Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2015–2016 **Aanhangsel van de Handelingen**

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

2943

Vragen van het leden **Oosenbrug** en **Fokke** (PvdA) aan de Minister van Binnenlandse Zaken en Koninkrijksrelaties over *het bericht «Gemeentelijke e-mail slecht beveiligd»* (ingezonden 6 juni 2016).

Antwoord van Minister **Plasterk** (Binnenlandse Zaken en Koninkrijksrelaties) (ontvangen 24 juni 2016).

Vraag 1
Kent u het bericht «Gemeentelijke e-mail gênant slecht beveiligd?[1]

Antwoord 1
Ja.

Vraag 2
Herinnert u zich uw antwoorden op eerdere vragen over de beveiliging van gemeentelijke e-mail?[2] [3]

Antwoord 2
Ja.

Vraag 3
Is het waar dat nog steeds vrijwel geen enkele gemeente voldoet aan de verplichte beveiligingsstandaarden voor e-mail? Zo ja, heeft u zicht op hoeveel gemeente niet voldoen aan de verplichte beveiligingsstandaarden voor e-mail? Zo nee, waarom niet?

Antwoord 3
In het bericht wordt gerefereerd aan de open beveiligingsstandaarden DKIM+SPF+DMARC (anti-phishing), DNSSEC (domeinnaambeveiliging) en STARTTLS (beveiligde verbindingen).
DKIM+SPF en DNSSEC staan op de *pas-toe-of-leg-uit lijst*van het Forum Standaardisatie. DMARC en STARTTLS in combinatie met DANE zijn kandidaat om opgenomen te worden. De open standaarden die op de

[1] http://www.binnenlandsbestuur.nl/digitaal/nieuws/gemeentelijke-e-mail-genant-slecht-beveiligd.9539030.lynkx?mt=FfLP8ugWOAONiqm3bqdd6g&vk=f17W0JP2dJnbybrtiBvkOg&pub=1002
[2] Aanhangsel Handelingen, vergaderjaar 2015–2016, nr. 319
[3] Aanhangsel Handelingen, vergaderjaar 2015–2016, nr. 928

ah-tk-20152016-2943
ISSN 0921 - 7398
's-Gravenhage 2016

pas-toe-of-leg-uit lijst staan, zijn verplicht bij aanschaf, aankoop, aanbesteding of ontwikkeling van nieuwe diensten.
Volgens cijfers van het Bureau Forum Standaardisatie [https://www.forumstandaardisatie.nl/fileadmin/os/publicaties/Monitor_OSb_2015_Definitief.pdf] was DKIM in 2015 bij 77 gemeenten geïmplementeerd. Concluderend meldt het rapport (p. 24): «Iets meer dan één vijfde van de domeinnamen van overheden is in 2015 voorzien van een DKIM-configuratie. De verschillen tussen de verschillende overheden zijn niet groot.»
Voor deze standaarden is door het Nationaal Beraad een adoptie-impuls afgesproken, met het streefbeeld om de beveiligingsstandaarden die reeds op de pas-toe-of-leg-uit-lijst staan (TLS, DKIM+SPF en DNSSEC) – daar waar van toepassing – uiterlijk eind 2017 te hebben geïmplementeerd.
Gemeenten werken op verschillende fronten aan de bestrijding van spam en phishing. In de eerste plaats gaat het om het vergroten van de bewustwording binnen gemeenten; dit geldt eveneens voor burgers en bedrijven. In de tweede plaats zijn er additionele maatregelen zoals antispam- en antivirusoplossingen voor e-mail en firewallinstellingen.
De Informatiebeveiligingsdienst voor gemeenten (IBD) maakt factsheets rond de implementatie van DMARC, SPF en DKIM, om gemeenten op de hoogte te brengen van de standaarden en de voordelen van het implementeren ervan. Verder informeert IBD de betrokken leveranciers van klantcontactcentra, hostingpartijen, providers e.d. over de standaarden, zodat ze zich klaar kunnen maken voor vragen van gemeenten.

Vraag 4
Deelt u de mening dat het zorgelijk is dat, vanwege de gebrekkige beveiliging van e-mailverkeer van gemeenten, de persoonsgegevens die worden uitgewisseld in verkeerde handen kunnen vallen? Zo ja, hoe gaat u de desbetreffende gemeenten daar op aanspreken? Zo nee, waarom niet?

