

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

2742

Vragen van de leden **Oosenbrug** en **Fokke** (beiden PvdA) aan de Minister van Binnenlandse Zaken en Koninkrijksrelaties over *het bericht «beveiliging tientallen gemeentesites lek: persoonsgegevens niet veilig»* (ingezonden 12 mei 2016).

Antwoord van Minister **Plasterk** (Binnenlandse Zaken en Koninkrijksrelaties) (ontvangen 6 juni 2016).

Vraag 1

Herinnert u zich uw antwoorden op eerdere vragen over het bericht «beveiliging tientallen gemeentesites lek: persoonsgegevens niet veilig»?¹

Antwoord 1

Ja.

Vraag 2

In hoeveel gemeenten is de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) inmiddels volledig geïmplementeerd? Zijn bij u, ondanks de implementatie van de BIG, toch nog berichten bekend dat er in gemeenten gebruik wordt gemaakt van een onbeveiligde https-verbinding wanneer zij naar vertrouwelijke informatie van burgers vragen? Zo ja, in hoeveel gemeenten wordt nog niet gebruik gemaakt van een beveiligde https-verbinding bij het verwerken van vertrouwelijke informatie van burgers? Zo nee, bent u bereid onderzoek te doen naar de beveiliging van gemeentewebsites en de verzameling en verwerking van vertrouwelijke informatie door gemeentes via deze websites?

Antwoord 2

Gemeenten zijn zoals afgesproken in de resolutie «informatieveiligheid, randvoorwaarde voor de professionele gemeente» bezig met het implementeren van de BIG. Deze baseline bevat een breed scala aan technische, organisatorische, fysieke en procedurele maatregelen. De implementatie ervan is een doorlopend proces waarbij gemeenten op basis van eigen afwegingen het gemeenschappelijke normenkader als leidraad gebruiken. Zo betekent bijvoorbeeld voor een gemeente die zijn ICT heeft ondergebracht bij een externe leverancier de implementatie iets heel anders dan voor een

¹ Aanhangsel-Handelingen vergaderjaar 2015–2016, nr. 2076

gemeente die zijn ICT 100% in eigen beheer uitvoert. In algemene zin hebben alle gemeenten inmiddels de voor hen belangrijkste maatregelen uit de BIG geïmplementeerd. Welke dat zijn hangt af van de lokale afweging per gemeente.

Mij is bekend, onder andere uit de pers en van individuele onderzoekers op het gebied van informatiebeveiliging dat niet alle gemeenten https gebruiken voor webformulieren waarmee de gemeente een burger om informatie vraagt, bijvoorbeeld in het kader van dienstverlening. Wanneer de gemeente persoonsgegevens verwerkt, dient de gemeente op basis van artikel 13 van de Wet bescherming persoonsgegevens een passend beveiligingsniveau te garanderen. De richtsnoeren van het College bescherming persoonsgegevens (thans Autoriteit persoonsgegevens) uit 2013 die hierop van toepassing zijn, schrijven voor dat de bewerker encryptie (versleuteling) toe dient te passen bij verzending van persoonsgegevens via het internet. Ook de BIG schrijft dit voor voor het veilig verwerken van gevoelige gegevens.

Ik heb kennis genomen van het onderzoek van RTL Nieuws dat aantoonde dat bij 10 van de 390 gemeenten het afsprakenformulier niet was beveiligd door middel van https. Deze 10 gemeenten zijn door de Informatiebeveiligingsdienst voor gemeenten (IBD) op de hoogte gesteld van dit feit en zij hebben alle in samenwerking met hun leveranciers deze situatie opgelost. Het gaat erom dat gemeenten adequate actie ondernemen bij het bekend worden van kwetsbaarheden. De gemeente is zelf verantwoordelijk voor het naleven van de wettelijke eisen om persoonsgegevens te beschermen. De Autoriteit Persoonsgegevens ziet daarop toe. De gemeente is ook zelf verantwoordelijk voor een afdoende beveiliging van gevoelige en vertrouwelijke informatie. Gemeenten leggen hierover verantwoording af aan de gemeenteraad. Een onderzoek zoals u dat schetst zou als momentopname van de toepassing van een enkele technische maatregel mijns inziens onvoldoende meerwaarde bieden ten opzichte van het huidige verantwoordingsstelsel.

Vraag 3

Zijn gemeenten naar uw mening voldoende uitgerust om op een goede en veilige manier vertrouwelijke informatie van burgers te verwerken via gemeentewebsites? Is er voldoende kennis en fte beschikbaar binnen gemeenten om gemeentewebsites te beheren? Zo nee, welke aanvullende maatregelen gaat u nemen om gemeenten beter uit te rusten om vertrouwelijke informatie van burgers te verwerken via gemeentewebsites en om deze sites te beheren?

