Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2019–2020

35 470 V Jaarverslag en slotwet Ministerie van Buitenlandse Zaken 2019

Nr. 6

LIJST VAN VRAGEN EN ANTWOORDEN

Vastgesteld 12 juni 2020

De vaste commissie voor Buitenlandse Zaken heeft een aantal vragen voorgelegd aan de Minister van Buitenlandse Zaken over het rapport *Resultaten verantwoordingsonderzoek 2019 bij het Ministerie van Buitenlandse Zaken* van de Algemene Rekenkamer (Kamerstuk 35 470 V, nr. 2).

De vragen zijn op 28 mei 2020 voorgelegd aan de Minister van Buitenlandse Zaken. Bij brief van 10 juni 2020 zijn de vragen beantwoord.

Voorzitter van de commissie,
Pia Dijkstra

Adjunct-griffier van de commissie,
Konings

kst-35470-V-6
ISSN 0921 - 7371
's-Gravenhage 2020

1 Loopt het Ministerie van Buitenlandse Zaken op dit moment informatie mis doordat er helemaal geen accreditatie is voor vijf communicatiesystemen?
Antwoord:
Nee.

2 Zijn er op dit moment voorbeelden van incidenten waarbij informatie is gelekt door de ondermaatse informatiebeveiliging? Zijn er ook reële risico's voor de persoonsgegevens van burgers die door het Ministerie van Buitenlandse Zaken opgeslagen zijn?
Antwoord:
Nee, althans niet gelieerd aan de door de Algemene Rekenkamer geconstateerde tekortkomingen. Over 2019 zijn in totaal 49 incidenten gemeld met een potentieel middel of hoog risico voor Buitenlandse Zaken. Deze hadden betrekking op systeemfalen en op menselijk handelen.
Voor de verwerking van persoonsgegevens worden Privacy Impact Analyses (PIA) uitgevoerd. Daarin worden de risico's verbonden aan de persoonsverwerking geanalyseerd en worden op basis hiervan passende organisatorische en technische maatregelen getroffen. Hiermee wordt de kans dat het risico zich voordoet en de impact van het risico geminimaliseerd.

3 Hoeveel cybercriminelen hebben zich in de laatste jaren gestort op vertrouwelijke informatie van het departement?
Antwoord:
Het exacte aantal is niet bekend. Daarnaast kan specifieke informatie hierover logischerwijs niet gegeven worden om geen onnodige inzage te geven in de detectie- en monitoringsactiviteiten van het ministerie. Voor een goed beeld kan wel verwezen worden naar het rapport «Cybersecuritybeeld 2019» van de Nationaal Coördinator Terrorismebestrijding en Veiligheid.

4 Zijn er aanwijzingen dat de IT-systemen van het Ministerie van Buitenlandse Zaken vatbaar zijn (geweest) voor cyberaanvallen, of dat er sprake is geweest van data-diefstal?
Antwoord:
In het algemeen kennen de informatiesystemen geregeld kwetsbaarheden waarop indien nodig direct maatregelen getroffen worden. Als voorbeeld kan Citrix genoemd worden, waarbij het ministerie de eerste was om dit systeem uit voorzorg uit te schakelen. Er zijn geen gevallen bekend van data-diefstal. In dit verband kan tevens worden verwezen naar de jaarverslagen van Algemene Inlichtingen- en Veiligheidsdienst en de Militaire Inlichtingen- en Veiligheidsdienst, waaruit de verhoogde interesse en toegenomen cyberaanvallen blijken.

5 Hebben zich al incidenten voorgedaan zoals sabotage, verstoring, diefstal en lekken van staatsgeheime, bedrijfsvertrouwelijke en privacygevoelige informatie, die te wijten zijn aan de gebrekkige informatiebeveiliging op het Ministerie van Buitenlandse Zaken?
Antwoord:
Nee, althans niet gelieerd aan de door de Algemene Rekenkamer geconstateerde tekortkomingen. Over 2019 zijn in totaal 49 incidenten gemeld met een potentieel middel of hoog risico voor Buitenlandse Zaken. Deze hadden betrekking op systeemfalen en op menselijk handelen.
Voor de verwerking van persoonsgegevens worden Privacy Impact Analyses (PIA) uitgevoerd. Daarin worden de risico's verbonden aan de persoonsverwerking geanalyseerd en worden op basis hiervan passende organisatorische en technische maatregelen getroffen. Hiermee wordt de kans dat het risico zich voordoet en de impact van het risico geminimaliseerd.