Antwoord 4
De betreffende standaarden DKIM / DMARC en SPF zorgen voor e-mailauthenticatie; hiermee wordt het mogelijk dat de ontvanger de identiteit van de afzender deels controleert. De standaarden hebben een belangrijke functie bij de mogelijke herkenning van spam en phishing voor zover deze gebruik maken van spoofing (waarbij een verzender zich voordoet als een ander).
Gebruik van deze standaarden is één van de schakels in de bestrijding van phishing en de beveiliging van persoonsgegevens. Omdat behalve gebruik van deze standaarden ook andere maatregelen genomen worden, onderschrijf ik niet dat door het enkele feit dat deze standaarden niet worden gebruikt persoonsgegevens in verkeerde handen vallen.

Vraag 5
Heeft u er zicht op in hoeveel gemeenten geen STARTLLS-standaard wordt aangehouden en er daardoor geen beveiligde internetverbinding mogelijk is?

Antwoord 5
De standaard STARTTLS is in combinatie met DANE (voor beveiligde mailverbindingen) in behandeling genomen door het Forum Standaardisatie en kan daardoor, mogelijk al in 2016, worden opgenomen op de lijst met open standaarden. Het Forum Standaardisatie zal vanaf dan ook de implementatie bij aanschaf, aankoop en aanbestedingen monitoren.

Vraag 6
Wat is volgens u de oorzaak van het probleem dat gemeenten de verplichte internetstandaarden voor de beveiliging van e-mail niet aanhouden? Hoe gaat u ervoor zorgen dat deze standaarden in alle gemeenten gehandhaafd worden?

Antwoord 6
De internetstandaarden die op de *pas-toe-leg-uit-lijst* staan, zijn verplicht bij aanschaf, aankoop, ontwikkeling of aanbesteding van nieuwe diensten, tenzij er een zwaarwegende reden is om hiervan af te wijken. Het handhaven in

bestaande situaties is niet aan de orde. De versnelde implementatie is onderdeel van een lokaal afwegingskader.
Door het uitvoeren van een impactanalyse heeft de IBD uitgezocht welke impact de implementatie van deze standaarden voor gemeenten heeft. Hieruit blijkt dat de implementatie van de standaarden meer impact heeft naarmate de organisatie groter en complexer is. Voor met name DMARC moeten alle gemeentelijke mailstromen in kaart zijn gebracht en worden vertaald in beveiligingsregels. Het fout instellen van deze standaarden leidt tot een verstoring in e-mail van en aan de gemeente.
Zoals ik uw Kamer heb aangegeven in mijn brief met uitgangspunten wetgeving GDI (Kamerstuk 26 643 nr. 373) werk ik in deze wet aan een grondslag waarmee – nader te bepalen – standaarden uit de *pas-toe-of-leg-uit-lijst* wettelijk verplicht kunnen worden gesteld voor bestuursorganen, onder andere voor uniformering voor burgers en bedrijven, en het garanderen van communicatie. Daarbij speelt ook informatiebeveiliging een rol. De VNG onderschrijft die uitgangspuntenbrief.

Vraag 7
Hebben de gemeenteraden en de Autoriteit Persoonsgegevens (AP) voldoende middelen om toezicht te houden op de naleving van de wettelijk geldende eisen voor de verwerking van persoonsgegevens? Geven de gemeenteraden en de AP voldoende prioriteit aan het toezicht houden op de naleving van de wettelijk geldende eisen voor de verwerking van persoonsgegevens? Zo nee, hoe gaat u ervoor zorgen dat hier meer prioriteit aan wordt gegeven? Zo ja, hoe kan het dan nog steeds mis gaan?

Antwoord 7
Gemeenteraden bestaan uit gekozen volksvertegenwoordigers. Op grond daarvan en de verantwoordelijkheden en bevoegdheden van gemeenten voortvloeiend uit de Grondwet en de Gemeentewet, voeren gemeenten hun wettelijke taken zelfstandig uit. In die zin acht ik gemeenteraden en het gemeentebestuur zeer wel in staat om zorg te dragen voor de naleving van privacyregels en voor een afdoende niveau van de gemeentelijke informatieveiligheid. Desalniettemin kan het Rijk op grond van de Gemeentewet – in het kader van interbestuurlijk toezicht – toezicht houden op het gemeentebestuur. Dat is bij mijn weten nog niet voorgekomen in het geval van tekortkomingen op het gebied van de verwerking van persoonsgegevens of informatieveiligheid.
Het specifieke toezicht op de naleving van de wettelijke bepalingen inzake de verwerking van persoonsgegevens wordt gehouden door de Autoriteit Persoonsgegevens (AP). De AP richt als onafhankelijke toezichthouder haar eigen toezicht in. In het uitvoeren van haar toezichthoudende en handhavende taak stelt de AP prioriteiten op basis van criteria, zoals de ernst en de duur van de overtreding.
De AP dient haar taken in onafhankelijkheid te kunnen uitoefenen, zonder inmenging van buitenaf. Daarnaast kan ik u mededelen dat er geen signalen bekend zijn waaruit blijkt dat de AP tekortschiet in het houden van toezicht op de naleving van de wettelijke eisen voor de verwerking van persoonsgegevens.

