Ons kenmerk: 13.027924
Relatie met:

GEMEENTE Schagen

Fractie D66 Schagen

Bezoekadres
Laan 19, 1741 EA Schagen
Postadres
Postbus 8, 1740 AA
Schagen

Tel. (0224) 210 400
Fax (0224) 210 455
postbus8@schagen.nl
www.schagen.nl

KvK 56838328
Bank NL25BNGH0285156721
BIC-code BNGHNL2G

Datum 9 december 2013
Ons kenmerk 13.027924
Afdeling FAC/IEA
Uw kenmerk
Contact M. Ligthart
Onderwerp Beantwoording Artikel 41 vragen fractie D66
Bijlagen
Afschrift

Geachte fractie ,

U heeft op 18 en 22 november jl. schriftelijke vragen gesteld over de onderwerpen:
- Bescherming van persoonsgegevens
- Beveiliging van de gemeentelijke website

Aangezien deze vragen beiden te maken met informatiebeveiliging combineren wij de beantwoording van beide vragen in één reactie.

Onderwerp: Bescherming van persoonsgegevens
Ingediend op 18 november 2013

Vragen
1) Is het college bekend met het onderzoek en de uitkomsten hiervan?
Het college is bekend met het onderzoek van de inspectie van Sociale Zaken en Werkgelegenheid waar naar wordt verwezen.

2) In hoeverre voldoet de bescherming van persoonsgegevens in de gemeente Schagen aan de normen die hiervoor zijn gesteld?
Gemeente Schagen heeft een privacyreglement voor de persoonsgegevens. Gemeente Schagen heeft twee privacybeheerders, die dagelijkse toezicht uitvoeren op de naleving van de privacyvoorschriften die voortvloeien uit de wet en de Wet bescherming persoonsgegevens.
Tevens heeft het college op 5 november j.l. het informatiebeveiligingsbeleid 2014-2018 goedgekeurd. Bij de behandeling van de volgende artikel 41 vragen omtrent beveiliging kunt u hier meer over lezen.

3) Heeft het college aanwijzingen dat er binnen de gemeente Schagen op ongeoorloofde wijze gegevens van bekende inwoners zijn geraadpleegd? Zo nee, is daar een gedragscode voor?
Het college heeft hiervoor geen aanwijzingen dat dit binnen de gemeentelijke organisatie het geval is. Het op ongeoorloofde wijze gegevens raadplegen van (bekende) inwoners zou kunnen duiden op een integriteitsprobleem. De medewerkers van de ambtelijke organisatie hebben allemaal in hun vorige gemeente (Harenkarspel, Schagen of Zijpe) een eed of gelofte afgelegd. In de nieuwe gemeente Schagen brengen wij opnieuw (en continue) de integriteit onder de aandacht, waarbij alle medewerkers nogmaals de eed of gelofte zullen afleggen.

In het onderzoek van de inspectie van Sociale Zaken en Werkgelegenheid wordt gerefereerd aan het systeem Suwinet. Via Suwinet kunnen overheidsorganisaties gegevens van burgers en bedrijven digitaal bij elkaar opvragen en naar elkaar sturen. Suwinet is primair bedoeld voor UWV, SVB en de gemeentelijke sociale diensten. De gemeenschappelijke regeling ISD Kop van Noord Holland controleert tweemaal per jaar op verleende toegangsrechten en raadplegingen. Uit deze controle blijkt dat er in 2012 vijfmaal oneigenlijk is geraadpleegd in Suwinet. Hiervoor zijn officiële waarschuwingen afgegeven.
Gemeente Schagen neemt de controle op de verleende toegangsrechten en oneigenlijke raadplegingen op persoonsgegevens op in haar controleplan 2014-2018.

4) Wat gaat het college doen om de bescherming van persoonsgegevens, indien nodig, te verbeteren?
Op dit moment zijn er geen redenen om extra aandacht te schenken aan de bescherming van persoonsgegevens.

Onderwerp: Beveiliging van de gemeentelijke website
Ingediend op 22 november 2013

Vragen
1) Is het college zich er van bewust dat de communicatie met de website van gemeente Schagen volledig onbeveiligd is?
Uit technisch onderzoek is gebleken dat de communicatie met de website van gemeente Schagen niet onbeveiligd is.

