

## 2015Z14424

Vragen van het lid **Oosenbrug** (PvdA) aan de ministers van Buitenlandse Zaken en voor Wonen en Rijksdienst over *het kapen van IP-adressen van het Ministerie van Buitenlandse Zaken* (ingezonden 28 juli 2015).

Vraag 1

Heeft u kennisgenomen van het bericht «IP-adressen ministerie gekaapt door Bulgaren»?<sup>1</sup>

Vraag 2

Deelt u de mening dat het bij digitale communicatie met de overheid van zeer groot belang is dat vertrouwd kan worden op de integriteit van de netwerken van de overheid?

Vraag 3

Is onderzocht op welke wijze de criminelen de controle over de bewuste IP-adressen hebben kunnen overnemen, hoe lang deze situatie geduurd heeft en op welke wijze die adressen in de bewuste periode misbruikt zijn? Zo ja, wat is daarvan de uitkomst? Zo nee, waarom is dit niet diepgaander onderzocht?

Vraag 4

Op welke basis kunt u met zekerheid zeggen dat de gekaapte adressen niet misbruikt zijn? Weet u bijvoorbeeld zeker dat er geen verkeer naar deze adressen is omgeleid, waarbij mensen dachten met de Nederlandse overheid te communiceren en mogelijk informatie is gedeeld?

Vraag 5

Wat zijn de mogelijke vormen van misbruik die voor kunnen komen bij een inbreuk als deze?

Vraag 6

Klopt het dat de inbreuk ontdekt is naar aanleiding van een melding door Spamhaus? Zo ja, welke activiteit hebben zij vanaf de gekaapte IP-adressen waargenomen?

<sup>1</sup> Volkskrant, 25 juli 2015

Vraag 7

Op welke wijze wordt de integriteit van de netwerken van de overheid gecontroleerd en gewaarborgd? Welke wijzigingen zijn daarin gemaakt naar aanleiding van deze inbreuk op de beveiliging?

Vraag 8

Hoe zorgt u ervoor dat bij de beveiliging van overheidsnetwerken de best beschikbare technieken toegepast worden. Deelt u de conclusie dat daar in dit geval geen sprake van geweest is? Zo nee, waarom niet? Zo ja, tot welke maatregelen heeft deze conclusie geleid?

Vraag 9

Is het beheer van de internet-infrastructuur van de rijksoverheid verspreid over de verschillende ministeries en meerdere internetbedrijven? Zo ja, leidt deze versnippering in uw ogen tot sub-optimale kennis en maatregelen? Zo nee, hoe is het beheer dan geregeld?

Vraag 10

Hoe wordt in de beveiliging van de informatiesystemen gebruik gemaakt van de gezamenlijke kennis die binnen de rijksoverheid en het Nationaal Cyber Security Centrum (NCSC) aanwezig is? Ziet u hierin mogelijkheden voor standaardisering en verbetering?