Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2011–2012

32 761 Verwerking en bescherming persoonsgegevens

Nr. 30

BRIEF VAN DE STAATSSECRETARIS VAN VEILIGHEID EN JUSTITIE EN DE MINISTER VAN ECONOMISCHE ZAKEN, LANDBOUW EN INNOVATIE

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal
Den Haag, 13 juni 2012

Het lid van uw Kamer mevrouw Leijten heeft namens mevrouw Gesthuizen (beiden SP) bij de regeling van werkzaamheden van 7 juni 2012 verzocht om een brief van het kabinet over het lekken van de gegevens van 6,5 miljoen mensen die bij LinkedIn zijn aangesloten (kamerstuk 32 761, nr. 16). Daarbij is ook gevraagd of het kabinet een taak voor zichzelf ziet weggelegd bij het informeren van Nederlanders over mogelijke fraude.

Op 6 juni 2012 werd bekend dat een lijst van 6,5 miljoen versleutelde wachtwoorden is verschenen op een Russisch hackersforum. Middels een blogpost op 6 juni 2012 bevestigt LinkedIn dat een aantal van de wachtwoorden correspondeert met LinkedIn-accounts. LinkedIn heeft een aantal maatregelen getroffen om het nadeel en de schade bij de betrokken leden zoveel mogelijk te verhelpen. LinkedIn heeft de gecompromitteerde wachtwoorden ongeldig gemaakt. De betrokken leden kregen per mail bericht over de wijze waarop een nieuw wachtwoord moet worden ingesteld. De betrokken leden kregen eveneens uitleg over de context en de achtergrond van het verzoek een nieuw wachtwoord in te stellen. LinkedIn heeft op 9 juni 2012 aangegeven dat de gestolen wachtwoorden niet gepubliceerd zijn in combinatie met inlognamen. En dat bij LinkedIn niet bekend is dat er ledengegevens gepubliceerd zijn gerelateerd aan de lijst met gestolen wachtwoorden.

LinkedIn heeft aangegeven dat er inmiddels een strafrechtelijk onderzoek is gestart en het bedrijf daaraan actief meewerkt. LinkedIn is gevestigd in de Verenigde Staten. Het onderzoek wordt daarom uitgevoerd door de Amerikaanse autoriteiten.

Het is niet bekend hoeveel wachtwoorden van Nederlandse leden door het beveiligingslek zijn getroffen. Het onttrekt zich aan onze beoordeling of de beveiliging van LinkedIn voldoende in orde was en de voorgestelde maatregelen op korte en lange termijn afdoende zijn om de schade en het

kst-32761-30
ISSN 0921 - 7371
's-Gravenhage 2012

nadeel weg te nemen. Op het handelen van LinkedIn is, naar moet worden aangenomen, Amerikaans recht van toepassing. Wij doen dan ook geen uitspraken over het handelen en nalaten van LinkedIn.

Wat de verantwoordelijkheid van de Nederlandse overheid betreft in verband met beveiligingslekken, wijzen wij op de brief van 7 februari 2012 aan uw kamer waarin de eerste ondergetekende samen met de Minister van Binnenlandse Zaken en Koninkrijksrelaties die verantwoordelijkheid heeft beschreven. Zou zich een beveiligingslek voordoen bij een overheidssite en -voorziening, dan zou een voorlichtende rol van de overheid over het lek en zijn gevolgen voor de hand liggen. Doet zich een beveiligingslek voor buiten de overheid, dan is het desbetreffende bedrijf verantwoordelijk voor de te verstrekken voorlichting en herstelactiviteiten. Dat geldt ook voor de daarmee gemoeide kosten. De overheid kan die verantwoordelijkheid niet overnemen.

Dat laat onverlet dat in dit specifieke geval het National Cyber Security Centrum (NCSC) op 7 juni 2012 gewaarschuwd heeft over deze kwestie. Vervolgens is op 8 juni 2012 via de website www.ncsc.nl en via de specifiek op burgers gerichte website www.waarschuwingsdienst.nl gewaarschuwd dat cybercriminelen misbruik maken van de acties voor getroffen accounts van LinkedIn door e-mails met malware te versturen naar gebruikers.

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. Zo is in 2010 de campagne «Wissel je wachtwoord» gevoerd. Mede naar aanleiding van deze gebeurtenis zal vanuit het door ECP gefaciliteerde programma Digivaardig & Digiveilig de campagne «Bescherm jul(l)i(e)» worden opgezet. Dit programma wordt door het ministerie van Economische Zaken, Landbouw en Innovatie gefinancierd. Gestart wordt met het ontwikkelen van een herhaling van de wachtwoordencampagne uit 2010. Verder zullen ECP en het NCSC 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.

Verder kunnen slachtoffers van identiteitsfraude voor advies en hulp terecht bij het Centraal Meldpunt Identiteitsfraude en -fouten. Het meldpunt is een initiatief van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

Tenslotte herinneren wij u eraan dat de eerste ondergetekende wetgeving in voorbereiding heeft voor een meldplicht voor datalekken. Wij verwachten dit wetsvoorstel kort na het zomerreces aan uw kamer aan te kunnen bieden.

De staatssecretaris van Veiligheid en Justitie,
F. Teeven

De minister van Economische Zaken, Landbouw en Innovatie
M. J. M. Verhagen