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

3134

Vragen van de leden **Bosman** en **Yeşilgöz-Zegerius** (beiden VVD) aan de Staatssecretaris van Defensie en de Minister van Justitie en Veiligheid over *het rapport «Digitalisering aan de grens; Cybersecurity van het grenstoezicht door de Koninklijke Marechaussee op Schiphol» van de Algemene Rekenkamer (20 april 2020)* (ingezonden 21 april 2020).

Antwoord van Minister **Bijleveld-Schouten** (Defensie), mede namens de Staatssecretaris van Justitie en Veiligheid (ontvangen 11 juni 2020).

Vraag 1, 3
Kunt u aangeven wanneer u van plan bent de goedkeuringsprocedure conform het defensiebeveiligingsbeleid voor de IT-systemen van de balie en de self-service op orde te hebben? Deelt u de mening dat het belangrijk is dit op korte termijn op orde te hebben en hierbij tenminste een duidelijke streefdatum en planning te hebben om naartoe te werken?
Kunt u aangeven per wanneer het self-servicesysteem is aangesloten op de detectiecapaciteit van het Security Operations Center van Schiphol?

Antwoord 1, 3
Voor zowel het IT systeem van de balie als de self-serviceportal geldt dat de goedkeuringsprocedure inmiddels loopt. De betrokken partijen hebben (gezamenlijk) de aanvullende beveiligingsmaatregelen geïdentificeerd die noodzakelijk zijn voor een (hernieuwde) goedkeuring en implementeren die momenteel. De aansluiting van het selfservicesysteem op het Security Operations Center (SOC) van Schiphol is onderdeel van de maatregelen die worden getroffen in het kader van de goedkeuringsprocedure en geschiedt bij de beslissing tot overdracht van het self-servicesysteem aan Schiphol (zie ook het antwoord op vraag 8). De volledige implementatie van de maatregelen is voorzien eind 2020, waarna de goedkeuringsprocedure kan worden afgerond.

Vraag 2
Bent u het met de Algemene Rekenkamer eens dat alle kritieke systemen van Defensie eigenlijk jaarlijks een beveiligingstest moeten doorlopen, gezien de snelle veranderingen van digitale dreigingen? Indien hiervoor de middelen ontbreken, kunt u dan aangeven welke middelen er nodig zijn om binnen afzienbare tijd wel dergelijke testen jaarlijks uit te voeren?

ah-tk-20192020-3134
ISSN 0921 - 7398
's-Gravenhage 2020

Antwoord 2
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 ook 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 4, 5
Kunt u ook aangeven per wanneer het baliesysteem en het systeem voor pre-assesment zijn aangesloten op het Security Operations Center van Defensie?
Kunt u aangeven wat de 14 kritieke ICT-systemen van Defensie zijn? Kunt u tevens aangeven of deze allemaal zijn aangesloten op het Security Operations Center?

Antwoord 4, 5
Processen en systemen die essentieel zijn 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 reeds een groot gedeelte van de risico's bij deze systemen.

Vraag 6, 7
Wanneer kunt u de Kamer informeren over de uitkomst van het overleg met ketenpartners om te oefenen op crisisbeheersing als gevolg van een cyberaanval op Schiphol? Deelt u de mening dat een dergelijke oefening binnen afzienbare tijd gehouden dient te worden en daarna ook periodiek herhaald dient te worden?
Kunt u in samenhang met de oefening ook richtlijnen opstellen over de omgang met voorstelbare scenario's, zoals de besmetting van systemen met «ransomware»?

Antwoord 6, 7
Inmiddels vinden gesprekken plaats over hoe een zinvolle oefening kan worden ingevuld. Daarbij wordt ook bekeken in hoeverre aansluiting bij bestaande oefeningen zoals ISIDOOR en gebruikmaking van documenten zoals het Nationaal Crisisplan Digitaal mogelijk is. Uw Kamer wordt hierover dit jaar geïnformeerd. Leerpunten uit oefeningen worden meegenomen in de actualisatie van richtlijnen over de omgang met bepaalde scenario's. Deze oefeningen dienen inderdaad periodiek herhaald te worden.

Vraag 8
Herkent u het door de Algemene Rekenkamer geschetste probleem van tegengestelde belangen, waarbij Defensie meer oog heeft voor veiligheid en Schiphol systemen snel wil implementeren om zo de doorstroming van passagiers te versnellen? Welke waarborgen gaat u inbouwen rond de

overdracht van het self-service systeem aan Schiphol? Kunt u de Kamer over deze waarborgen informeren voordat overdracht plaatsvindt?

Antwoord 8
Voor zowel Schiphol als de ministeries van Defensie en Justitie en Veiligheid heeft veiligheid bij het grenstoezicht de hoogste prioriteit. Schiphol en de betrokken ministeries werken nauw samen om de veiligheid te verzekeren. Alvorens te besluiten tot overdracht van het eigenaarschap van het selfservicesysteem aan Schiphol wordt bekeken hoe de veiligheid het effectiefst kan worden gewaarborgd. Dit sluit aan op het goedkeuringsproces volgens het Defensieveiligheidsbeleid. Het voltooien van het goedkeuringsproces en het blijvend voldoen aan de functionele en beveiligingseisen vanuit het Ministerie van Defensie zijn voorwaarden voor een overdracht van het systeem aan Schiphol. Het kabinet zal de Kamer nader informeren over het voorgenomen besluit en de voorwaarden waaronder dit gebeurt voordat overdracht plaatsvindt.