GEMEENTE VELSEN

Beantwoording vragen van de raad

Datum collegevergadering	20-12-2016
Registratienummer	Rs16.00782
Naam raadslid	Bram Diepstraten
Fractie	Velsen lokaal
Portefeuillehouder(s)	R. Vennik

Onderwerp: Datalek WOZ-gegevens

Toelichting bij de vragen:
Velsen Lokaal bedankt het college voor de uitgebreide informatie rondom het datalek bij een leverancier die betrokken is bij werkzaamheden in het kader van de Wet waardering onroerende zaken (WOZ). Het college heeft daarvoor een melding datalek bij de Autoriteit Bescherming Persoonsgegevens gedaan.

Velsen Lokaal hecht sterk aan de best mogelijke beveiliging van persoonsgegevens van onze inwoners en bedrijven. Daarom heeft mijn fractie een aantal vragen naar aanleiding van collegebericht 141 van vandaag.

Vraag 1

De Autoriteit Bescherming Persoonsgegevens spreekt van een meldingsplicht bij een ernstig datalek. En noemt alleen al het verlies van een laptop een duidelijk voorbeeld van een dergelijk datalek. Waarom spreekt het college van een 'mogelijk' datalek en niet van een ernstig beveiligingsincident?

Antwoord vraag 1

Het is duidelijk dat sprake is van een ernstig beveiligingsincident aangezien op de gestolen laptop persoonsgegevens zijn opgeslagen. Er kan niet worden vastgesteld of zich hieronder ook persoonsgegevens van, uit Velsen afkomstige, personen bevinden. Dit leek uitgesloten op basis van de verstrekte informatie over de diefstal. Er was, in eerste instantie, sprake van dat de persoonsgegevens via e-mailberichten op de laptop terecht gekomen zijn. Velsen levert deze gegevens op een andere, beveiligde, wijze bij het bedrijf aan.

Op 8 december 2016 heeft de Informatie Beveiligingsdienst Gemeenten (IBD) aangegeven dat ondanks deze beveiligde wijze van aanlevering niet volledig kan worden uitgesloten dat er toch gegevens van de gemeente Velsen bij het datalek zijn betrokken. Gezien het feit dat niet onomstotelijk kan worden vastgesteld of persoonsgegevens van inwoners uit Velsen op de betreffende laptop staan spreekt het college van een ‘mogelijk’ datalek. Dit neemt niet weg dat het incident door het college wel degelijk als ‘ernstig datalek’ wordt behandeld. Van het mogelijke datalek is daarom melding gedaan bij de Autoriteit Persoonsgegevens.

Vraag 2

Het College is volgens eigen zeggen op 2 december 2016 door de Informatiebeveiligingsdienst Gemeenten (IBD) geïnformeerd over het ernstige datalek. Andere gemeenten en belastingsamenwerkingsverbanden zeggen al op 30 november 2016 op de hoogte te zijn gesteld.

Hoe kan het dat Velsen pas op 2 december is geïnformeerd? Waarom heeft het college besloten om inwoners en de raad pas vandaag (9 december 2016) te informeren?

Antwoord vraag 2

De informatieverstrekking aan betrokken gemeenten is naar onze mening nogal rommelig verlopen. Op 30 november heeft de eigenaar van de gestolen laptop aan de IBD de diefstal van de laptop gemeld. Op dat moment was kennelijk van een aantal gemeenten al bekend dat hun bestanden op die laptop waren opgeslagen.

Op 2 december kwam er bericht van de IBD dat er mogelijk ook bestanden van andere gemeenten bij het datalek betrokken waren, waaronder Velsen. In de bijgevoegde brief van de eigenaar werd echter expliciet gesproken over bijlagen bij e-mails. Aangezien Velsen dit soort bestanden nooit per e-mail stuurt, maar via een beveiligde ftp-verbinding (bestanden komen dan niet op een laptop terecht maar staan direct op een server in de beveiligde netwerkomgeving van de ontvanger), hebben wij toen moeten concluderen dat er van een datalek voor de gemeente Velsen geen sprake was.