Antwoord 3

In het algemeen zijn gemeenten voldoende toegerust om op een goede en veilige manier vertrouwelijke informatie te verwerken. Ze hebben zich geïmplementeerd aan de implementatie van de BIG. Zie ook het antwoord op vraag 2. Hoeveel kennis en fte er beschikbaar is of moet zijn om gemeentewebsites te beheren, verschilt van gemeente tot gemeente. Het is daarom niet zonder meer mogelijk om algemene uitspraken te doen over maatregelen.

Gemeenten werken dagelijks samen met hun leveranciers aan informatiebeveiliging, of dit nu gaat om de website of anderszins. Gemeenten hebben zeer veel kennis in huis en kunnen tevens, onder andere via de IBD, kennis van andere gemeenten benutten. Ik heb geen signalen dat gemeenten onvoldoende fte beschikbaar hebben om de website te beheren.

Vraag 4

Deelt u de mening dat burgers afhankelijk zijn van hun eigen gemeente voor dienstverlening en dat daarom in alle gemeenten de kwaliteit en veiligheid van de dienstverlening via gemeentewebsites hetzelfde niveau moet hebben?

Antwoord 4

Ik ben het eens met de stelling dat burgers voor de dienstverlening afhankelijk zijn van de gemeente waarin ze wonen. Daarnaast moeten de kwaliteit en veiligheid op een adequaat niveau zijn. Hoe hoog dat niveau is, zal nog steeds van gemeente tot gemeente kunnen verschillen, met dien verstande dat de toezichthouder Autoriteit persoonsgegevens toezicht houdt op het minimumniveau van gegevensbescherming. Daar mag een gemeente nooit onder zakken.

In algemene zin zijn er uiteraard wel maatregelen te benoemen die altijd genomen dienen te worden om een minimumniveau te garanderen. Het versleutelen van gegevens op internet is daarvan een voorbeeld.

Vraag 5

Herinnert u zich de vragen over de mogelijkheid om één kernwebsite voor alle gemeenten te maken? Deelt u de mening dat dit voor de veiligheid, kwaliteit en het beheer van deze websites voordelen kan opleveren? Bent u bereid opnieuw naar dit voorstel te kijken? ²

Antwoord 5

Ja, ik herinner mij die vragen en ik deel de mening dat één kernwebsite voordelen kan opleveren. In mijn brief van 20 april 2015 heb ik in de Kamer verslag gedaan van mijn overleg met de VNG over dit onderwerp (Kamerstuk 26 643, nr. 357). De VNG gaf aan dat één uniforme (model-)website naar haar mening geen recht doet aan de verschillen die er tussen gemeenten bestaan. Ik blijf echter attent op de mogelijkheid om een kernwebsite dichterbij te brengen. Het Kwaliteitsinstituut Nederlandse Gemeenten (KING) ontwikkelt momenteel een *proof of concept* voor een Generieke Transactievoorziening waarbij gemeentelijke formulieren voor ondernemers centraal worden aangeboden. Als deze *proof of concept* slaagt, zal ik met de VNG gaan overleggen over de mogelijkheden om dit ook te doen met formulieren voor burgers.

Vraag 6

Deelt u de mening dat de privacy van burgers vanuit de BIG onvoldoende gewaarborgd is? Wat vindt u van het voorstel om naast de BIG een privacy-BIG in te stellen om de privacy van burgers te waarborgen? Bent u inmiddels in gesprek met de Vereniging van Nederlandse Gemeenten (VNG) en KING (Kwaliteitsinstituut Nederlandse Gemeenten) over de haalbaarheid van zo'n privacy-BIG en wat is de stand van zaken met betrekking tot dit voorstel?

Antwoord 6

De BIG, de naam zegt het al, biedt een baseline voor informatiebeveiliging. Een deugdelijke beveiliging van gegevens is één van de aspecten die aandacht verdienen bij het beschermen van persoonsgegevens, waaraan gemeenten gehouden zijn op grond van de Wet bescherming persoonsgegevens. Daarnaast behelst het adequaat waarborgen van de privacy van burgers vele andere aspecten, die onder andere genoemd zijn in de Rijksvisie over privacy in het sociaal domein; «zorgvuldig en bewust» en in de Privacy Impact Assessment 3D.

Met het in de EU aannemen van de algemene verordening gegevensbescherming (PbEU 2016, L 119), die op 25 mei 2018 van toepassing wordt en de huidige Wet bescherming persoonsgegevens grotendeels zal vervangen, zullen gemeenten net als andere verantwoordelijken voor gegevensverwerking bovendien moeten voldoen aan diverse nieuwe plichten, zoals maatregelen van *privacy by design*, het uitvoeren van *privacy impact assessments* en het aanstellen van een functionaris voor de gegevensbescherming. Naast de BIG zijn er dus andere waarborgen voor de bescherming van persoonsgegevens.

Op ambtelijk niveau zijn de gesprekken die ik heb toegezegd tijdens het algemeen overleg op 20 april gestart. Ik zal uw Kamer over de uitkomsten daarvan informeren.

² Algemeen overleg Informatie- en communicatietechnologie (ICT), Kamerstuk 26 643, nr. 276