Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2020–2021

Aanhangsel van de Handelingen

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

2380

Vragen van het lid **Buitenweg** (GroenLinks) aan de Minister van Justitie en Veiligheid over *kwetsbaarheden in de cybersecurity van scanners in de Rotterdamse haven* (ingezonden 15 februari 2021).

Antwoord van Minister **Grapperhaus** (Justitie en Veiligheid) en van Staatssecretaris **Van Huffelen** (Financiën – Toeslagen en Douane), mede namens de Staatssecretaris van Economische Zaken en Klimaat (19 april 2021). (Zie ook Aanhangsel Handelingen, vergaderjaar 2020–2021, nr. 1918).

Vraag 1
Bent u bekend met het bericht «Scanners in Rotterdamse haven broos voor Chinese spionage»?[1]

Antwoord 1
Ja.

Vraag 2
Bent u voorts bekend met het bericht «Veiligheidsdiensten slaan alarm wegens Chinese cyberdreiging»?[2]

Antwoord 2
Ja.

Vraag 3
Wat is uw appreciatie van de gezamenlijke waarschuwing van de AIVD, MIVD en de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) in het FD artikel dat digitale spionage uit China een onmiddellijke dreiging vormt voor de Nederlandse economie en dat de vitale infrastructuur regelmatig doelwit is van cyberaanvallen? Deelt u deze zorgen?

[1] NRC Handelsblad, 12 februari 2021, «Scanners in Rotterdamse haven broos voor Chinese spionage»
[2] Financieele Dagblad, 11 februari 2021, «Veiligheidsdiensten slaan alarm wegens Chinese cyberdreiging»

ah-tk-20202021-2380
ISSN 0921 - 7398
's-Gravenhage 2021

Antwoord 3
Digitale spionage is een belangrijke dreiging voor de nationale veiligheid, zoals beschreven in het Dreigingsbeeld Statelijke Actoren (DBSA)[3]. Om de weerbaarheid tegen deze dreiging te vergroten werkt de Minister van Justitie en Veiligheid samen met partners binnen en buiten de overheid aan de aanpak statelijke dreigingen[4]. Onderdeel van deze aanpak is dat zowel op nationaal als op EU-niveau maatregelen worden genomen om de weerbaarheid van de vitale infrastructuur te versterken. In het Dreigingsbeeld Statelijke Actoren en de genoemde Kamerbrief komt deze dreiging, en de maatregelen die we hier tegen nemen, uitgebreid aan bod.

Vraag 4
Klopt het dat de helft van de grote scanners in de Rotterdamse haven zijn geleverd door het Chinese bedrijf Nuctech? Zo ja, hoe verhoudt dit gegeven zich tot uw antwoord op vraag 3?

Antwoord 4
Ja, in de Rotterdamse haven zijn zeven grote ladingscanners geïnstalleerd, waaronder vier van Nuctech. Douane Nederland (hierna: de Douane) besteedt structureel – ongeacht welke leverancier scan apparatuur levert – aandacht aan de bescherming en beveiliging van gegevens. Tevens laat de Douane een externe audit uitvoeren op de scan- en detectiesystemen en daaraan gerelateerde IT-inrichting, om te verzekeren dat de scan- en detectieprocessen zo veilig mogelijk zijn ingericht. De opdracht voor dit onderzoek is in september geïnitieerd nadat de Douane signalen ontving over de Nuctech scanners en het onderzoek zal in maart starten. Het doel van het onderzoek is om inzicht te verschaffen in het niveau van de informatiebeveiliging van de scan- en detectiesystemen en daaraan gerelateerde IT-inrichting. Ook wil de Douane geïnformeerd worden over mogelijke risico's en advies over eventuele mitigerende maatregelen. Verwacht wordt dat de resultaten van het onderzoek in de zomer beschikbaar zijn. Daarnaast wordt in samenspraak met andere relevante overheidspartijen aanvullend onderzoek uitgevoerd, waarin de resultaten van deze externe audit worden meegenomen.

Vraag 5
Vindt u het wenselijk om in de vitale infrastructuur gebruik te maken van Chinese leveranciers? Zo ja, welke veiligheidswaarborgen zijn er om Chinese leveranciers te screenen?

