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

1367

Vragen van het lid **Gesthuizen** (SP) aan de ministers van Economische Zaken, Landbouw en Innovatie en van Veiligheid en Justitie over *een geheime keylogger op 141 miljoen smartphones* (ingezonden 2 december 2011).

Antwoord van minister **Verhagen** (Economische Zaken, Landbouw en Innovatie) (ontvangen 31 januari 2012) Zie ook Aanhangsel Handelingen, vergaderjaar 2011–2012, nr. 1043.

Vraag 1
Klopt het bericht dat het bedrijf Carrier IQ miljoenen smartphones heeft uitgerust met geheime spyware, zoals vermeld staat in het artikel «Geheime keylogger op 141 miljoen smartphones»?[1]

Antwoord 1
Vanuit Nederland valt niet wereldwijd te onderzoeken op hoeveel smartphones software van Carrier IQ is geïnstalleerd. Carrier IQ geeft zelf aan dat het software voor mobiele apparaten zoals smartphones levert waarmee de prestaties van het apparaat worden geteld en samengevat (www.carrieriq-.com). Het bedrijf stelt dat daarbij geen toetsaanslagen worden vastgelegd noch «tracking tools» worden verschaft. Deze gegevens worden volgens Carrier IQ versleuteld verstuurd naar aanbieders of fabrikanten die klant zijn van het bedrijf, die daarmee hun dienstverlening aan de gebruiker van het apparaat willen verbeteren.

Vraag 2
Bent u ervan op de hoogte of dit bedrijf ook in Nederland gegevens verzamelt door smartphones te voorzien van software die dienst doet als keylogger, sms-berichten onderschept en sms-berichten en https-verkeer registreert? Zo ja, worden er door dit bedrijf wetten en regels overtreden? Zo nee, deelt u de mening dat een verbod voor het installeren van software die, zonder medeweten van de gebruiker, een registratie maakt van toetsaanslagen, sms-berichten en https-verkeer, wenselijk is?

Antwoord 2
Gezien de grote aantallen in gebruik zijnde smartphones, waarvan een deel buiten Nederland is gekocht en de grote vraag bij het publiek naar diverse veranderende typen en modellen smartphones, is het niet mogelijk om een

[1] http://webwereld.nl/nieuws/108720/geheime-keylogger-op-141-miljoen-smartphones.html

ah-tk-20112012-1367
ISSN 0921 - 7398
's-Gravenhage 2012

100% sluitend onderzoek naar alle in Nederland voorkomende smartphones te doen.
Vanuit het Ministerie van EL&I en vanuit de Onafhankeljke Post en Telecommunicatie Autoriteit is afzonderlijk navraag gedaan bij aanbieders in Nederland van smartphones naar het gebruik van vergelijkbare programmatuur en vergelijkbare werkwijzen. Daarnaast heeft de brancheverenigingICT~Office navraag gedaan bij zowel aanbieders als fabrikanten. Deze vraagstellingen zien dus op meer dan alleen de programmatuur van Carrier IQ. De resultaten daarvan geven aan dat voor zover deze aanbieders en fabrikanten bekend is dergelijke programmatuur niet aanwezig is op smartphones op moment van levering aan of van aankoop door de gebruiker in Nederland. Om die reden bestaat er voor mij geen aanleiding om na te gaan hoe een eventueel verbod op het installeren van de in de vraag omschreven software zich verhoudt tot de al bestaande bepalingen uit de Wet computercriminaliteit en de Wet bescherming persoonsgegevens.

Vraag 3
Is het waar dat Carrier IQ de verzamelde data niet alleen doorgeeft aan haar klanten maar deze informatie ook verkoopt aan derden? Zo ja, deelt u de mening dat dit zeer onwenselijk is omdat het een inbreuk doet op de privacy en de veiligheid van de smartphone-eigenaar?