6 De Algemene Rekenkamer schrijft dat er «tegenstrijdigheden in de beschrijving van verantwoordelijkheden rond de informatiebeveiliging» zijn; zijn deze beschrijvingen inmiddels aangepast?
Antwoord:
De bevindingen van de Algemene Rekenkamer zijn opgenomen in een project dat is opgestart om alle bevindingen structureel op te lossen. Doelstelling van dit project is om de beoogde aanpassing van beleid, procedures en verantwoordelijkheden zoveel mogelijk eind 2020 te realiseren. De geconstateerde tegenstrijdigheden in de beschrijvingen maken hier onderdeel van uit.

7 Bent u het eens met de kritiek van de Algemene Rekenkamer over het «ontbreken van aansturing en steun van het senior management voor de doelen van informatiebeveiliging»? Welke stappen zijn er, behalve het aanstellen van een *Chief Information Officer*, gezet om hier iets aan te doen?
Antwoord:
Het ministerie erkent dat de voortgang zoals die inmiddels is geboekt nog onvoldoende is. Dat doet niets af aan het belang dat het ministerie hecht aan informatiebeveiliging. Om de voortgang te versnellen wordt sturing versterkt en extra capaciteit ingezet. Zo is een stuurgroep ingesteld, die maandelijks de voortgang bewaakt en aan de plv. Secretaris-Generaal rapporteert. De Minister wordt elke drie maanden geïnformeerd over de vorderingen.

8 Kunt u duidelijkheid verschaffen wie verantwoordelijk is voor de verschillende ketens van informatiesystemen die departementoverstijgend zijn?
Antwoord:
Verantwoordelijkheid voor een keten is afhankelijk van welke keten het betreft. Het is het mij niet duidelijk naar welke ketens de Algemene Rekenkamer verwijst in haar rapport.

9 Is het Ministerie van Buitenlandse Zaken de zwakste schakel in het informatiebeveiligingssysteem?
Antwoord:
Ik kan alleen een uitspraak doen over de eigen informatiebeveiliging van het ministerie.

10 Is de informatiebeveiliging bij het Ministerie van Buitenlandse Zaken voldoende op orde?
Antwoord:
Het ministerie heeft de afgelopen jaren veel geïnvesteerd in de opbouw van een informatie beveiligingsorganisatie (Security Centre en Chief Information and Security Officer), het verbeteren van de feitelijke weerbaarheid, bewustwording van medewerkers en het onafhankelijk toezicht op informatiebeveiliging. De Algemene Rekenkamer merkt echter terecht op dat er weliswaar stappen zijn gezet om de aanbevelingen over het jaar 2018 op te volgen, maar dat een en ander nog niet is afgerond. De aanbevelingen die de Algemene Rekenkamer thans doet voor verbetering van de informatiebeveiliging onderschrijf ik. Deze hebben ertoe geleid dat het reeds gestarte project inmiddels een uitgewerkt plan van aanpak heeft opgeleverd met daarin duidelijke mijlpalen om de beoogde resultaten zoveel mogelijk eind 2020 te realiseren.

11 Wanneer gaat het Ministerie van Buitenlandse Zaken een risicomanagementproces implementeren?
Antwoord:
Na afronding van het onderzoek van de Algemene Rekenkamer, dat plaatsvond in de periode oktober 2019 – januari 2020, is de risicomanagementprocedure voor informatiesystemen verder uitgewerkt en vastgesteld door het senior management van het ministerie. Deze procedure wordt op dit moment geïmplementeerd.

12 Wanneer wordt het incidentmanagementproces geïmplementeerd?
Antwoord:
Het incidentmanagementproces is reeds opgesteld en wordt momenteel met de intern betrokkenen afgestemd. De vaststelling door het senior management is voorzien in juni 2020, waarna implementatie plaats zal vinden.

13 Is er sprake geweest van compromitteren, verlies of diefstal van data, dan wel inbreuk op systemen, als gevolg van de gebrekkige beveiliging en inrichting van de informatiebeveiliging?
Antwoord:
Nee, althans niet gelieerd aan de door de Algemene Rekenkamer geconstateerde tekortkomingen. Over 2019 zijn in totaal 49 incidenten gemeld met een potentieel middel of hoog risico voor Buitenlandse Zaken. Deze hadden betrekking op systeemfalen en op menselijk handelen.
Voor de verwerking van persoonsgegevens worden Privacy Impact Analyses (PIA) uitgevoerd. Daarin worden de risico's verbonden aan de persoonsverwerking geanalyseerd en worden op basis hiervan passende organisatorische en technische maatregelen getroffen. Hiermee wordt de kans dat het risico zich voordoet en de impact van het risico geminimaliseerd.