Antwoord 5
Een open economie, een open wetenschappelijk klimaat en vrijhandel liggen sinds jaar en dag aan de basis van het Nederlandse verdienvermogen en onze sterke positie. Nederland profiteert van de kansen en mogelijkheden die dit biedt; hierdoor kan Nederland gebruik maken van hoogwaardige materialen, technologie en kennis die in het buitenland – waaronder in China – wordt ontwikkeld.
Ook voor de vitale infrastructuur is het wenselijk dat gebruik wordt gemaakt van kwalitatief hoogwaardige producten en diensten. Aangezien geen land beschikt over alle kennis en productiemiddelen om technologisch onafhankelijk te opereren, is een afhankelijkheid van buitenlandse technologie dan ook een gegeven. Naast de genoemde kansen, bestaat echter ook het risico dat met technologische toeleveringen de digitale spionage- en sabotagemogelijkheden toenemen[5].
Om de weerbaarheid tegen deze dreiging te vergroten werkt de Minister van Justitie en Veiligheid samen met partners binnen en buiten de overheid aan de aanpak statelijke dreigingen, waarover uw Kamer op 3 februari j.l. de laatste stand van zaken heeft ontvangen[6]. Bij elke casus moet worden bezien hoe risico's voor de nationale veiligheid beheersbaar kunnen worden gemaakt. Dit vergt een gedetailleerde analyse van de te beschermen belangen, de dreiging en de (huidige) weerbaarheid.

---

[3] Kamerstuk 30 821, nr. 124
[4] Kamerstuk 30 821, nr. 125
[5] Kamerstuk 30 821, nr. 124
[6] Kamerstuk 30 821, nr. 125

Met betrekking tot het door uw Kamer genoemde vraagstuk is specifiek het overheidsbeleid dat nationale veiligheidsoverwegingen worden meegewogen bij de inkoop en aanbesteding van producten en diensten relevant. Bij de aanschaf van gevoelige apparatuur zal volgens dit beleid bij aanschaf en implementatie rekening gehouden worden met zowel eventuele risico's in relatie tot de leverancier, als met het concrete gebruik van de systemen, bijvoorbeeld waar het gaat om de toegang tot systemen door derden. Dit ten aanzien van nationale veiligheidsrisico's verscherpt inkoop en aanbestedingsbeleid is eind 2018 geïmplementeerd voor de rijksoverheid.
Ter ondersteuning van dit beleid is instrumentarium ontwikkeld dat organisaties handvatten biedt bij het maken van een risicoanalyse en het nemen van mitigerende maatregelen. Behoeftestellende partijen zijn zelf verantwoordelijk voor de toepassing van dit instrumentarium en het meewegen van nationale veiligheidsrisico's. Het instrumentarium is ter beschikking gesteld binnen de rijksoverheid en medeoverheden, alsmede aan organisaties die onderdeel zijn van de vitale processen.

Vraag 6
Wordt er, in navolging van het beleid rond het 5G-netwerk, ook in andere sectoren, zoals die van beveiligingsapparatuur, gewerkt met lijsten van onbetrouwbare leveranciers? Zo ja, op welke manier wordt dit vormgegeven? Zo nee, waarom niet?

Antwoord 6
Voor de telecomsector is een structureel proces ingericht waarin samen met relevante stakeholders bekeken wordt op welke manier de telecomnetwerken ook in de toekomst weerbaar kunnen blijven tegen veranderingen in het dreigingsbeeld en technologische ontwikkelingen. De focus ligt hierbij op het doen van risicoanalyses, het inzichtelijk maken van afhankelijkheden, en het in kaart brengen waar adaptieve maatregelen mogelijk zijn. De komende periode wordt in kaart gebracht wat er nodig is om deze structurele aanpak op telecom te verbreden naar andere vitale processen.
Bij de beoordeling van risico's ten aanzien van spionage, beïnvloeding of sabotage door statelijke actoren of andere partijen bij (digitale) producten hanteert het kabinet de overwegingen die zowel bij c2000[7] als bij de veiligheid van de telecomnetwerken[8] zijn gebruikt:
1. Is de partij die de dienst of product levert afkomstig, of staat hij onder controle van een partij, uit een land met wetgeving die commerciële of particuliere partijen verplicht samen te werken met de overheid van dat land, in het bijzonder met staatsorganen die zijn belast met een inlichtingen- of militaire taak, of is de partij een staatsbedrijf?
2. Is de partij die de dienst of product levert afkomstig uit een land met een actief offensief inlichtingenprogramma gericht op Nederland en Nederlandse belangen of een land waarmee de Nederlandse relatie dusdanig gespannen is dat acties die Nederlandse belangen aantasten voorstelbaar zijn?

