Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2019–2020

Vragen gesteld door de leden der Kamer

2020Z07742

Vragen van de leden **Van Dam** en **Van Helvert** (beiden CDA) aan de ministers van Justitie en Veiligheid en van Defensie over *het rapport van de Algemene Rekenkamer «Digitalisering aan de grens; Cybersecurity van het grenstoezicht door de Koninklijke Marechaussee op Schiphol»* (ingezonden 30 april 2020).

Vraag 1
Hebt u kennisgenomen van het rapport van de Algemene Rekenkamer van 20 april 2020 «Digitalisering aan de grens; Cybersecurity van het grenstoezicht door de Koninklijke Marechaussee op Schiphol»?[1]

Vraag 2
Kunt u een korte schets geven van de drie IT-systemen die onderwerp van onderzoek van de Algemene Rekenkamer waren? Kunt u daarbij aangeven met wat voor soort informatie, op welke wijze en door wie deze IT-systemen gevoed worden, maar ook wat voor soort informatie en ten behoeve van wie deze IT-systemen data opleveren? Wilt u bij de beantwoording van deze vraag ook duiden onder welk privacyregime (Algemene verordening gegevensbescherming (AVG) of Wet politiegegevens (Wpg)) deze gegevens verwerkt worden?

Vraag 3
Kunt u aangeven wie eigenaar is van de data die worden verzameld via de IT-systemen die gebruikt worden voor grenstoezicht? Is dat in het geval van het selfservicesysteem de eigenaar, te weten Schiphol N.V.? Wat is in dat verband de reden dat het eigenaarschap van het selfservicesysteem wordt overgedragen aan Schiphol N.V.?

Vraag 4
Acht u het wenselijk dat er geen wettelijke beperkingen gelden voor het overdragen van IT-eigenaarschap bij vitale overheidstaken, zoals grenstoezicht, aan partijen met commerciële belangen?

[1] Algemene Rekenkamer, 20 april 2020, «Digitalisering aan de grens», https://www.rekenkamer.nl/publicaties/rapporten/2020/04/20/digitalisering-aan-de-grens

Vraag 5
Op welke wijze is het proces van implementatie van het nieuwe selfservice-systeem ingericht zodat er voldoende waarborgen bestaan dat commerciële belangen niet zomaar de overhand krijgen boven de veiligheid van een dergelijk systeem?

Vraag 6
Welke gegevensverwerking is toegestaan ten aanzien van de verzamelde gegevens via het grenstoezicht? Mogen verzamelde gegevens ook privaat en/of commercieel gebruikt worden?

Vraag 7
Worden passagiersgegevens (PNR-gegevens) gebruikt voor het uitvoeren van het grenstoezicht? Mogen deze gegevens verwerkt worden door partijen met een commercieel belang in het kader van het uitvoeren van grenstoezicht?

Vraag 8
Wie ziet er toe op de goedkeuringsprocedure voor het IT-systeem voor de selfservice op Schiphol? Wat is de reden dat het Defensiebeveiligingsbeleid niet is doorlopen bij de goedkeuringsprocedure?

Vraag 9
Kunt u aangeven of van het selfservicesysteem en het IT-systeem voor de pre-assessment de veiligheid gegarandeerd kan worden nu niet de gehele goedkeuringsprocedure is doorlopen?

Vraag 10
Hoe kan het dat er tweemaal een tijdelijke goedkeuring is afgegeven voor het selfservicesysteem, waarvan de laatste in 2018 is afgegeven, waardoor er al twee jaar geen goedkeuring van het systeem is afgegeven?

Vraag 11
Welke kaders bestaan er ten aanzien van het gebruik van IT-systemen bij grenstoezicht indien deze niet (meer) zijn goedgekeurd? Hoe lang is een tijdelijke goedkeuring geldig?

Vraag 12
Waarom wordt er maar eens per drie jaar een beveiligingstest uitgevoerd op grote systemen? Acht u deze termijn wenselijk in de huidige tijd waar (cyber)beveiliging steeds wendbaarder moet worden om alle dreigingen het hoofd te bieden?

Vraag 13
Is het staand beleid dat de IT-systemen van grenstoezicht niet aangesloten zullen worden op de detectiecapaciteit van het Security Intelligence Operations Center (SIOC)?

Vraag 14
Volstaat het voor u dat het selfservicesysteem aangesloten zal worden op het Security Operations Center (SOC) van Schiphol N.V en niet op bijvoorbeeld het SIOC?

Vraag 15
Welke kwetsbaarheden ziet u in de huidige systematiek waarbij grenstoezicht niet is aangesloten op het SIOC?

Vraag 16
Kunt u inzichtelijk maken welke stappen er worden doorlopen op het moment dat gesignaleerd wordt door het Ministerie van Defensie en/of het SIOC dat er een digitale aanval op het grenstoezicht plaatsvindt?

Vraag 17
Zijn er evaluatierapporten uitgebracht door het Defensie Computer Emergency Response Team (DefCERT) ten aanzien van de cyberveiligheid van de IT-systemen voor het grenstoezicht op Schiphol? Kunt u de resultaten van gedane beveiligingstesten delen met de Kamer?

Vraag 18
Bestaat er een risicoanalyse of een cybercriminaliteitsbeeldanalyse ten aanzien van vitale ICT-systemen op en rond Schiphol, in het bijzonder daar waar het gaat om veiligheid en grenstoezicht? In welke mate wordt er aan dit onderwerp aandacht besteed in het kader van Beveiliging en Publieke Veiligheid Schiphol (BPVS)? Wat zijn in BPVS-verband de meest recente ontwikkelingen op het vlak van cyberveiligheid, inclusief de preparatie op hack- en andere cyberdreigingen?