Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2019–2020

Aanhangsel van de Handelingen

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

3130

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).

Antwoord van Minister **Bijleveld-Schouten** (Defensie), mede namens de Staatssecretaris van Justitie en Veiligheid (ontvangen 11 juni 2020). Zie ook Aanhangsel Handelingen, vergaderjaar 2019–2020, nr. 2868.

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]

Antwoord 1
Ja.

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?

Antwoord 2
De Algemene Rekenkamer heeft onderzoek gedaan naar drie systemen. Ten eerste het systeem voor pre-assessment van personen op vluchten van buiten het Schengengebied. Persoonsgegevens van de passagiers en bemanningsleden worden door luchtvaartmaatschappijen aangeleverd en in het systeem vergeleken met politieregisters en profielen. Als het systeem aangeeft dat sprake is van een positieve vergelijking, wordt deze handmatig gevalideerd. De gegevensverwerkingen van passagiers binnen dit systeem

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

ah-tk-20192020-3130
ISSN 0921 - 7398
's-Gravenhage 2020

vallen in beginsel onder de AVG. Bij een verdenking van een strafbaar feit, komen diens persoonsgegevens te vallen onder de Wpg. De gegevens uit de politieregisters vallen standaard onder de Wpg.
Ten tweede het systeem voor controle van reisdocumenten. Dit systeem wordt in de manuele balies gebruikt en daarbij worden de politieregisters geautomatiseerd geraadpleegd. Met een sensor worden uit het reisdocument van de reiziger persoonsgegevens verzameld. Naam, geboortedatum en documentnummer worden vervolgens door het systeem getoetst aan de politieregisters. Daarnaast vindt een echtheidscontrole van het reisdocument plaats, waarbij het systeem de handmatige controle door de KMar-medewerker ondersteunt door ook (bij de meeste, modernere reisdocumenten) de elektronische chip van het document te controleren. De gegevens vallen in beginsel onder de AVG, totdat een verdenking van een strafbaar feit ontstaat of wordt geconstateerd. Dan is de Wpg van toepassing. De gegevens uit de politieregisters vallen standaard onder de Wpg.
Ten derde het selfservicesysteem voor grenscontroles in de e-gates van Schiphol. Hiermee worden grenscontroles automatisch uitgevoerd in plaats van handmatig. Het systeem kan niet automatisch een negatieve beslissing nemen. Het systeem beslist positief of verwijst door naar de grenswachters van de KMar. In dit systeem is sprake van verwerking van nagenoeg dezelfde persoonsgegevens als bij de echtheidscontrole. Tevens wordt een live foto van de reiziger geverifieerd met de foto in het aangeboden paspoort. Het systeem kent een automatische koppeling met dezelfde politieregisters als de andere systemen. Ook hier is de AVG van toepassing op de verwerkingen van persoonsgegevens, met uitzondering van de gegevens uit de politieregisters en de gevallen waarin uit die registers een hit volgt.

Vraag 3, 5
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.?
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?

Antwoord 3, 5
Voor verwerkingen in het kader van de uitoefening van de publiekrechtelijke taak van de Koninklijke Marechaussee is de Minister van Defensie de *verwerkingsverantwoordelijke*, zoals bepaald in artikel 4 lid 7 AVG. Dit geldt ook voor de persoonsgegevens verwerkt in de systemen voor grenstoezicht. In de Regeling AVG Defensie (art 1.3) is de Commandant van de Koninklijke Marechaussee aangewezen als AVG-beheerder; de AVG-beheerder is het diensthoofd dat namens de Minister belast is met de zorg voor de naleving van de AVG en de wet ten aanzien van verwerkingen die gevoerd worden binnen het dienstonderdeel.
Het Ministerie van Justitie en Veiligheid is momenteel eigenaar van het selfservicesysteem. In het najaar van 2020 is besluitvorming voorzien of het eigenaarschap van de selfservicesysteem wordt overgedragen. Zoals aangegeven in de beantwoording van vragen van de leden Bosman en Yeşilgöz-Zegerius, wordt de Tweede Kamer geïnformeerd over de redenen en de voorwaarden voor de veiligheid waaronder dit gebeurt indien besloten wordt tot overdracht van het eigenaarschap aan Schiphol. Ook indien het eigenaarschap van het selfservicesysteem wordt overgedragen, blijft de verwerkingsverantwoordelijkheid van de data overigens bij de Minister van Defensie. Ook verandert een overdracht niets aan de bestaande wettelijke verantwoordelijkheden inzake de uitvoering van het grenstoezicht.

