Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2011–2012

Aanhangsel van de Handelingen

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

2918

Vragen van het lid **Verhoeven** (D66) aan de minister van Economische Zaken, Landbouw en Innovatie over *het onvoldoende versleuteld opslaan van wachtwoorden* (ingezonden 8 juni 2012).

Antwoord van minister **Verhagen** (Economische Zaken, Landbouw en Innovatie) (ontvangen 3 juli 2012).

Vraag 1
Heeft u kennisgenomen van het bericht Wachtwoorden miljoenen LinkedIn-gebruikers op straat ?[1]

Antwoord 1
Ja.

Vraag 2
Hoe beoordeelt u een dergelijke inbraak? Hoe ver reikt in uw ogen de verantwoordelijkheid van LinkedIn voor het veilig opslaan van wachtwoorden en het versleutelen daarvan?

Antwoord 2
LinkedIn is primair zelf verantwoordelijk voor de beveiliging van haar dienstverlening. In de privacyverklaring op haar website geeft LinkedIn aan de ontvangen gegevens «in overeenstemming met industriële normen en technologie» te beveiligen, zonder verder te specificeren welke normen dit zijn.
Mede gezien de vraagstelling over de verantwoordelijkheid van het bedrijfsleven, verwacht ik dat mijn opvolger in het volgende kabinet nader op deze problematiek zal ingaan als onderdeel van de uitvoering van de motie Gesthuizen/Verhoeven. In deze motie is verzocht om een visie op de privacy, veiligheid en bescherming van burgers op internet[2].

Vraag 3
Bent u, gezien de dominante positie die LinkedIn heeft in haar sociale media niche zonder enige concurrentie en daarmee dus zonder enig alternatief voor de gebruiker, bereid LinkedIn aan te spreken op deze inbraak en afspraken

[1] Tweakers.net, 6 juni 2012.
[2] Tweede Kamer, vergaderjaar 2011–2012, 24 095, nr. 294.

ah-tk-20112012-2918
ISSN 0921 - 7398
's-Gravenhage 2012

met LinkedIn te maken over het veilig opslaan van de wachtwoorden van in ieder geval de Nederlandse gebruikers?

Antwoord 3
Wat de verantwoordelijkheid van de Nederlandse overheid betreft in verband met beveiligingslekken, verwijs ik naar de brief die ondergetekende en de staatssecretaris van Veiligheid en Justitie op 13 juni 2012 over deze affaire aan de voorzitter van de Tweede Kamer hebben gezonden. In deze brief wordt aangegeven dat, indien zich een beveiligingslek bij een bedrijf voordoet, deze zelf verantwoordelijk is voor de te verstrekken voorlichting en herstelactiviteiten. Dat geldt ook voor de daarmee gemoeide kosten. De overheid zal die verantwoordelijkheid niet overnemen.
In dit specifieke geval is, door de media-aandacht en het onderzoek dat de Amerikaanse overheid heeft gestart naar deze kwestie, LinkedIn afdoende gewezen op haar verantwoordelijkheden en heeft zij aangekondigd maatregelen te treffen. Een onderhoud met het bedrijf biedt in deze geen toegevoegde waarde meer.
Overigens draagt de overheid in algemene zin bij aan het vergroten van het bewustzijn bij zowel burgers als bedrijven van het veilige gebruik van internet via onder meer voorlichtingscampagnes. Via ECP, een publiek-privaat platform voor de informatiesamenleving, worden al enige jaren activiteiten ontplooid die ook ingaan op het veilig gebruik van wachtwoorden. Dit programma wordt door het Ministerie van Economische Zaken, Landbouw en Innovatie gefinancierd. Zo is in 2010 de campagne «Wissel je wachtwoord» gevoerd. Mede naar aanleiding van deze gebeurtenis zal een al in voorbereiding zijnde voorlichtingscampagne worden geactualiseerd. Gestart wordt met het ontwikkelen van een herhaling van de wachtwoordencampagne uit 2010. Verder zullen ECP en het Nationaal Cyber Security Centrum dit jaar de campagne «Secure November» uitvoeren, dat zich richt op het vergroten van de awareness in het veilig gebruik van internet.
GOVCERT.NL, nu onderdeel van het NCSC, heeft in 2011 factsheets uitgegeven met een overzicht van de risico's verbonden aan deelname aan sociale netwerken, de maatregelen die gebruikers kunnen treffen, wat de gevolgen kunnen zijn en het handelingsperspectief is wanneer persoonlijke gegevens (zoals gebruikersnaam en wachtwoord) onderdeel zijn van een datalek en op internet gepubliceerd worden.

Vraag 4
Zijn er wettelijke regels voor het veilig opslaan van wachtwoorden? Is het anders mogelijk om met enkele grote partijen een overleg te voeren hoe dit soort situaties in de toekomst voorkomen kunnen worden?

Antwoord 4
Er zijn in Nederland geen wettelijke regels die specifiek over het opslaan en beveiligen van wachtwoorden gaan. Maar er is wel wettelijk de verplichting om persoonsgegevens te beveiligen tegen verlies of vormen van misbruik. De Wet bescherming persoonsgegevens (Wbp) geeft aan:
«De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen».
Omdat LinkedIn een in Amerika gevestigd bedrijf is, daar zijn feitelijke werkzaamheden verricht en daar ook gegevens van gebruikers verwerkt, is het aannemelijk dat deze bepaling in dit specifieke geval niet van toepassing is.
Een vergelijkbare verplichting geldt voor aanbieders van openbare telecommunicatiediensten en -netwerken als gevolg van artikel 11.2 in samenhang met 11.3 Telecommunicatiewet. Overigens is LinkedIn niet aan te merken als een in deze artikelen bedoelde aanbieder.
Om deze redenen is deze kwestie voldoende aanleiding om in de eerder genoemde uitvoering van de motie Gesthuizen/Verhoeven hier op terug te komen.
Tenslotte kan ik melden dat de staatssecretaris van Veiligheid en Justitie wetgeving in voorbereiding heeft voor een meldplicht voor datalekken. Dat

wetsvoorstel zal nog voor het zomerreces aan de ministerraad worden aangeboden, en zal uw Kamer na dat reces bereiken.