14 Kunt u aangeven welke functie de vijf van de elf systemen die helemaal niet beschikken over een geldige accreditatie vervullen? Kunt u daarbij aangeven wanneer u verwacht dat deze systemen wél over een geldige accreditatie beschikken?
Antwoord:
De functie van de systemen zoals vermeld in het rapport van de Algemene Rekenkamer betreft interne systemen van het ministerie die betrekking hebben op de digitale werkomgeving. Voor 2020 is voorzien om voor drie systemen een FATO[1] te verkrijgen. FATO's voor de overige systemen zijn voorzien in 2021. In de tussentijd zal het ministerie voor deze systemen met IATO's (interim- Approval To Operate) blijven werken. De voortgang van de nog uit te voeren werkzaamheden om tot een FATO te komen, zal worden gemonitord.

15 Hoe apprecieert u de kwalificatie dat de informatiebeveiliging bij het Ministerie van Buitenlandse Zaken als een ernstige onvolkomenheid wordt beschouwd?
Antwoord:
Het ministerie heeft de afgelopen periode veel geïnvesteerd in informatiebeveiliging. Er is ook voortgang. Tegelijk erken ik dat de voortgang in het wegwerken van de tekortkomingen nog onvoldoende is. Er wordt nu extra sturing en capaciteit ingezet om de onvolkomenheid op te lossen. Deze werkzaamheden zijn echter nog niet afgerond.

16 Is er sprake van (geweest) dat Nederland EU- en NAVO-informatie niet meer digitaal ontvangt vanwege achterlopende accreditaties?
Antwoord:
Nee.

17 Is het daadwerkelijk een werkbare optie om terug te stappen naar papieren communicatie, de «traditionele manier van communiceren» met de NAVO en EU bij gebrek aan accreditaties in de digitale systemen? Kan gegarandeerd worden dat indien teruggevallen moet worden op de «traditionele manier van communiceren», Nederland niet verstoken blijft van enig NAVO of EU-document/communicatie?
Antwoord:
Het terug gaan naar papieren communicatie dient te worden gezien als een uiterste uitwijkmogelijkheid en zeker niet als een wenselijke situatie. Temeer daar de digitale informatievoorziening de grootste garantie biedt dat Nederland tijdig en volledig informatie ontvangt. Het ministerie hoeft momenteel van deze terugval optie geen gebruik te maken, aangezien drie belangrijke systemen die EU en NAVO gebruiken om met het ministerie te communiceren een accreditatie hebben en een systeem zich in de afrondende fase van een accreditatie bevindt. Daarnaast zijn tijdens de inspecties door de EU en NAVO in 2019 geen grote tekortkomingen geconstateerd. Het ministerie wacht echter nog op de formele rapportages.

18 Zijn er als gevolg van het ontbreken van accreditaties al gevolgen geweest voor de communicatie met de NAVO en de EU, zoals het verzenden of ontvangen van stukken en documenten? Zo ja, welke en in welke mate?
Antwoord:
Nee, het proces van verlengen van accreditaties heeft geen gevolgen gehad. Het ministerie ontvangt alle informatie van de EU en NAVO.

19 Heeft u de EU- en NAVO-bondgenoten geïnformeerd over de problemen bij de accreditatiesystemen?
Antwoord:
De EU- en NAVO zijn beide bij de recente inspecties in het najaar van 2019 geïnformeerd over de status van de lopende accreditaties.
Het terug gaan naar papieren communicatie dient te worden gezien als een uiterste uitwijkmogelijkheid en zeker niet als een wenselijke situatie. Temeer daar de digitale informatievoorziening de grootste garantie biedt dat Nederland tijdig en volledig informatie ontvangt. Het ministerie hoeft momenteel van deze terugval optie geen gebruik te maken, aangezien drie belangrijke systemen die EU en NAVO gebruiken om met het ministerie te communiceren een accreditatie hebben en een systeem zich in de afrondende fase van een accreditatie bevindt. Daarnaast zijn tijdens de inspecties door de EU en NAVO in 2019 geen grote tekortkomingen geconstateerd. Het ministerie wacht echter nog op de formele rapportages

20 Hebben bondgenoten u aangesproken op deze ernstige onvolkomenheid in de accreditatiesystemen?
Antwoord:
Nee.

21 Wanneer verwacht u de problemen met de accreditaties opgelost te hebben?
Antwoord:
Conform het huidige plan van aanpak zullen eind 2020 zeven systemen een accreditatie hebben (FATO of SOC voor drie jaar) en wordt voor de vier resterende systemen in 2021 een accreditatie afgerond.