3a. Krijgt de partij die de dienst of product levert uitgebreide toegang tot gevoelige locaties, gevoelige ICT-systemen en vitale infrastructurele installaties of werken, waarbij misbruik een nationaal veiligheidsrisico kan vormen?

3b. Zijn er beheersmaatregelen mogelijk en realiseerbaar die de nationale veiligheidsrisico's die in het geding zijn voldoende beschermen?

Deze risico's worden op een zeer zorgvuldige en *case-by-case*-basis bezien.

Vraag 7
Hoe beoordeelt u de uitspraak van de directeur van de Nederlandse tak van Nuctech dat de Chinese overheid zich niet met Nuctech bemoeit? Vindt u dit geloofwaardig, ook gezien het feit dat het staatsbedrijf China National Nuclear Corporation (CNNC) een van de aandeelhouders is?

---

[7] Kamerstuk 25 124, nr. 96
[8] Staatsblad 2019, nr. 457

Antwoord 7
In algemene zin kan worden gesteld dat de Chinese overheid nauw betrokken is bij het Chinese bedrijfsleven, zowel via staatsbedrijven als private bedrijven, en dat er sprake is van nauwe verwevenheid tussen civiele en militaire sectoren in China. Dit wordt ook beschreven in de beleidsnotitie «Nederland-China: een nieuwe balans»[9]. Specifiek zien we dat het CNNC 21% aandeel heeft in de voornaamste aandeelhouder van Nuctech (Tongfang Co. Ltd., met een aandeel van 76%). Het CNCC heeft daarmee dus indirect 15,96% aan aandelen in Nuctech.

Vraag 8
Wat is uw reactie op klachten van concurrenten dat Nuctech onder de kostprijs levert dankzij Chinese staatssteun? Heeft u signalen die deze klachten ondersteunen? Hoe staat het in dit kader met het voorstel voor een*level playing field instrument* dat het Nederlandse kabinet heeft ingebracht bij de Europese Commissie? Welke mogelijkheden zijn er momenteel voor aanbestedende diensten om mogelijk ongeoorloofde staatssteun mee te nemen in de aanbestedingsprocedure?

Antwoord 8
Zoals ook aangegeven in het antwoord op vraag 7, is het niet uit te sluiten dat er (indirecte) invloed is vanuit de Chinese overheid op dit bedrijf. In bredere zin zijn er al langere tijd zorgen over bedrijven die op de interne markt concurreren met staatssteun uit derde landen. Daarom heeft de Staatssecretaris van Economische Zaken in 2019 het voorstel voor een *level playing field instrument* gedaan, voor het realiseren van een gelijk speelveld op de interne markt om in te kunnen grijpen bij verstorende effecten van subsidies van derde landen. Mede op basis hiervan heeft de Europese Commissie in de zomer van 2020 een witboek gepresenteerd over het gelijktrekken van het speelveld op de interne markt in relatie tot overheidssubsidies uit derde landen. Zie in dit verband ook de kabinetsreactie op het Commissievoorstel COM (2020 253 – Witboek over buitenlandse subsidies op de interne markt)[10]. Een concreet wetgevend voorstel wordt verwacht in het tweede kwartaal van 2021.
De Europese aanbestedingsrichtlijnen bieden aanbestedende diensten mogelijkheden voor omgang met inschrijvingen met een abnormaal lage prijs. In Nederland zijn die richtlijnen omgezet in de Aanbestedingswet 2012. Aanbestedende diensten moeten op basis van artikel 2.116 van die wet bij een inschrijving die abnormaal laag lijkt, nader onderzoek doen door de betreffende onderneming te vragen om uitleg over hoe de prijs tot stand is gekomen. Wanneer een inschrijver het lage niveau van de voorgestelde prijs niet goed kan onderbouwen met bewijsmateriaal, kan de aanbestedende dienst deze inschrijving ter zijde leggen. Abnormaal lage inschrijvingen als gevolg van niet-naleving van verplichtingen op het gebied van milieu, sociaal en arbeidsrecht moeten zelfs door de aanbestedende dienst ter zijde worden gelegd. Dit geldt voor alle inschrijvingen, ongeacht het land van herkomst van de inschrijver. Dit draagt bij aan een gelijk speelveld voor ondernemers. De Europese richtlijnen bieden aanbestedende diensten momenteel geen mogelijkheden om ongeoorloofde staatssteun uit derde landen mee te nemen in de aanbestedingsprocedure. In het witboek stelt de Commissie een mogelijke toekomstig instrument voor, dat voorziet in een meldplicht voor ondernemingen die mogelijk overheidsondersteuning uit een derde land genieten wanneer zij op de interne markt inschrijven op een aanbesteding.

