Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2014–2015

Aanhangsel van de Handelingen

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

3181

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).

Antwoord van Minister **Koenders** (Buitenlandse Zaken), mede namens de Minister voor Wonen en Rijksdienst (ontvangen 27 augustus 2015)

Vraag 1 en 2
Heeft u kennisgenomen van het bericht «IP-adressen ministerie gekaapt door Bulgaren»?[1]
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?

Antwoord 1 en 2
Ja.

Vraag 3 en 4
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?
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?

Antwoord 3 en 4
Onderzoek heeft uitgewezen, dat een set IP-adressen van BZ door onbekenden tijdelijk is «gekaapt». Daarbij is gebruik gemaakt van een methode, die BGP hijacking wordt genoemd, een vorm van adresvervalsing. Het betrof IP-adressen, die BZ op dat moment niet actief gebruikte. De kaping vond tussen 19 en 27 november 2014 plaats op het internet. Nadat op 27 november de kapingsmelding van het Nationaal Cyber Security Centrum (NCSC) is ontvangen door de interne ICT-dienstverlener van BZ is geconstateerd dat er

[1] Volkskrant, 25 juli 2015

ah-tk-20142015-3181
ISSN 0921 - 7398
's-Gravenhage 2015

geen dreiging heeft bestaan voor het interne BZ-netwerk en dat de kaping definitief voorbij was.
Het is onbekend of en in hoeverre de gekaapte IP-adressen in de bewuste periode daadwerkelijk zijn misbruikt. Het verrichten van sluitend onderzoek daarnaar is vanwege het wereldwijde karakter van het internet niet realistisch. Er is contact geweest met de in de Volkskrant genoemde bron, het bedrijf Spamhaus. Deze organisatie heeft de desbetreffende IP-adressen op de zwarte lijst gezet, omdat de IP-adressen waren geannonceerd uit een Bulgaars netwerk. Of er daadwerkelijk spam verstuurd is vanuit deze IP-adressen kan ook Spamhaus niet met zekerheid zeggen.

Vraag 5
Wat zijn de mogelijke vormen van misbruik die voor kunnen komen bij een inbreuk als deze?

Antwoord 5
Bij deze vorm van IP-hijacking worden de IP-adressen voornamelijk gebruikt voor het verzenden van spam. Daarbij worden gekaapte IP-adressen vaak tijdelijk gebruikt als afzender om opsporing te bemoeilijken.

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?

Antwoord 6
Nee. Het Nationaal Cyber Security Centrum (NCSC) heeft op 27 november 2014 de melding ontvangen uit het operationele CERT-netwerk en deze doorgezet naar de interne ICT-dienstverlener van BZ. De melding betrof een ongebruikelijke routering van de bewuste IP-adressen.
Zie verder het antwoord op vraag 4.

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?

Antwoord 7
De beheerorganisaties van de rijksoverheid en hun leveranciers monitoren hun netwerkonderdelen continu op aanvallen. Bij dit incident is geen sprake geweest van een aanval of inbreuk op netwerken van de rijksoverheid. Daarom heeft dit incident niet geleid tot wijzigingen in het beheer.

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?

Antwoord 8
De mogelijkheden en daaraan onlosmakelijk verbonden dreigingen in het digitale domein zijn continu in beweging. De middelen, ook de technische, die de rijksoverheid inzet om haar netwerken te beveiligen worden daar doorlopend op aangepast via processen van kwaliteitsbeheer op basis van rijksnormenkaders voor informatiebeveiliging. Dit is onder andere aan de orde bij aanbestedingen voor ICT-diensten, teneinde voor de rijksoverheid ICT-diensten te verwerven die op de laatste stand der techniek zijn ingericht. Er is geen relatie tussen het incident en de voor de beveiliging van rijksoverheidsnetwerken gebruikte technieken. Er zijn derhalve geen nieuwe technische maatregelen genomen.

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?

Antwoord 9
Ja, het beheer is verspreid, met dien verstande dat het aantal interne aanbieders van ICT-diensten binnen de rijksoverheid in de afgelopen jaren fors is teruggebracht.
Er is echter geen sprake van suboptimale kennis en maatregelen aangezien deze interne leveranciers hun krachten bundelen en samenwerken in interdepartementale overlegorganen. Dit bevordert tevens de standaardisering. Op de onderliggende niveaus wordt veel kennis tussen deze organisaties gedeeld via de reguliere overlegstructuren en kennisuitwisselingsinitiatieven.

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?

Antwoord 10
Zie ook het antwoord op vraag 9 voor de kennisdeling en standaardisering binnen de rijksoverheid. Het NCSC deelt op zowel bestuurlijk als operationeel niveau kennis met partners in het binnen- en buitenland.