22 Welke verklaring heeft u dat ondanks de herhaaldelijke waarschuwingen vanuit de Algemene Rekenkamer het probleem met de accreditaties niet is opgelost?
Antwoord:
Het afgelopen jaar hebben de opbouw van de informatie beveiligingsorganisatie, de voorbereidingen voor de EU- en NAVO-inspecties, alsmede de feitelijke weerbaarheid tegen cyberaanvallen veel gevergd van de beschikbare capaciteit. Ook is het verkrijgen van de vereiste bewijsstukken en de interne en externe toetsing ten behoeve van een accreditatie in toenemende mate een intensief proces, waarbij het ministerie afhankelijk is van verschillende partijen. Verder heeft de verhuizing in 2017 van het ministerie en de systemen voor een vertraging gezorgd in het afronden van de desbetreffende accreditaties.

23 Welke verklaring heeft u dat de Kamer te positief gekleurde informatie heeft gekregen over de stand van zaken met betrekking tot de accreditaties?
Antwoord:
De Tweede Kamer is geïnformeerd over de situatie tot oktober 2019. Toen had één systeem een accreditatie, was voor vier systemen een IATO verkregen en werd aangegeven dat voor zes systemen aan afronding werd gewerkt. Intussen hebben twee systemen daarvan een accreditatie (FATO of een vergelijkbaar driejarig SOC), bevindt een systeem zich in de afrondende fase van accreditatie (driejarig SOC) en wordt voor drie systemen een IATO verkregen.

24 Klopt het dat juist bij het Ministerie van Buitenlandse Zaken meer inzicht in het belang van goede informatiebeveiliging nodig is gelet op de dreiging van onder meer statelijke actoren?
Antwoord:
Ja.

25 Hoe verklaart u het gebrek aan inzicht in het belang van goede informatiebeveiliging bij uw ministerie?
Antwoord:
Het ministerie hecht al jaren groot belang aan een goede informatiebeveiliging. De wereld van cyber security is in het afgelopen decennium sterk veranderd en de dreigingen zijn toegenomen. Dit heeft ook geleid tot een forse uitbreiding van de personele capaciteit op dit gebied. Daarbij heeft het ministerie zich de afgelopen jaren vooral gericht op de feitelijke technische weerbaarheid, bewustwording van medewerkers en nog onvoldoende op het risicomanagement en accreditaties.

26 Hoe vaak is het reeds voorgekomen dat Nederland informatie van de EU, NAVO of individuele bondgenoten/lidstaten digitaal niet (of met vertraging) heeft ontvangen omdat de informatiebeveiliging niet op orde was?
Antwoord:
Dit is niet voorgekomen.

27 Kan worden aangegeven wat exact wordt bedoeld met de «traditionele wijze» van communicatie? Welke risico's en beperkingen kleven er aan deze «traditionele wijze» van communiceren ten opzichte van een goed beveiligde digitale communicatie die men zou mogen verwachten?
Antwoord:
Met de traditionele manier wordt bedoeld dat informatie en stukken via de papieren procedure gedeeld worden. De risico's en beperkingen hangen dan ook samen met deze manier, zoals snelheid, snelheid van verspreiding, registratie en verlies van stukken.

28 Voor welke diensten ondervindt het ministerie de meeste hinder van de problemen in de IT-systemen?
Antwoord:
Er zijn geen bekende specifieke problemen in de IT-systemen zelf. Indien er problemen of storingen optreden is het geheel afhankelijk van de aard van het probleem en bijvoorbeeld de aanwezigheid van uitwijkmogelijkheden en alternatieve oplossingen in welke mate het ministerie hiervan hinder ondervindt. Diensten die in hoge mate afhankelijk zijn van IT-systemen zijn: Communicatie, consulaire diensten en interne diensten op het vlak van financiën, personeel, samenwerking en archivering.

29 Is nu duidelijk welk overheidsorgaan verantwoordelijk is voor de beveiliging en werking van interdepartementaal digitaal verkeer? Zo ja, welke?
Antwoord:
Wat betreft het interdepartementale e-mailverkeer (de zogeheten Haagse Ring) is het Ministerie van Binnenlandse Zaken in Koninkrijksrelaties verantwoordelijk voor de werking en de beveiliging.