Vraag 9
Deelt u de mening van de experts waar NRC mee sprak dat, ondanks de toezegging van de douane dat de scans in eigen beheer worden geëxploiteerd op een gesloten datanetwerk, de beveiliging van de Nuctech scanners toch kwetsbaar is? Zo nee, waarom niet?

[9] Kamerstuk 35 207, nr. 1
[10] Kamerstuk 22 112, nr. 2902

Antwoord 9
In algemene zin valt te zeggen, dat een maatregel zoals het afsluiten van het netwerk altijd onderdeel is van een breed pakket van beheersmaatregelen die zowel preventie, detectie als (incident) response omvatten.
Zoals bij vraag 4 is aangegeven, laat de Douane een externe audit uitvoeren op de scan- en detectiesystemen en daaraan gerelateerde IT-inrichting, om te verzekeren dat de scan- en detectieprocessen zo veilig mogelijk zijn ingericht. Het doel van het onderzoek is om inzicht te verschaffen in het niveau van de informatiebeveiliging van de scan- en detectiesystemen en daaraan gerelateerde IT-inrichting. Ook wil de Douane geïnformeerd worden over mogelijke risico's en advies over eventuele mitigerende maatregelen. Daarnaast wordt in samenspraak met andere relevante overheidspartijen een aanvullend onderzoek uitgevoerd, waarin de resultaten van deze externe audit worden meegenomen.

Vraag 10
Klopt het dat monteurs van defecte scanners in principe een mobiele dataverbinding met het hoofdkantoor kunnen opzetten om zo de problemen snel te verhelpen? Zo ja, bent u bereid om de deze mogelijkheden stop te zetten?

Antwoord 10
In geval van software storingen wordt bij scanners die hierover beschikken gebruik gemaakt van een remote verbinding. Dit betreft ongeveer een derde van de storingen op deze scans. Monteurs kunnen hierbij een storing met behulp van een beveiligde verbinding op afstand oplossen om de storing zo snel mogelijk te verhelpen.
Zoals ook vermeld bij de beantwoording van vraag 4 en 9, laat de Douane een externe audit uitvoeren op de scan- en detectiesystemen en daaraan gerelateerde IT-inrichting, om te verzekeren dat de scan- en detectieprocessen zo veilig mogelijk zijn ingericht. Daarnaast wordt in samenspraak met andere relevante overheidspartijen een aanvullend onderzoek uitgevoerd, waarin de resultaten van deze externe audit worden meegenomen. De remote verbinding voor onderhoud wordt in afwachting van het extern onderzoek niet stilgezet, omdat het opheffen hiervan het risico met zich meebrengt dat scanapparatuur langdurig in storing blijft staan. Als dat gebeurt kent het scanproces geen voortgang en nemen de risico's op de invoer van verdovende middelen toe.

Vraag 11
Deelt u de mening van de aangehaalde experts dat het feit dat de servers van verschillende scannerfabrikanten in één ruimte zijn gehuisvest een kwetsbaarheid met zich meebrengt? Zo ja, bent u bereid om de servers van elkaar te scheiden? Zo nee, waarom niet?

Antwoord 11
Deze mogelijke kwetsbaarheid is eerder gesignaleerd en daarom is het initiatief gestart om de beveiliging van deze servers te optimaliseren. In 2021 wordt de ruimte waarin de verschillende servers staan omgebouwd naar een computerruimte met alle bijbehorende aanvullende veiligheidsmaatregelen. Als het externe onderzoek van de Douane daartoe aanleiding geeft, zullen tevens aanvullende aanpassingen worden verricht.

