LIJST VAN VRAGEN

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 voorzitter van de commissie,
Pia Dijkstra

De adjunct-griffier van de commissie,
Konings

Nr	Vraag
1	Loopt het Ministerie van Buitenlandse Zaken op dit moment informatie mis doordat er helemaal geen accreditatie is voor vijf communicatiesystemen?
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?
3	Hoeveel cybercriminelen hebben zich in de laatste jaren gestort op vertrouwelijke informatie van het departement?
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?
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?
6	De Algemene Rekenkamer schrijft dat er «tegenstrijdigheden in de beschrijving van verantwoordelijkheden rond de informatiebeveiliging» zijn; zijn deze beschrijvingen inmiddels aangepast?
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?
8	Kunt u duidelijkheid verschaffen wie verantwoordelijk is voor de verschillende ketens van informatiesystemen die departementoverstijgend zijn?
9	Is het Ministerie van Buitenlandse Zaken de zwakste schakel in het informatiebeveiligingssysteem?
10	Is de informatiebeveiliging bij het Ministerie van Buitenlandse Zaken voldoende op orde?
11	Wanneer gaat het Ministerie van Buitenlandse Zaken een risicomanagementproces implementeren?
12	Wanneer wordt het incidentmanagementproces geïmplementeerd?
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?
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?
15	Hoe apprecieert u de kwalificatie dat de informatiebeveiliging bij het Ministerie van Buitenlandse Zaken als een ernstige onvolkomenheid wordt beschouwd?
16	Is er sprake van (geweest) dat Nederland EU- en NAVO-informatie niet meer digitaal ontvangt vanwege achterlopende accreditaties?
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?
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?

19 Heeft u de EU- en NAVO-bondgenoten geïnformeerd over de problemen bij de accreditatiesystemen?
20 Hebben bondgenoten u aangesproken op deze ernstige onvolkomenheid in de accreditatiesystemen?
21 Wanneer verwacht u de problemen met de accreditaties opgelost te hebben?
22 Welke verklaring heeft u dat ondanks de herhaaldelijke waarschuwingen vanuit de Algemene Rekenkamer het probleem met de accreditaties niet is opgelost?
23 Welke verklaring heeft u dat de Kamer te positief gekleurde informatie heeft gekregen over de stand van zaken met betrekking tot de accreditaties?
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?
25 Hoe verklaart u het gebrek aan inzicht in het belang van goede informatiebeveiliging bij uw ministerie?
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?
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?
28 Voor welke diensten ondervindt het ministerie de meeste hinder van de problemen in de IT-systemen?
29 Is nu duidelijk welk overheidsorgaan verantwoordelijk is voor de beveiliging en werking van interdepartementaal digitaal verkeer? Zo ja, welke?
30 Kunt u verzekeren dat privacygevoelige informatie veilig is bij uw ministerie?
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?
32 Erkent u dat de verantwoordelijkheid voor *lifecycle management* niet kan worden uitbesteed en dat u daarvoor verantwoordelijk bent en blijft?
33 Wanneer verwacht u het *lifecycle-management*-proces volledig ingericht te hebben? Stelt u daar voldoende middelen ter beschikking voor?
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?
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?
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?
37 Onderschrijft u de aanbevelingen van de Algemene Rekenkamer om de reisadviezen beter te maken, en bent u van plan deze door te voeren?
38 Onderschrijft u het advies om de kleur leidend te maken in de reisadviezen?
39 Gaat u onderzoeken of reisadviezen sneller aangepast kunnen worden bij een verandering van de veiligheidssituatie? Wanneer verwacht u resultaat van dit onderzoek?

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?

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?

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?

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?

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