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

Antwoord 4
Zo'n 80% van de Nederlandse vitale processen is in handen van private partijen. In het algemeen geldt dat vitale aanbieders verantwoordelijk zijn voor de continuïteit en weerbaarheid van vitale processen. Daarbij hoort het verkrijgen van inzicht in dreigingen, kwetsbaarheden en risico's en het ontwikkelen en onderhouden van capaciteiten waarmee de weerbaarheid van vitale processen wordt verhoogd en geborgd.[2] Ook bij het overdragen van eigenaarschap is het de verantwoordelijkheid van de vitale aanbieder om de risico's voor de nationale veiligheid in kaart te brengen en te mitigeren. Door middel van toezicht wordt gecontroleerd of vitale aanbieders hiertoe de juiste maatregelen nemen.
Het kabinet is waakzaam op de aantasting van continuïteit van dienstverlening van vitale diensten en processen. De Minister van Justitie en Veiligheid heeft uw Kamer reeds geïnformeerd over de aanvullende maatregelen die het kabinet hiertoe neemt, zoals maatregelen ter bescherming van nationale veiligheid bij inkoop en aanbesteding en bij overnames en investeringen.[3] Daarnaast bekijkt het kabinet hoe huidige wet- en regelgeving ter bescherming van nationale veiligheidsrisico's bij private ondernemingen beter benut en aangescherpt kan worden.[4]

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?

Antwoord 6
De via het grenstoezicht verkregen persoonsgegevens worden onder de AVG slechts verwerkt ten behoeve van een deugdelijke uitvoering van het grenstoezicht. Wanneer bij grenstoezicht sprake is van een positieve vergelijking uit de politieregisters, kunnen politiegegevens onder de voorwaarden van de Wpg worden verstrekt aan de in die wet aangewezen (publiekrechtelijke) partijen. Commercieel en/of privaat gebruik van de persoonsgegevens is niet toegestaan.

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?

Antwoord 7
PNR-gegevens worden verwerkt door de Passagiersinformatie-eenheid Nederland (Pi-NL), ten behoeve van het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven en ernstige criminaliteit, op grond van de PNR-wet. De Pi-NL valt onder de verantwoordelijkheid van de Minister van Justitie en Veiligheid en is ondergebracht bij de Koninklijke Marechaussee. Pi-NL kan aan bevoegde instanties op hun verzoek PNR-gegevens verstrekken, niet aan commerciële partijen.
PNR-gegevens van luchtvaartpassagiers worden tevens gebruikt door de Douane ten behoeve van de controles in het kader van douanetoezicht op de door deze passagiers meegevoerde goederen, op grond van het Douanewetboek van de Unie en de Algemene Douanewet. De Douane valt onder de verantwoordelijkheid van het Ministerie van Financiën.

Vraag 8, 9, 10
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?
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?

---

[2] Voor meer informatie over de verantwoordelijkheden van vitale aanbieders, zie https://www.nctv.nl/documenten/publicaties/2018/02/01/factsheet-weerbare-vitale-infrastructuur
[3] Kamerstuk 30 821, nr. 72
[4] Kamerstuk 30 821, nr. 72

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?