Antwoord 3
Carrier IQ geeft zelf aan dat het geen informatie verkoopt aan derden (www.carrieriq.com).
Ik verwijs naar mijn antwoord op vraag 2. Mocht toch blijken dat dergelijke programmatuur voorkomt op in Nederland geleverde smartphones, dan ligt het op de weg van het College bescherming persoonsgegevens, de Onafhankelijke Post en Telecommunicatie Autoriteit of het Openbaar Ministerie om te beoordelen of er vanuit hun verantwoordelijkheden aanleiding is onderzoek te doen naar het verzamelen van gegevens door Carrier IQ en de eventuele doorgifte van gegevens aan derden. Ik verwijs tenslotte naar onze antwoorden op eerdere schriftelijke vragen van het lid Gesthuizen van uw Kamer (Kamerstukken II, 2010–2011, Aanhangsel handelingen, nr. 2427, antwoord 3).

Vraag 4
Hoe kijkt u aan tegen het feit dat het onmogelijk blijkt te zijn om de geheime afluisterdienst uit te zetten via een normale, door de consument te begrijpen manier? Deelt u de mening dat deze software op iedere smartphone kosteloos verwijderd dient te worden? Op welke manier kan de consument eventueel geleden schade op het bedrijf verhalen?

Antwoord 4
Gezien mijn antwoord op vraag 2 zijn deze vragen voor zover mij thans bekend voor Nederland niet aan de orde. Mocht toch blijken dat de programmatuur voorkomt op in Nederland geleverde smartphones, dan is van belang dat volgens berichtgeving op internet de handelingen die nodig zijn om de software uit te zetten niet in alle gevallen gelijk zijn.
Programmatuur dient, waar dat relevant is, door de gebruiker kosteloos verwijderbaar te zijn. Consumenten kunnen met hun klachten over een product terecht bij de verkoper van het product of bij de dienstverlener, die het product in combinatie met een dienst heeft aangeboden. Er bestaat recht op schadevergoeding indien de wederpartij toerekenbaar tekort is geschoten in de nakoming van een verbintenis en de consument door deze toerekenbare tekortkoming schade heeft geleden. De consument zal deze schade moeten kunnen aantonen. De beoordeling van deze aspecten en of schadevergoeding dient te worden toegekend is in eerste instantie aan partijen en uiteindelijk aan een geschillencommissie of aan de rechter.

Vraag 5
Bent u ervan op de hoogte of de smartphones die binnen overheidsinstanties gebruikt worden voorzien zijn van deze spyware? Kunt u garanderen dat er geen overheidsinformatie afgetapt is die de veiligheid van de Nederlandse bevolking in gevaar kan brengen? Kunt u uw antwoord toelichten?

Antwoord 5
De verschillende overheden hebben ook binnen het contract van OT2010 de mogelijkheid om zelf de soorten toestellen te kiezen die het beste bij deze organisaties passen. Hierdoor zijn vele soorten toestellen van veel merken bij de overheid in gebruik. Gezien mijn antwoord op vraag 2 zijn er momenteel geen aanwijzingen dat de veiligheid van de Nederlandse bevolking in gevaar is gebracht als gevolg van deze programmatuur. Ik acht het wel van belang om dit onderwerp via de geëigende kanalen (zoals het I-NUP-programma en het Kenniscentrum Nederlandse Gemeenten voor de gemeenten) onder de aandacht laten brengen.

Vraag 6
Is er bij u andere software bekend die via smartphones en tablets privacygevoelige gegevens bijhoudt, opslaat of anderszins verzamelt? Bestaat dergelijke software ook voor Iphone-apparatuur?

Antwoord 6
Ik verwijs naar mijn antwoord op vraag 2. Er bestaat wel programmatuur die door fabrikanten gebruikt wordt ten behoeve van storingsdiagnose, reparatie of herstel. Dit soort programmatuur bestaat overigens voor ieder type ICT apparatuur bedoeld voor het invoeren van gegevens door de gebruiker. De fabrikant dient de klant te informeren als dergelijke programmatuur is geïnstalleerd of ingezet gaat worden, waarbij de klant altijd de gelegenheid moet worden geboden dit te weigeren.