30 Kunt u verzekeren dat privacygevoelige informatie veilig is bij uw ministerie?

Antwoord:

Ik neem de passende maatregelen die hiervoor nodig zijn. Het ministerie heeft een formele toezichthouder (de FG) die hierop toeziet. Ook is in lijn met de Algemene Verordening Gegevensbescherming een PDCA-cyclus («plan, do, check, act») ingericht, waarbij tevens periodiek wordt gecontroleerd. Mede op basis van deze controles worden – waar nodig – de maatregelen verder aangescherpt.

Voorbeeld hiervan is dat voor de verwerking van persoonsgegevens wordt voorzien in de uitvoering van een Privacy Impact Analyses (PIA). Daarin worden de risico's verbonden aan de persoonsverwerking geanalyseerd en worden op basis hiervan passende organisatorische en technische maatregelen getroffen. Hiermee wordt de kans dat het risico zich voordoet en de impact van het risico geminimaliseerd.

31 Heeft het «recente Citrix incident» directe en specifieke betrekking gehad op het Ministerie van Buitenlandse Zaken? Zo ja, wat voor en in welke mate?

Antwoord:

Ja.

De impact voor het ministerie was zeer beperkt, omdat met het werkplekconcept van het ministerie overal ter wereld mobiel gewerkt kan worden zonder Citrix-verbinding. De Citrix-verbinding is voor de medewerkers van het ministerie voornamelijk een terugvaloptie.

Het ministerie heeft op basis van kwetsbaarheden in Citrix in januari 2020, vooruitlopend op het Rijksbrede advies van het Nationaal Cyber Security Centrum, opdracht aan de leverancier gegeven om mitigerende maatregelen te treffen. Toen latere duiding uitwees dat deze maatregelen onvoldoende weerstand boden, is het Citrix-informatiesysteem vroegtijdig uitgezet door het ministerie.

Het uitzetten van Citrix betekende wel dat enkele ketenpartners tijdelijk geen toegang hadden tot het netwerk van het ministerie en dat twee posten tijdelijk verminderde toegang hadden.

32 Erkent u dat de verantwoordelijkheid voor *lifecycle management* niet kan worden uitbesteed en dat u daarvoor verantwoordelijk bent en blijft?

Antwoord:

Ja. Het ministerie heeft de uitvoering van de ICT uitbesteed aan externe leveranciers, maar daarmee is niet de verantwoordelijkheid voor het bieden van continuïteit en het grip houden op de ICT uitbesteed. Het ministerie was, is en blijft zelf verantwoordelijk voor (het managen van) de lifecycle van ICT.

33 Wanneer verwacht u het *lifecycle-management*-proces volledig ingericht te hebben? Stelt u daar voldoende middelen ter beschikking voor?

Antwoord:

Op dit moment loopt de inventarisatie van de bouwstenen en activiteiten die nog ontbreken om tot inrichting van het volledige proces te komen. Op basis van dit onderzoek wordt een plan van aanpak opgesteld. Dit moet eind 2020 zijn afgerond. De implementatie is voorzien vanaf januari 2021 en moet zijn afgerond in de tweede helft van 2021. Dit valt samen met de voorziene herinrichting van de IV-organisatie. Mogelijke quick-wins die tijdens het onderzoek worden geïdentificeerd, zullen dit jaar nog worden gerealiseerd. Voor het onderzoek worden voldoende mensen en middelen vrijgemaakt. Mensen en middelen voor de implementatie en uitvoering worden opgenomen in het genoemde plan van aanpak.

34 Hoe wordt verklaard dat de informatievoorziening aan de Tweede Kamer over de implementatie van de plannen in het postennetwerk beperkt is? Bent u voornemens dit te verbeteren en zo ja, hoe?

