2013Z17658

Vragen van de leden Schouw en Verhoeven (beiden D66) aan de ministers van Binnenlandse Zaken en Koninkrijksrelaties, van Economische Zaken en van Veiligheid en Justitie over het bericht dat de Amerikaanse National Security Agency (NSA) via telecomaanbieders het internationaal telefoonverkeer afluistert (ingezonden 18 september 2013)

1

Heeft u kennisgenomen van het bericht dat de Amerikaanse inlichtingendienst NSA zich sinds 2011 toegang verschaft tot telefoonverkeer dat via de Belgische telecomprovider Belgacom verloopt? 1)

Ja.

2

Wat is uw reactie op het gegeven dat de Amerikaanse inlichtingendienst NSA zich toegang heeft verschaft tot een van de grootste telecombedrijven in een direct buurland?

Het bericht in De Standaard meldt onder meer dat niet zeker is wie verantwoordelijk is voor de inbreuk op de infrastructuur van het Belgische bedrijf Belgacom. Heimelijke activiteiten van statelijke actoren zijn in beginsel niet uit te sluiten.

3

Zijn er afgelopen twee jaar vergelijkbare veiligheidsinbreuken geweest op de communicatie-infrastructuur van Nederlandse telecomaanbieders? Zo ja, wat was de aard van de inbreuk, hoe vaak heeft het zich voorgedaan en was er sprake van malware geplaatst door een buitenlandse inlichtingendienst?

Er zijn geen aanwijzingen voor een vergelijkbare inbreuk op de infrastructuur van Nederlandse aanbieders van telecommunicatiediensten. De AIVD doet onderzoek naar aanleiding van de berichten. Er zijn vooralsnog geen aanwijzingen dat Nederland een direct doelwit is van de aanval.

De inbreuk bij KPN in het voorjaar van 2012 was overigens geen activiteit van een statelijke actor. KPN heeft naar aanleiding van die inbreuk aanvullende veiligheidsmaatregelen genomen.

De AIVD heeft herhaaldelijk gewezen op de kwetsbaarheden van de Nederlandse ICT-infrastructuur en de dreiging van digitale spionage. De afhankelijkheid van de Nederlandse samenleving en de economie van ICT is aanzienlijk, en de kwetsbaarheid van de ICT is hoog. Digitale aanvallen worden daarnaast steeds complexer en geavanceerder. De impact van digitale aanvallen op de nationale veiligheid en het economisch welzijn van de samenleving kan bijzonder groot zijn.

4

Is u bekend of Nederlandse telecomaanbieders afgelopen drie jaar een veiligheidsonderzoek hebben laten uitvoeren naar zeer geavanceerde malware op hun communicatie-infrastructuur? Zo ja, wat is daarvan de uitkomst? Zo nee, bent u in het licht van de Amerikaanse praktijken en mogelijke hacks door andere landen, voornemens om bij telecomaanbieders aan te dringen op een dergelijk onderzoek?

Private partijen, waaronder aanbieders van openbare elektronische communicatiediensten, zijn zelf verantwoordelijk voor de veiligheid van hun infrastructuur. De Telecommunicatiewet (Tw) bevat voor deze aanbieders verplichtingen voor de borging van de integriteit en de veiligheid van hun netwerken en diensten, waaronder het waarborgen van de vertrouwelijkheid van de telecommunicatie en de beschikbaarheid van de dienstverlening. Het gaat daarbij om technische en organisatorische maatregelen. De grote aanbieders zetten hiervoor structureel eigen capaciteit in. Indien zij dat nodig achten, zetten zij hiervoor expertise van derden in. De recente berichten in de media onderstrepen het belang van deze maatregelen. Indier aanleiding voor is, kan de aanbieder worden verplicht bepaalde technische of organis

maatregelen te nemen of een veiligheidscontrole door een onafhankelijke deskundige te laten uitvoeren (art. 11a vijfde resp. zesde lid van de Telecommunicatiewet).

Naar aanleiding van de berichtgeving is KPN gestart met het uitvoeren van aanvullende onderzoeken.

De AIVD en het NCSC ondersteunen de vitale sectoren bij het beveiligen van hun ICT-infrastructuur. De AIVD heeft onder meer een methodiek ontwikkeld voor de analyse van kwetsbaarheden voor spionage. Digitale spionage is daarbij één van de aandachtspunten. Deze methodiek is bij de vitale sectoren onder de aandacht gebracht om hen te ondersteunen de eigen kwetsbaarheden inzichtelijk te maken.

5

Heeft u of Nederlandse telecomaanbieders afgelopen jaren verzoeken ontvangen van de Amerikaanse inlichtingendienst NSA dan wel andere buitenlandse inlichtingendiensten, om toegang te verschaffen tot internationaal telefoonverkeer? Zo ja, wat was daarop de reactie?

Het is de regering niet bekend of buitenlandse mogendheden Nederlandse aanbieders van telecommunicatie hebben benaderd. Over contacten tussen de Nederlandse inlichtingen- en veiligheidsdiensten en buitenlandse diensten worden in het openbaar geen mededelingen gedaan.

6

Heeft u de hacks op Europese, en Nederlandse communicatiesystemen in het bijzonder, aan de orde gesteld bij de Amerikaanse regering? Zo ja, was de uitkomst van die gesprekken? Zo nee, bent u voornemens de privacyschending van Nederlandse burgers aan de orde te stellen bij de Amerikaanse regering?

7

Bent u bereid de inbreuken door de VS en mogelijk ook andere landen, actief te agenderen in de eerstvolgende Raad van Justitie en Binnenlandse Zaken (JBZ-Raad) en te pleiten voor gezamenlijk Europees optreden tegen deze schendingen van privacy van Europese burgers?

6 & 7: De Eurocommissarissen van Justitie en van Binnenlandse Zaken hebben naar aanleiding van mediaberichten op 14 juni jl. overleg gevoerd met de Amerikaanse minister van Justitie. Inmiddels buigt een EU-VS expertgroep zich over de bescherming van de persoonlijke levenssfeer en van elektronische gegevens van burgers, met als doel wederzijds inzicht in elkaars programma's en de wijze waarop deze zijn verankerd in de rechtsstaat. De Nederlandse regering steunt dit initiatief. Naar verwachting voltooit de expertgroep dit najaar zijn eindrapport. Het onderwerp PRISM is besproken en marge van de JBZ-raad van 7 oktober jl.

1) http://www.standaard.be/cnt/dmf20130915_00743233