Antwoord 8, 9, 10
Nadat twee keer een tijdelijke goedkeuring voor het selfservicesysteem is gegeven, is gekozen om in het vervolg slechts goedkeuring te geven wanneer de doorontwikkeling van de software gereed is. Dan kan een definitieve goedkeuring gegeven worden.
Deze doorontwikkeling duurt langer dan voorzien. De goedkeuringsprocedure voor het selfservicesysteem is echter reeds gestart. De ministeries van Defensie, Justitie en Veiligheid en Schiphol NV hebben gezamenlijk de te treffen maatregelen geïdentificeerd en werken momenteel aan de implementatie van deze maatregelen. Dit gebeurt conform het Defensieveiligheidsbeleid. Het streven is om alle voor goedkeuring noodzakelijke maatregelen dit jaar te implementeren. Momenteel houdt het Ministerie van Justitie en Veiligheid toezicht op het doorlopen van de goedkeuringsprocedure.
Conform de informatiebeveiligingsrichtlijnen van de rijksoverheid zijn verschillende maatregelen genomen ten behoeve van de veiligheid. Het gaat bijvoorbeeld om de fysieke beveiliging, maar ook het opzetten van een firewall. Er kunnen altijd kwetsbaarheden zijn die nog niet bekend zijn. Er worden echter continu verbeteringen doorgevoerd om de beveiliging te versterken.
Voor het systeem voor de pre-assessment, waar u ook om vraagt, is een goedkeuring voor ingebruikname 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?

Antwoord 11
Defensie hanteert voor haar systemen een goedkeuringsproces voor ingebruikname. Afhankelijk van de inschatting van de impact van eventuele gebreken, worden afspraken gemaakt over een verbetertraject. Bij een tijdelijke goedkeuring wordt een tijdstermijn afgesproken over de noodzakelijke verbeteringen waarna een terugkoppeling moet worden gegeven over de afwikkeling van deze verbeteringen. In principe wordt maximaal een jaar aan een dergelijke goedkeuring gegeven, waarna een herbeoordeling plaatsvindt.

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?

Antwoord 12
In het cyberdomein ontstaan voortdurend nieuwe kwetsbaarheden, dreigingen en aanvalsscenario's. Op basis van de inlichtingencapaciteit treft Defensie gericht beveiligingsmaatregelen. Daarnaast is het patchmanagementproces (het regelmatig doorvoeren van belangrijke softwareupdates) belangrijk voor het beperken van risico's van kwetsbaarheden in systemen. Reguliere beveiligingstesten zijn dus niet het enige middel om de weerbaarheid van de IT-systemen te waarborgen. Zoals aangegeven in de reactie op het rapport van de Algemene Rekenkamer beschikt Defensie momenteel niet over de personele capaciteit om de frequentie te verhogen. Het verhogen van de testfrequentie van alle kritieke systemen naar één keer per jaar betekent dat de huidige personele en materiële cybersecurityonderzoekscapaciteit nagenoeg moet worden verdubbeld. Omdat Defensie concurreert met andere partijen op de arbeidsmarkt bij de werving van dit specialistisch personeel is dat niet haalbaar.

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)?

Antwoord 13
Essentiële processen en systemen voor het kunnen inzetten van militaire eenheden worden aangemerkt als kritiek. In verband met veiligheidsoverwegingen kan ik hier ze niet allemaal noemen.
Nog niet alle kritieke systemen zijn aangesloten op het SOC. Bij het aansluiten van systemen op het SOC geeft Defensie voorrang aan de IT-systemen die voor de krijgsmacht de hoogste prioriteit hebben. Na een zorgvuldige risicoanalyse is voorrang gegeven aan de laag gerubriceerde infrastructuur, de defensiebrede P&O-, financiële en logistieke applicaties en de Hoog Gerubriceerde systemen. Het systeem dat wordt gebruikt bij het pre-assessment, wordt volgens planning in 2021 aangesloten.
Het baliesysteem staat niet op de lijst van kritieke systemen en is daarom voorlopig nog niet in de planning opgenomen. Voor zowel het systeem van het pre-assessment als het systeem in de balie geldt dat zij draaien op de laag gerubriceerde infrastructuur waarop reeds wordt gemonitord. Hiermee ondervangt Defensie een groot gedeelte van de risico's bij deze systemen.

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?

