Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2012–2013

Aanhangsel van de Handelingen

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

1419

Vragen van de leden **Gesthuizen** en **Ulenbelt** (beiden SP) aan de ministers van Veiligheid en Justitie en van Sociale Zaken en Werkgelegenheid over *de beveiliging van de website van het Uitvoeringsinstituut Werknemersverzekeringen (UWV)* (ingezonden 4 februari 2013).

Antwoord van minister **Asscher** (Sociale Zaken en Werkgelegenheid) (ontvangen 27 februari 2013).

Vraag 1
Bent u op de hoogte van de melding van een verlopen veiligheidscertificaat op de klachtenpagina van de website van het UWV?[1] Zo ja, wat is uw reactie hierop?

Antwoord 1:
UWV heeft mij laten weten dat in de periode van 21 januari 2013 tot en met 1 februari 2013 er sprake is geweest van een verouderd certificaat op klachten.uwv.nl. Op 1 februari is de fout geconstateerd en terstond verholpen. In deze periode heeft uwv.nl, waar de website voor klachtmeldingen onderdeel van is, verstoringen ervaren. UWV heeft – mijns inziens terecht – prioriteit gegeven aan het verhelpen van de verstoring. Helaas is daarbij abusievelijk het verouderde certificaat gehanteerd.

Vraag 2
Wat zijn de risico's van het ongeldige veiligheidscertificaat voor de bezoeker van klachten.uwv.nl?

Vraag 5
Zijn er reeds meldingen bekend waaruit blijkt dat door het verlopen van het veiligheidscertificaat er gegevens zijn onderschept door al dan niet kwaadwillende derde partijen? Zo ja, hoeveel bezoekers zijn hier reeds de dupe van geworden?

Antwoord 2 en 5:
Een verouderd certificaat verhoogt het risico op schending van de vertrouwelijkheid van de klacht, omdat door de bezoeker van klachten.uwv.nl lastiger is vast te stellen of er inderdaad met de webpagina van UWV wordt gecommu-

[1] klachten.uwv.nl

ah-tk-20122013-1419
ISSN 0921 - 7398
's-Gravenhage 2013

niceerd. In dit geval communiceerden klanten daadwerkelijk met de webpagina van UWV.

Om in dit specifieke geval misbruik te kunnen maken van het verouderde certificaat, zou een kwaadwillende ontdekt moeten hebben dat sprake is van een verouderd certificaat en zou die persoon op een eerder moment (op frauduleuze wijze) de beschikking gekregen moeten hebben over een kopie van het verouderde certificaat. Daarnaast zijn er op internetverkeer meer beveiligingsmaatregelen van toepassing, waar een veiligheidscertificaat er één van is. Het UWV heeft geen inbraak of misbruik kunnen vaststellen. Bovendien zijn er door UWV geen meldingen van misbruik van gegevens ontvangen.

Vraag 3
Deelt u de mening dat mensen met klachten over het UWV de mogelijkheid moeten hebben om op een veilige manier klachten te uiten? Zo ja, garandeert u op dit moment deze veiligheid?

Vraag 4
Deelt u de mening dat het UWV zijn beveiligingsbeleid serieus dient te nemen en dient te voorkomen dat gegevensuitwisseling met haar website onderschept kan worden door al dan niet kwaadwillende derde partijen?
Antwoord 3 en 4:
UWV voert een beveiligingsbeleid dat bestaat uit een uitvoerige set maatregelen die gelden voor alle systemen, ook voor de website klachten.uwv.nl. UWV controleert regelmatig de uitvoering van de maatregelen, bijvoorbeeld door het verrichten van audits en «hack-testen». Indien UWV een externe ICT-leverancier inhuurt, wordt in contracten eenzelfde beveiligingsniveau afgesproken en de naleving hiervan eveneens getoetst.
Ik deel uw mening dat veilig gegevens met UWV uitgewisseld moeten kunnen worden. UWV staat in voor deze veiligheid. Ik ben van mening dat op basis van het voorgaande, klanten de websites van UWV veilig kunnen bezoeken en in opzet een veilige gegevensuitwisseling is geborgd.