De Tweede Kamer wordt jaarlijks over de vorderingen van de versterking van het postennet in de begroting en in het jaarverslag van Buitenlandse Zaken geïnformeerd. Daarnaast vormen de middelen voor de versterking van het postennet onderdeel van de totale apparaatsuitgaven op de begroting van Buitenlandse Zaken. Hierover wordt, naast de begroting en het jaarverslag, ook in de suppletoire begrotingen aan de Tweede Kamer gerapporteerd. Tot slot is de Tweede Kamer bij brief van 15 december 2019 (Kamerstuk 32 734, nr. 39) op de hoogte gesteld, alsmede in de antwoorden op de naar aanleiding van deze brief gestelde vragen (Kamerstuk 32 734, nr. 40). Met de brief van 15 december 2019 heb ik gevolg gegeven aan de aanbeveling uit het Verantwoordingsonderzoek 2018 om niet alleen te rapporteren over voorgenomen bestedingen, maar de Tweede Kamer ook achteraf op de hoogte te stellen van de vordering van de investeringen. Verder heb ik in het Jaarverslag over 2019 met een interactieve kaart per post aangeven welke resultaten met de investeringen konden worden geboekt. Ik heb met het oog op verdere rapportage aan de Tweede Kamer de Accountantsdienst Rijk (ADR) gevraagd onderzoek te doen dat inzicht moet geven in de verbeteringen die mogelijk zijn in de wijze waarop Buitenlandse Zaken de, met behulp van de intensiveringsgelden, extra behaalde resultaten van het postennet kan rapporteren.

De Algemene Rekenkamer stelt vast dat de besteding van de voor het postennet beschikbare extra middelen plaatsvindt in overeenstemming met de brieven die ik op 2 juli 2018 (Kamerstuk 32 734, nr. 31) en 8 oktober 2018 (Kamerstuk 32 734, nr. 32) aan de Tweede Kamer heb gezonden. Hoewel de Algemene Rekenkamer concludeert dat de informatievoorziening aan de Tweede Kamer beperkt is, is zij niet van oordeel dat deze gebrekkig is.

35 Hoe wordt verklaard dat de plannen voor de uitbreiding van het postennet in juist in Europa en Noord-Afrika vaak voor minder dan de helft gerealiseerd zijn?

Antwoord:

De extra middelen uit het Regeerakkoord voor het postennet lopen op van EUR 10 miljoen in 2018 tot EUR 40 miljoen structureel in 2021. De extra personele inzet op de posten vindt daarom gefaseerd plaats en is op dit moment nog gaande. In Afrika is een aantal nieuwe posten geopend. Voordat extra personeel kan worden uitgezonden, moet eerst voor voldoende veilige werkplekken worden gezorgd.

36 Hoe verklaart u de gebrekkige informatievoorziening aan de Kamer omtrent de uitbreiding van het postennet? Welke stappen neemt u om dit in te toekomst te verbeteren?

De Tweede Kamer wordt jaarlijks over de vorderingen van de versterking van het postennet in de begroting en in het jaarverslag van Buitenlandse Zaken geïnformeerd. Daarnaast vormen de middelen voor de versterking van het postennet onderdeel van de totale apparaatsuitgaven op de begroting van Buitenlandse Zaken. Hierover wordt, naast de begroting en het jaarverslag, ook in de suppletoire begrotingen aan de Tweede Kamer gerapporteerd. Tot slot is de Tweede Kamer bij brief van 15 december 2019 (Kamerstuk 32 734, nr. 39) op de hoogte gesteld, alsmede in de antwoorden op de naar aanleiding van deze brief gestelde vragen (Kamerstuk 32 734, nr. 40). Met de brief van 15 december 2019 heb ik gevolg gegeven aan de aanbeveling uit het Verantwoordingsonderzoek 2018 om niet alleen te rapporteren over voorgenomen bestedingen, maar de Tweede Kamer ook achteraf op de hoogte te stellen van de vordering van de investeringen. Verder heb ik in het Jaarverslag over 2019 met een interactieve kaart per post aangeven welke resultaten met de investeringen konden worden geboekt. Ik heb met het oog op verdere rapportage aan de Tweede Kamer de Accountantsdienst Rijk (ADR) gevraagd onderzoek te doen dat inzicht moet geven in de verbeteringen die mogelijk zijn in de wijze waarop Buitenlandse Zaken de, met behulp van de intensiveringsgelden, extra behaalde resultaten van het postennet kan rapporteren.

De Algemene Rekenkamer stelt vast dat de besteding van de voor het postennet beschikbare extra middelen plaatsvindt in overeenstemming met de brieven die ik op 2 juli 2018 (Kamerstuk 32 734, nr. 31) en 8 oktober 2018 (Kamerstuk 32 734, nr. 32) aan de Tweede Kamer heb gezonden. Hoewel de Algemene Rekenkamer concludeert dat de informatievoorziening aan de Tweede Kamer beperkt is, is zij niet van oordeel dat deze gebrekkig is.

37 Onderschrijft u de aanbevelingen van de Algemene Rekenkamer om de reisadviezen beter te maken, en bent u van plan deze door te voeren?