Antwoord 14
De ministeries van Defensie en Justitie en Veiligheid en Schiphol NV onderzoeken hoe de eis van veiligheidsmonitoring effectief ingevuld kan worden. De verwachting is dat het SOC van Schiphol NV voldoende waarborgen biedt.

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

Antwoord 15
De systemen voor pre-assessment documentcontrole in de manuele balie zijn ingebed op de netwerkstructuur van Defensie. Dit netwerk is alleen toegankelijk voor geautoriseerde medewerkers van Defensie. Dat wordt door het SOC gemonitord. Daarnaast heeft alleen geautoriseerd grensbewakingspersoneel via de netwerkstructuur toegang tot de genoemde systemen. Daarmee zijn de risico's op misbruik beperkt. Omdat de systemen zelf niet worden gemonitord, is het evenwel mogelijk dat een systeemincident niet direct gedetecteerd wordt. Daarom worden de kritieke systemen op het SOC aangesloten, waarbij wordt opgemerkt dat de schaarse aansluitcapaciteit bij het SOC initieel wordt ingezet om de belangrijkste kritieke systemen aan te sluiten.

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?

Antwoord 16
Indien het SOC (onderdeel van het Defensie Cyber Security Centrum (DCSC)) een digitale aanval signaleert, start het DCSC het incident responseproces op. Daartoe beschikt het DCSC over een incidentcoördinator die met een team van cyberspecialisten het zogenaamde triageproces uitvoert. Tijdens de triage worden de aard en oorzaak van het incident geanalyseerd en de te nemen maatregelen vastgesteld. Daarvoor beschikt het DCSC ook over forensisch onderzoekscapaciteit. In nauw overleg met de lokale commandant en de lokale IT-beheerorganisatie worden de maatregelen uitgevoerd om de schade voor de eenheid zoveel mogelijk te voorkomen dan wel te beperken. Daarbij adviseert het DCSC de beheerorganisatie op welke wijze zij herhaling van het cyberincident kunnen voorkomen. In algemene zin geldt verder dat bij een mogelijk strafbaar feit de KMar wordt geïnformeerd en bij de betrokkenheid van een statelijke actor de MIVD wordt ingelicht. Als dat vanuit veiligheidsoverwegingen mogelijk is, worden ook andere organisaties (zoals het NCSC, NATO, EU) geïnformeerd over de cyberaanval.

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?

Antwoord 17
Het DefCERT (onderdeel van het Defensie Cyber Security Centrum (DCSC)) heeft op beide KMar-systemen een cybersecurityonderzoek uitgevoerd; op het baliesysteem in 2016 in opdracht van de KMar en op het pre-assessmentsysteem in 2019 op verzoek van de Algemene Rekenkamer. De onderzoeksresultaten van het baliesysteem zijn gerubriceerd en kunnen daarom niet gedeeld worden. De resultaten van het onderzoek naar het pre-assessmentsysteem door de Algemene Rekenkamer zijn tevens gerubriceerd. De bevindingen die zijn opgelost zijn opgenomen in het ARK-rapport. Verder is het DCSC op dit moment betrokken bij het cybersecurityonderzoek van het systeem waarmee automatische grenscontroles worden uitgevoerd in opdracht van het Ministerie van Justitie en Veiligheid. Dit onderzoek is nog niet afgerond.

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?

Antwoord 18
In BPVS-verband is op structurele basis aandacht voor het thema cybersecurity. Tussen de luchtvaartpartijen op en rond Schiphol en in verschillende samenwerkingsverbanden worden op reguliere basis actuele ontwikkelingen en trends gedeeld. Hierbij wordt specifiek aandacht besteed aan actuele dreigingsbeelden en het inzichtelijk maken van risico's voor de luchtvaartsector. Ook toepasselijke nationale- en internationale cyber security wet- en regelgeving komen hier aan de orde. Gelet op de vertrouwelijkheid van de informatie kan ik inhoudelijk niet ingaan op de specifieke ontwikkelingen en concrete ondernomen acties rondom cyberveiligheid.