Vraag 8
Herinnert u zich uw antwoorden op de vele vragen die gesteld zijn over de beveiliging en verwerking van persoonsgegevens in gemeenten?[4] [5] [6] [7]

Antwoord 8
Ja.

[4] Aanhangsel Handelingen, vergaderjaar 2015–2016, nr. 1613
[5] Aanhangsel Handelingen, vergaderjaar 2015–2016, nr. 2076
[6] Aanhangsel Handelingen, vergaderjaar 2015–2016, nr. 2401
[7] Aanhangsel Handelingen, vergaderjaar 2015–2016, nr. 2643

Vraag 9
Deelt u de mening dat gemeenten onzorgvuldig omgaan met de persoonsgegevens van hun inwoners? Deelt u de mening dat het bericht «Gemeentelijke e-mail gênant slecht beveiligd» past in dit beeld?

Antwoord 9
Neen. Gemeenten hebben zich gecommitteerd aan de beveiliging van persoonsgegevens en hechten hieraan grote waarde. De implementatie van open standaarden heeft een plek in de activiteiten die gemeenten ontplooien om het gemeentelijk informatielandschap te beveiligen conform de uitgangspunten en kaders van hun gemeenschappelijk normenkader de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). De volgorde van implementatie van maatregelen (ook technische detailmaatregelen, maar vooral ook fysieke en organisatorische maatregelen) is gebaseerd op een lokale risicoafweging waar het college van B&W voor verantwoordelijk is.

Vraag 10
Zijn er volgens u ook goede voorbeelden van gemeenten die voldoen aan alle wettelijke eisen en zorgvuldig omgaan met de persoonsgegevens van burgers? Welke zijn dit? Waarom lukt het hier wel? Hoe gaat u ervoor zorgen dat dit goede voorbeeld gedeeld wordt met andere gemeenten?

Antwoord 10
Zonder in te gaan op de specifieke casuïstiek van individuele gemeenten, zijn er voorbeelden bekend van gemeenten waar bijvoorbeeld de gemeentelijke rekenkamer onderzoek heeft gedaan naar de mate van beveiliging van informatie. Dergelijke onderzoeken stellen college en raad in de gelegenheid om het niveau van informatieveiligheid te verhogen.
Uiteraard moeten gemeenten voldoen aan wettelijke eisen en dienen ze zorgvuldig om te gaan met persoonsgegevens. Dat wil niet zeggen dat er nooit iets mis gaat. Gemeenten werken aan bewustwording bij medewerkers, werken aan informatieveiligheid en weten zich gesteund door de IBD. De IBD draagt ook bij aan kennisdeling op het gebied van best practices. Daarnaast is privacy een belangrijk onderdeel van het programma ISD van de VNG. Ook via dat programma worden vele goede praktijken van gemeenten gedeeld.

Vraag 11
Wat vindt u het voorstel om naast de Baseline Informatiebeveiliging Nederlandse Gemeenten (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 11
De Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) maakt deel uit van de Resolutie Informatieveiligheid waarmee de leden van de VNG op 29 november 2013 hebben ingestemd. Een voorstel om daarnaast een privacy-BIG in te stellen, lijkt me in dat kader iets voor de gemeenten om te besluiten.
VNG en gemeenten vinden, net als ik, een goede omgang met privacy zeer belangrijk. Onlangs werd op de ALV van de VNG privacy als prioriteit op de agenda gezet met het Position Paper Privacy. Gemeenten geven daarin aan dat het borgen van privacy en een correcte gegevensbescherming in alle gemeenten van groot belang zijn en een zeer belangrijke basis voor het vertrouwen van burgers, bedrijven, ketenpartners en medeoverheden in gemeenten. Gemeenten willen hun inzet op het gebied van het privacyvraagstuk versterken en collectiviseren. In het position paper zijn hiervoor tien actiepunten opgenomen. Een van de actiepunten houdt in dat de VNG in overleg met bestuurders (waaronder ook raadsleden), ambtenaren, ketenpartners en experts onderzoek doet naar de mogelijkheid om gezamenlijke privacykaders (normen) te ontwikkelen. Ik blijf in contact met de VNG over de ontwikkelingen en voortgang hiervan.