Technisch onderzoek:
Onze website wordt gehost door de SIMgroep. Naar aanleiding van de verplichte DigiD audit voor website met een DigiD koppeling is de beveiliging van de website door Ernst & Young geaudit op het normenkader dat is vastgesteld door Logius, onderdeel van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties. De beveiliging vanuit de SIMgroep voldoet aan de gestelde eisen.
Uw vraag richt zich de afspraakmodule. Deze module draait op een virtuele sever (beschermd achter een firewall in een demilitarized zone), het enige onderdeel van de website dat in deze situatie binnen onze ICT-omgeving is geplaatst. De gegevens die in de afspraakmodule worden ingevoerd door de burger, worden via een e-mail middels een beveiligde Gemnet verbinding naar deze virtuele server verzonden. De Gemnet verbinding is een beveiligde en beheerde verbinding. Gemnet is onderdeel van KPN Lokale Overheid,
Wij achten het risico daardoor acceptabel. Wij realiseren dat het voor een burger wellicht als niet-veilig wordt ervaren. Om dit gevoel te minimaliseren, hebben wij een SSL certificaat geïmplementeerd op de virtuele server. Dit zorgt voor een versleuteling van de gegevens van de e-mail en een zichtbaar 'slotje' op de website. Overigens wil dit eventuele externe bedreigingen (bijvoorbeeld door hackers) niet uitsluiten.

2) Is het college zich bewust van de risico's die de gemeente hiermee loopt?
Wij zijn ons bewust van de risico's die internet met zich meebrengt voor onze informatievoorziening. Wij maken een continue risicoafweging en kwalificeren het risico in deze situatie als acceptabel..

3) Is het college het met ons eens dat het zeer verstandig is om het deel van de website met het afsprakenformulier per direct af te sluiten?
Wij zien daartoe op dit moment geen reden.

4) Op welke termijn gaat het college het probleem oplossen en op welke wijze?
Zie antwoord vraag 1

5) Is het college het met ons eens dat er beleid gemaakt moet worden dat herhaling van deze situatie voorkomt en de beveiliging van persoonsgegevens op duurzame wijze borgt?
Op 5 november j.l. heeft het college ingestemd met het informatiebeveiligingsbeleid 2014-2018 met daarbij als hoofdmotto 'Van onbewust risico's lopen, naar bewust risico's nemen.' Zoals reeds eerder genoemd, maken wij bij beveiligingsrisico's een risicoafweging en worden indien noodzakelijk beveiligingsmaatregelen ingezet.
In tijd van snelle digitale ontwikkelingen is het namelijk niet de vraag of een beveiligingsrisico manifest wordt, maar wanneer. Het is daarom zaak om te weten hoe we dan moeten handelen, zodat de dienstverlening minimaal hinder hiervan ondervindt.

Tijdens de Buitengewone Algemene Ledenvergadering van de VNG op 29 november j.l. is ingestemd met de resolutie omtrent informatiebeveiliging, waarin o.a. staat vermeld dat elke gemeente verplicht is de Baseline Informatiebeveiliging Nederlandse Gemeenten te implementeren. Het informatiebeveiligingsbeleid 2014-2018 van gemeente Schagen is hier reeds op gebaseerd. Wij nemen elk signaal omtrent beveiligingsrisico's uiterst serieus en nodigen u ook uit hier over mee te (blijven) denken.

Bijgevoegd: Informatiebeveiligingsbeleid 2014-2018

Uitkomst gesprek 28-11-2013 omtrent beveiliging van de I-pads
Aanwezig vanuit de gemeenteraad: De heren van de Beek (VVD) en Bas (D66)
Aanwezig vanuit de organisatie: Albert van Tuil (afdelingshoofd Facilitair), Maaike Ligthart (adviseur informatiebeveiliging), Ricardo Bouwkamp (medewerker Helpdesk, contactpersoon Ipads)
Aanwezig namens Cloudyday: Bart Bosschieter

De heren van de Beek en Bas hebben hun zorgen geuit over het gevoerde beleid rondom Mobile Device Management door een extern ingehuurd bedrijf, namelijk CloudyDay. Afgesproken is, dat de raads- en commissieleden in januari een schriftelijke inlichting mogen ontvangen waarin het een en ander rondom Mobile Device Management en de rol van CloudyDay zal worden uiteengezet.

Met vriendelijke groet,
burgemeester en wethouders van de gemeente Schagen

de secretaris,

N.H. Swellengrebel

de burgemeester,

M.J.P. van Kampen-Nouwen