Antwoord:

Het ministerie is continu bezig de toegankelijkheid, betrouwbaarheid en gebruiksvriendelijkheid van de reisadviezen verder te vergroten. Ik zal het onderzoek van de Algemene Rekenkamer dan ook gebruiken als basis om de reisadviezen verder te verbeteren, zowel qua inhoud als de processen van totstandkoming en archivering ervan.

38 Onderschrijft u het advies om de kleur leidend te maken in de reisadviezen?

Antwoord:

Bij elk reisadvies wordt de veiligheidssituatie van landen met vier kleurcodes op een kaart weergegeven. Deze codes hangen samen met de tekstuele classificatie die is gebaseerd op een zorgvuldige analyse van de veiligheidsrisico's in een land. De kleurcode vormt een middel voor herkenbaarheid en presentatie, maar neemt niet het belang van de tekst weg, welke altijd leidend is. Enkel de kaart of kleurcodes leidend maken acht ik onwenselijk. De kleur geeft immers een algemeen beeld, waarbij de tekst de nuances weergeeft in de verschillende veiligheidsrisico's. Ook in de huidige situatie ten tijde van Corona is het juist de tekst die aangeeft welke veiligheidsrisico's naast het Coronavirus in acht genomen dienen te worden. Wel zie ik aanleiding in een volgend gebruikersonderzoek aandacht te besteden aan de vraag in hoeverre burgers die het reisadvies gebruiken zich in hun keuzes baseren op de kaart/ kleurcodering, dan wel op de toelichtende tekst. Op basis daarvan kan worden bezien of het format van het reisadvies verder kan worden geoptimaliseerd, zodat gebruikers zo goed mogelijk op de belangrijkste onderwerpen in de tekst wordt gewezen.

39 Gaat u onderzoeken of reisadviezen sneller aangepast kunnen worden bij een verandering van de veiligheidssituatie? Wanneer verwacht u resultaat van dit onderzoek?

Antwoord:

Bij het aanpassen van de reisadviezen gaat het om een constante afweging tussen snelheid en zorgvuldigheid. De zorgvuldigheid van de inhoud blijft echter voorop staan. Het is essentieel dat slechts op basis van voldoende gecontroleerde informatie wordt gebruikt en gepubliceerd. Dit om de betrouwbaarheid en toegevoegde waarde van de reisadviezen zoveel mogelijk te garanderen.

Er zijn maatregelen getroffen om reisadviezen sneller aan te kunnen passen, waaronder de 24 uurs inzetbaarheid van de medewerkers die reisadviezen opstellen. Hierdoor is het mogelijk dat, ingeval daar aanleiding toe bestaat, reisadviezen 24 uur per dag en 7 dagen in de week aangepast kunnen worden. Om de snelheid te verbeteren, zonder dat afbreuk wordt gedaan aan de zorgvuldigheid, wordt sinds enkele maanden ook een processtap gebruikt waarbij binnen 24 uur een waarschuwing wordt opgenomen in het reisadvies dat er een ramp of crisis heeft plaatsgevonden. Tegelijkertijd wordt zorgvuldig onderzocht wat de (mogelijke) impact van de ramp/crisis is voor de veiligheid van Nederlanders om op basis van die informatie het reisadvies zo nodig opnieuw aan te passen.

40 Wat vindt u een reële streeftijd om bij verandering van de veiligheidssituatie in een land het reisadvies aan te passen? Is langer dan 24, dan wel 48 uur, naar uw oordeel acceptabel?
Antwoord:
Het streven is de reisadviezen binnen 24 uur aan te passen in geval van een crisis of calamiteit, via de toevoeging van procesinformatie met benoeming van de (mogelijke) situatie en een handelingsperspectief («laat uw familie/vrienden weten hoe het met u gaat en heeft u hulp nodig bel het 24/7 contact center»). Dit wordt sinds enkele maanden gedaan. Tegelijkertijd wordt zorgvuldig onderzocht wat de (mogelijke) impact van de ramp/crisis is voor de veiligheid van Nederlanders om op basis van die informatie het reisadvies inhoudelijk aan te passen. Dit om te kunnen voldoen aan de gewenste snelle aanpassing, maar tegelijkertijd de zorgvuldigheid te kunnen borgen welke van de overheid verwacht mag worden.

