Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2009–2010

Aanhangsel van de Handelingen

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

22

Vragen van de leden **De Roon** en **Brinkman** (beiden PVV) aan de minister-president, minister van Algemene Zaken, en de ministers van Binnenlandse Zaken en Koninkrijksrelaties, van Buitenlandse Zaken, van Defensie, van Economische Zaken, van Financiën, voor Jeugd en Gezin, van Justitie, van Landbouw, Natuur en Voedselkwaliteit, van Onderwijs, Cultuur en Wetenschap, voor Ontwikkelingssamenwerking, van Sociale Zaken en Werkgelegenheid, van Verkeer en Waterstaat, van Volksgezondheid, Welzijn en Sport, van Volkshuisvesting, Ruimtelijke Ordening en Milieubeheer en voor Wonen, Wijken en Integratie over *slechte beveiliging van persoonsgegevens in databestanden van de overheid*. (Ingezonden 4 augustus 2009)

1
Kent u de berichtgeving, dat 570 overheidswebsites dermate onvoldoende beveiligd zijn, dat buitenstaanders via die websites persoonsgegevens van burgers kunnen bemachtigen?[1]

2
Welke websites (voor zover – direct of indirect – vallend onder uw verantwoordelijkheid) betreft dit?

3
Hoe beoordeelt u, per site, de conclusie van de onderzoekers dat persoonsgegevens door onbevoegden kunnen worden bemachtigd?

4
Onderschrijft u de opvatting dat het risico groot is dat vanaf overheidswebsites gestolen persoonsgegevens door criminelen worden misbruikt?

5
Welke verklaring geeft u, per site, voor de eventueel ontoereikende beveiliging van de persoonsgegevens?

6
Welke maatregelen gaat u, per site, nemen om de beveiliging te verbeteren? Op welke termijn zal die beveiliging voldoende zijn? Wat gaat u doen om in de tussentijd te voorkomen dat persoonsgegevens worden gestolen?

[1] Networking4all: «Websites overheid onveilig» http://www.networking4all.com/nl/over+ons/nieuws/bedrijfsnieuws/overheid+onveilig/

Antwoord

Antwoord van staatssecretaris **Bijleveld-Schouten** (Binnenlandse Zaken en Koninkrijksrelaties), mede namens de minister president en de ministers van Binnenlandse Zaken en Koninkrijksrelaties, van Buitenlandse Zaken, van Defensie, van Economische Zaken, van Financiën, voor Jeugd en Gezin, van Justitie, van Landbouw, Natuur en Voedselkwaliteit, van Onderwijs, Cultuur en Wetenschap, voor Ontwikkelingssamenwerking, van Sociale Zaken en Werkgelegenheid, van Verkeer en Waterstaat, van Volksgezondheid, Welzijn en Sport, van Volkshuisvesting, Ruimtelijke Ordening en Milieubeheer en voor Wonen, Wijken en Integratie (ontvangen 17 september 2009), Zie ook Aanhangsel Handelingen, vergaderjaar 2008–2009, nr. 3617

1
Ja.

2
De berichtgeving is gebaseerd op een onderzoek van de firma NETWORKING4ALL, leverancier van SSL-certificaten. Met deze firma is contact opgenomen om te kunnen beschikken over de lijst van 570 websites; NETWORKING4ALL heeft deze lijst tot nu toe niet kunnen aanleveren. Naar aanleiding van het onderzoek van NETWORKING4ALL zijn alle departementen bezig met het doorlichten van hun websites.

3
Een beoordeling per site kan ik niet geven, gegeven het feit dat de lijst niet beschikbaar is gesteld en de departementen nog met hun eigen doorlichting bezig zijn. In algemene zin kan ik wel zeggen dat de

KVR37638
2009Z14497
0910tkkvr22
ISSN 0921 - 7398
Sdu Uitgevers
's-Gravenhage 2009

conclusies van de onderzoekers gebaseerd zijn op de mogelijkheid om de communicatie met een website die niet met SSL beveiligd is «af te luisteren». Dat is inderdaad in beginsel mogelijk, maar het afluisteren van gegevensverkeer naar een website – door een internetverbinding naar de server af te tappen – is technisch ingewikkeld en kostbaar. Het afluisteren van onbeveiligd draadloos internetverkeer van een burger is technisch wel eenvoudig, maar is erg ongericht, waardoor de opbrengst aan persoonsgegevens op voorhand erg onzeker is.

4
De onveiligheid die het rapport van NETWORKING4ALL aankaart betreft hoofdzakelijk het onderscheppen van individuele online invulformulieren waarmee burgers een brochure kunnen aanvragen of een klacht kunnen indienen. Het betreft nadrukkelijk niet het ongeautoriseerd toegang krijgen tot integrale databestanden met persoonsgegevens (waarnaar in de aanhef van uw vragen wordt gerefereerd) of het verzenden van digitale belastingaangiften. Voor zover via invulformulieren uitsluitend naam- en adresgegevens (zogenaamde telefoonboekgegevens) worden uitgewisseld acht ik het risico op diefstal en op misbruik beperkt.

5
Voor mij toont het onderzoek van NETWORKING4ALL niet aan dat de beveiliging van de websites van de Rijksoverheid ontoereikend is. De regelgeving omtrent het beschermen van persoonsgegevens vereist niet dezelfde mate van beveiliging voor alle gegevens. In het rapport van NETWORKING4ALL wordt geen onderscheid gemaakt naar de aard van de informatie die met contactformulieren wordt ingewonnen. Ook als een niet beveiligd contactformulier uitsluitend een emailadres uitvraagt wordt dit door NETWORKING4ALL als ontoereikende beveiliging aangemerkt.

6
Lopende de analyse van de websites van de Rijksoverheid kan ik nog niet per site aangeven of er maatregelen moeten worden getroffen. Wel kan ik zeggen dat bij de analyse niet alleen de regelgeving als uitgangspunt zal dienen, maar ook het feit dat het kabinet het van groot belang acht dat de burger de overheid en haar websites kan vertrouwen. Daarom zullen ook waar dat vanuit juridisch oogpunt niet strikt nodig is maar wel vanuit het oogpunt van vertrouwen in de overheid (en voor zover dat nog niet gebeurd is) contactformulieren beveiligd worden met een SSL-certificaat, bij voorkeur van PKI-Overheid. De CIO's van de departementen zullen er op toezien dat eventuele maatregelen worden genomen.
De afweging of de beveiliging van een website voldoende is moet periodiek door de voor de website verantwoordelijke overheidsorganisatie worden geëvalueerd, waarbij zonodig (aanvullende) maatregelen dienen te worden getroffen. De medeoverheden hebben ten aanzien van informatiebeveiliging hun eigen verantwoordelijkheid voor wat betreft de interne, ketenonafhankelijke, bedrijfsvoering.