord:

De open standaard IPv6 is geen standaard die een relatie heeft met informatiebeveiliging. Wij zullen deze standaard wel gaan toepassen op onze website, aangezien naar de toekomst toe de bereikbaarheid anders wordt aangetast.

De prioriteit ligt in eerste instantie bij de toepassing van de overige genoemde standaarden. Deze zorgen wel voor extra beveiliging en zijn ook door de IBD aangegeven om met voorrang op te pakken. Hierover is eind juni al contact geweest met de ICT WBW om zo snel mogelijk te komen tot een projectmatige aanpak voor de invoering van deze standaarden. Bij het niet goed invoeren van deze standaarden lopen we het risico dat e-mail en/of onze website niet meer bereikbaar zijn, vandaar dat dit zorgvuldig moet gebeuren.

6. Is uw college bereid om een externe beveiligingsspecialist de huidige website te laten doorlichten op veiligheidsaspecten?

Antwoord:

Jaarlijks wordt dit via een digid-audit ook getoetst door een onafhankelijke specialist op onze website. Deze audit hebben wij altijd met een positief resultaat afgerond. Voor het komende half jaar worden ook enkele onafhankelijke audits uitgevoerd op de infrastructuur bij de ICT WBW.

De bedoelde beveiligingsstandaarden hebben ook geen directe relatie met de software voor onze website, maar betreffen meer technische maatregelen. Vandaar dat wij ook contact hebben opgenomen met ICT WBW. ICT WBW zal samen met de provider van onze website moeten onderzoeken hoe deze standaarden zo snel mogelijk ingevoerd kunnen worden.

7. In januari 2015 is de website naar de mededeling van de gemeente Bergen op Zoom vernieuwd. In hoeverre is de beveiliging up-to-date gebracht?

Antwoord:

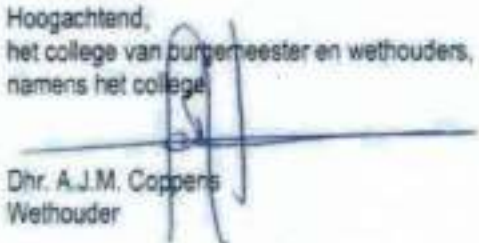
De vernieuwing van de website betrof een nieuwe versie van ons softwaresysteem (Content Management Systeem) en een nieuw uiterlijk. Het is dus geen volledig "nieuw" systeem, maar alleen een softwarematige aanpassing. De genoemde open standaarden hebben ook geen directe relatie met de softwarematige kant, maar vallen meer onder de categorie technische maatregelen.

ICT raadswerkgroep

Informatiebeveiliging is een veel breder onderwerp dan open standaarden. Graag willen wij in overleg met de griffie en de voorzitter van de ICT raadswerkgroep in een komend overleg van de raadswerkgroep een nadere toelichting geven op deze casus en laten zien hoe we informatiebeveiliging binnen onze gemeente hebben georganiseerd.

Mocht u over deze brief nog vragen of opmerkingen hebben dan kunt u contact opnemen met Drs. J.E. Dijk, bereikbaar via telefoonnummer (0164) 277531.

Hoogachtend,
het college van burgemeester en wethouders,
namens het college


Dhr. A.J.M. Coppens
Wethouder