Op 8 december werden wij vervolgens door de IBD geïnformeerd dat er mogelijk toch bestanden vanuit de netwerkomgeving van de eigenaar naar de laptop gekopieerd zijn. Daarop is de behandeling van dit incident als datalek in gang gezet. Het lek is op 8 december gemeld aan de Autoriteit Persoonsgegevens. Op 9 december zijn de gemeenteraad en inwoners van Velsen op de hoogte gesteld.

Vraag 3

De betreffende leverancier heeft een van de meest elementaire beveiligingsmaatregelen om persoonsgegevens te beschermen geschonden. Wie is de leverancier? Op welke wijze heeft het college voorafgaande aan de werkzaamheden de leverancier gewezen op de veiligheidsmaatregelen die genomen moeten worden en hoe controleert het college leveranciers die persoonsgegevens van inwoners en bedrijven verwerken en opslaan? En gaat het college over tot ontbinding van de samenwerking met deze leverancier? Zo nee, waarom niet?

Antwoord vraag 3

De leverancier is het bedrijf Geotax. De gemeente Velsen heeft al lange tijd een zakelijke relatie met dit bedrijf. In de, met Geotax gesloten overeenkomst is een beschrijving opgenomen van de beveiligingsmaatregelen die zijn genomen om hun bedrijfsnetwerk te beveiligen. Dit wordt jaarlijks gecontroleerd door middel van het ICT Beveiligingsassessment DigiD.
Het buiten het bedoelde beveiligde bedrijfsnetwerk op een laptop beschikbaar hebben van dergelijke persoonsgegevens valt uiteraard niet te rijmen met de naleving van de Wet bescherming persoonsgegevens. Niet in het algemeen en zeker niet in relatie tot de met Geotax afgesproken veiligheidsmaatregelen.

Door de gegevens op een slecht beveiligde computer buiten de netwerkomgeving van Geotax mee te nemen is er een onverantwoord risico genomen. Uw vraag om de zakelijke relatie met Geotax ter discussie te stellen is daarom terecht. Het college heeft dit nog in beraad en daarom is er over eventuele ontbinding van de samenwerking nu nog geen uitspraak te doen.

Vraag 4

Uit het collegebericht en de informatie voor inwoners komt wat Velsen Lokaal betreft onvoldoende naar voren dat overheden, in dit geval de gemeente Velsen, hoofdverantwoordelijk zijn voor een veilige verwerking en opslag van persoonsgegevens. Is het college er zich voldoende bewust van dat hij hoofdverantwoordelijke is voor beveiliging van persoonsgegevens en dus voor ernstige

veiligheidsincidenten? Hoe waarborgt het college dat leveranciers die voor de gemeente Velsen persoonsgegevens verwerken en opslaan dit volgens richtlijnen van de IBD doen? Is het Informatiebeveiligingsbeleid van de gemeente Velsen voldoende in de ogen van het college? Zo nee, gaat het college het beleid aanscherpen? En is dat beleid goed bekend bij leveranciers?

Antwoord vraag 4

Het college is zich terdege bewust van haar verantwoordelijkheid voor de veilige verwerking en opslag van persoonsgegevens. In het collegebericht staat daarom ook dat de gemeente Velsen in overleg met de informatiebeveiligingsdienst en de betrokken leverancier werkt aan een zorgvuldige afhandeling. Het waarborgen van een veilige gegevensbewerking volgens de richtlijnen van de IBD wordt geregeld door het sluiten van bewerkersovereenkomsten met de afzonderlijke leveranciers. Hierin staat precies beschreven welke maatregelen uit de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) de gemeente Velsen in werking wil hebben bij het aangaan van een zakelijke relatie waarbij sprake is van verwerking van persoonsgegevens.
Het gemeentelijk ‘Beleid Informatiebeveiliging’ is gebaseerd op de genoemde BIG-normen en is van toepassing op de gehele informatievoorziening van de gemeente Velsen. In combinatie met het recentelijk vastgestelde ‘Overkoepelend beleid privacy & gegevensbescherming’ biedt deze regeling een toereikend kader voor een veilige en zorgvuldige verwerking van persoonsgegevens. Dit gemeentelijk beleid is, door middel van het afsluiten van bewerkersovereenkomsten, ook bekend bij de leveranciers.

Het college van burgemeester en wethouders van de gemeente Velsen