41 U geeft aan de «beoogde resultaten» voor de informatiebeveiliging «zoveel mogelijk» in 2020 te willen realiseren. Hoeveel geldt hierbij als «zoveel mogelijk», en wanneer zal de informatiebeveiliging geheel op orde zijn? Komt er hiervoor een plan van aanpak, en kan dit met de Kamer gedeeld worden?
Antwoord:
Met het reeds opgestelde plan van aanpak streef ik ernaar om alle geconstateerde tekortkomingen op te lossen. Het grootste gedeelte hiervan wordt conform planning in 2020 gerealiseerd. Gezien de benodigde doorlooptijd is een uitloop van een aantal activiteiten in 2021 noodzakelijk. De activiteiten die in 2021 doorlopen betreffen de implementatie van een centraal systeem voor beheersing van het risicomanagementproces, alsmede de afronding van alle accreditaties, Voor vier resterende systemen zijn FATO's voorzien in de eerste helft van 2021. Over de voortgang van het project zal maandelijks aan het senior management, worden gerapporteerd. De Minister wordt elk kwartaal geïnformeerd. Gezien de aard en inhoud van het projectplan kan deze niet breed gedeeld worden. Wel kan de Tweede Kamer op verzoek inzage krijgen in realisatie en voortgang.

42 U geeft aan ten aanzien van het *lifecycle management* van de ICT dat er in 2020 een «verdere uitwerking van procesbeschrijvingen en werkwijzen» komt. Wanneer zal deze uitwerking afgerond zijn? En wanneer zal er een adequaat systeem van lifecycle managment zijn? Bent u van plan hiervoor een plan met tijdlijn op te stellen, en kan dit met de Kamer gedeeld worden?
Antwoord:
Op dit moment loopt de inventarisatie van de bouwstenen en activiteiten die nog ontbreken om tot inrichting van het volledige proces te komen. Op basis van dit onderzoek wordt een nader plan van aanpak opgesteld. Dit moet eind 2020 zijn afgerond. De implementatie is voorzien vanaf januari 2021 en moet zijn afgerond in de tweede helft van 2021. In genoemd plan van aanpak wordt tevens een planning opgenomen. Gezien de aard en inhoud van het projectplan kan deze niet breed gedeeld worden. Wel kan de Tweede Kamer op verzoek inzage krijgen in realisatie en voortgang.

43 U heeft in uw reactie op het rapport aangegeven zich meer in te gaan spannen om de Tweede Kamer meer inzicht te bieden in hoeverre het extra beschikbare budget daadwerkelijk voor de versterking van het postennet is gebruikt; hoe voorziet u dat deze inspanning eruit gaat zien?

Antwoord:

In mijn reactie op het rapport van de Algemene Rekenkamer heb ik opgemerkt dat de formatieve uitbreiding is voorzien van een specifiek label, te weten «Rutte III». Op die manier wordt getracht inzichtelijk te maken dat hiervoor een deel van de extra middelen is aangewend. De extra inspanning die ik in deze reactie heb toegezegd betreft het inzicht in de resultaten die met het postennet worden behaald. De interactieve kaart die met het jaarverslag 2019 is meegestuurd, waarin de extra resultaten die met de extra middelen zijn behaald inzichtelijk zijn gemaakt, is daarvan een voorbeeld. Daarnaast wordt vier keer per jaar, via de geijkte begrotingsmomenten, een toelichting gegeven op de ontwikkeling van de apparaatsuitgaven. De extra middelen voor het postennet vormen daarvan onderdeel.

44 Welke inspanningen moeten er geleverd worden de aanbevelingen over informatiebeveiliging voor eind 2020 te implementeren?

Antwoord:

Het ministerie erkent dat de voortgang zoals die inmiddels is geboekt nog onvoldoende is. De aanbevelingen van de Algemene Rekenkamer helpen om de informatiebeveiliging beter op orde te krijgen. Inmiddels is in extra sturing en personele capaciteit voorzien. Een plan van aanpak is opgesteld met daarin duidelijke mijlpalen om te borgen dat de tekortkomingen versneld worden verholpen. Een stuurgroep is ingesteld, die maandelijks de voortgang bewaakt en aan de plv. Secretaris-Generaal rapporteert. De Minister wordt elke drie maanden geïnformeerd over de vorderingen. Eind 2020 moet zoveel als mogelijk zijn gerealiseerd, maar ik moet ook realistisch zijn en de verwachting uitspreken dat ook in de eerste helft van 2021 nog het nodige werk moet worden verricht.

[1] Toelichting bij de verschillende accreditatietermen:
– In nationaal verband is FATO de eindfase van een accreditatie, IATO een tijdelijke accreditatie en een SOC de voorfase;
– In internationaal (EU/ NAVO) verband is SOC de eindfase van een accreditatie.