Vraag 12
Hoe is het toegangsbeheer tot de scanners, zowel tot die van Nuctech als tot die van andere leveranciers, geregeld?

Antwoord 12
Monteurs hebben zelfstandig toegang tot de scanapparatuur. De monteur staat altijd geregistreerd bij de Douane bij onderhoud aan de scanners. Bij preventief (gepland) onderhoud zijn de bezoeken contractueel vastgelegd, in overleg met de Douane en de containerterminal. Als de monteur correctief (ongepland) onderhoud bij een storing moet uitvoeren, wordt er een werkvergunning bij de containerterminal aangevraagd. In beide gevallen vindt het onderhoud plaats in afstemming met medewerkers van Douane. Tevens zijn bij alle scans op de containerterminals camera's geïnstalleerd

waarmee de systeemoperator van de Douane zicht heeft op de scanapparatuur. In het geval dat de monteur in de serverruimte van het Douanekantoor Maasvlakte moet zijn, moet de monteur zich altijd melden bij de systeemoperator van Douane. Die verleent de monteur toegang aan de serverruimte.

Vraag 13
Klopt het dat een Verklaring Omtrent het Gedrag (VOG) volstaat om toegang te krijgen tot de scanners in de haven, terwijl de toegang tot gevoelige apparatuur op Schiphol een Verklaring van Geen Bezwaar (VGB) vereist? Zo ja, wat is de reden voor dit verschil?

Antwoord 13
Er zijn geen uniforme eisen aan de toegang tot apparatuur voor havens en luchthavens. Onder andere op basis van de locatie en de toepassing van apparatuur wordt aan de hand van het risico vastgesteld wat voor restricties er gelden voor fysieke toegang tot de apparatuur en wat er nodig is om informatie te beveiligen.

Vraag 14
Klopt het ook dat de aanbestedingseisen op het gebied van cybersecurity voor ict-apparatuur op de luchthavens strenger zijn dan die voor ict-apparatuur in de havens? Zo ja, wat is de reden voor dit verschil? Bent u bereid om de aanbestedingseisen voor de havens aan te scherpen?

Antwoord 14
Zoals genoemd in het antwoord op vraag 5 is het beleid van de rijksoverheid dat nationale veiligheidsoverwegingen worden meegewogen bij de inkoop en aanbesteding van producten en diensten relevant. Bij de aanschaf van gevoelige apparatuur zal volgens dit beleid bij aanschaf en implementatie rekening gehouden worden met zowel eventuele risico's in relatie tot de leverancier, als met het concrete gebruik van de systemen, bijvoorbeeld waar het gaat om de toegang tot systemen door derden. Dit geldt zowel voor de apparatuur van de rijksoverheid op havens als op luchthavens.
Voor bedrijven worden geen specifieke eisen gesteld vanuit de overheid ten aanzien van de aanbesteding voor de aanschaf van ICT-apparatuur op havens en luchthavens. Het in het antwoord op vraag 5 genoemde instrumentarium dat organisaties ondersteunt in het meewegen van nationale veiligheidsrisico's bij inkoop en aanbesteding is ter beschikking gesteld aan organisaties die onderdeel vormen van de vitale processen.

Vraag 15
Klopt het dat beveiligingsprotocollen met betrekking tot het testen van apparatuur en het valideren van updates voor apparatuur op de luchthavens verregaander zijn dan die voor apparatuur in de havens? Zo ja, wat is de reden voor dit verschil? Bent u bereid om de beveiligingsprotocollen voor apparatuur in de havens aan te scherpen?

Antwoord 15
Er is geen uniform protocol voor havens of luchthavens ten aanzien van de beveiliging van netwerk- en informatiesystemen. De inhoud van een beveiligingsprotocol hangt sterk af van de te beschermen bedrijfsprocessen en de specifieke risico's die daarbij een rol spelen. Aanscherping van een beveiligingsprotocol in de havens vraagt om maatwerk van de bedrijven in havens zelf. De overheid controleert het proces waarmee havens en luchthavens risico's in kaart brengen en maatregelen vaststellen om mogelijke risico's te beheersen.