Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2020–2021

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 774

BRIEF VAN DE MINISTER VAN JUSTITIE EN VEILIGHEID

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 16 juli 2021

Bij de beantwoording van Kamervragen en het «Algemeen overleg Cybersecurity» op 9 december 2020 heb ik toegezegd uw Kamer te informeren over de voortgang op de aanbevelingen gedaan door de Algemene Rekenkamer (ARK) in het Rapport «Digitalisering aan de grens»[1].
Ook heb ik toegezegd u te informeren over het voorgenomen besluit om het eigenaarschap van het self service passport control systeem (SSPC) over te dragen van het Ministerie van het Ministerie van Justitie en Veiligheid aan Schiphol en de voorwaarden die aan deze beoogde overdracht verbonden worden.

De ARK beoordeelt het niveau van de cybersecurity van het grenstoezicht op Schiphol als onvoldoende en niet toekomstgericht[2]. De ARK heeft aanbevelingen gedaan om de beveiliging van de grenstoezichtsystemen op Schiphol te verbeteren. Hieronder informeer ik u mede namens de Staatssecretaris van Justitie en Veiligheid en de Minister van Defensie over de voortgang op de aanbevelingen.

Gezamenlijke aanbevelingen

Het ARK-rapport heeft individuele en gezamenlijke aanbevelingen gedaan aan het Ministerie van Justitie en Veiligheid en het Ministerie van Defensie. De voortgang op de eerste gezamenlijke aanbeveling: «het jaarlijks uitvoeren van beveiligingstesten op de grenstoezichtsystemen» wordt later in deze brief toegelicht. De tweede aanbeveling betreft het oefenen met alle relevante ketenpartijen van een crisis als gevolg van een

[1] Antwoorden op de Kamervragen van de leden Bosman en Yesilgöz-Zegerius over het rapport «Digitalisering aan de grens; Cybersecurity van het grenstoezicht door de Koninklijke Marechaussee op Schiphol» van de Algemene Rekenkamer (Aanhangsel Handelingen II 2020/21, nr. 3134) en Kamerstuk 28 684, nr. 645 verslag van een algemeen overleg vastgesteld 8 januari 2021.
[2] ARK rapport: Digitaliseren aan de grens (20 April, 2020); Kamerstuk 26 643, nr. 677

kst-26643-774
ISSN 0921 - 7371
's-Gravenhage 2021

cyberaanval op de drie IT-systemen van het grenstoezicht op Schiphol. In antwoord op de Kamervragen van 11 juni 2020 is toegezegd dat bekeken zal worden in hoeverre aansluiting bij bestaande oefeningen zoals de nationale cyberoefening ISIDOOR en gebruikmaking van documenten zoals het Nationaal Crisisplan Digitaal mogelijk is. De conclusie van deze verkenning is dat aansluiting bij ISIDOOR en het Nationaal Crisisplan Digitaal op zichzelf niet voldoende is voor het oefenen met het beheersen van een crisis als gevolg van een cyberaanval op de grenstoezichtsystemen op Schiphol. In aansluiting daarop is specifieke oefen-inzet in deze keten nodig. Derhalve is het Ministerie van Defensie zelf gestart met het ontwikkelen van een geschikte cybercrisisbeheersingsoefening. De verwachting is dat deze na zes maanden uitgevoerd kan worden met de ketenpartners. Deze crisisoefening wordt periodiek herhaald.

Individuele aanbevelingen aan het Ministerie van Justitie en Veiligheid

Het doorlopen van de goedkeuringsprocedure van het Defensiebeveiligingsbeleid voor het Self Service Passport Control (SSPC) systeem.

Naar aanleiding van bovengenoemd ARK-rapport hebben het Ministerie van Justitie en Veiligheid, het Ministerie van Defensie en Schiphol gezamenlijk de beveiligingsmaatregelen geïdentificeerd die noodzakelijk zijn om de goedkeuringsprocedure voor het SSPC conform het Defensiebeveiligingsbeleid succesvol te doorlopen.
Het volledig implementeren van de verbetermaatregelen loopt helaas aanzienlijk vertraging op. Als gevolg hiervan is de toezegging om in Q4 van 2020 de goedkeuringsprocedure aan te vragen niet gehaald. Het is de huidige verwachting dat in Q2/Q3 van 2022 de goedkeuringsprocedure aangevraagd kan worden.

De vertraging van de implementatie van deze aanbeveling heeft verschillende oorzaken. Allereerst brengt de publiek-private samenwerking en diversiteit van uitvoeringsorganisaties de nodige uitdagingen en samenwerkingsvraagstukken met zich mee. Bij verschillende stakeholders is schaarse specialistische capaciteit beschikbaar voor de innovatieve grensprojecten. Daarnaast hebben technische en financiële vraagstukken bijgedragen aan de vertraging. Technische vraagstukken zijn onder andere het gevolg van de Covid-19 pandemie. Door de beperkte reizigersstromen waren er niet voldoende gegevens beschikbaar en konden technische testen niet volledig uitgevoerd worden. Financiële vraagstukken zijn onder andere het gevolg van toenemende cybercriminaliteit. Sinds de covid-19 pandemie is deze stijging zelfs exponentieel. Dit heeft ertoe geleid dat de investeringen die nodig zijn voor beveiligingsmaatregelen om cybercriminaliteit tegen te gaan zijn toegenomen.

Op dit moment worden risico's beperkt door het beveiligde netwerk van Schiphol. Dit vormt een eerste beveiligingslaag voor het tegengaan en detecteren van mogelijke cyberaanvallen op het netwerk. In het kader van de goedkeuringsprocedure dient dit netwerk verder aangepast te worden.

Aansluiting van het SSPC systeem op het detectiesysteem van een Security Operation Control (SOC)

Ten tijde van het opstellen van een reactie op de bevindingen van de ARK waren er activiteiten gericht om het SSPC systeem aan te sluiten op het SOC van Schiphol. Door de heroverweging van de overdracht van het SSPC systeem aan Schiphol zijn deze werkzaamheden niet volledig doorgezet.

Aansluiting van het SSPC systeem op een SOC is onderdeel van de goedkeuringsprocedure. Ook is een SOC aansluiting onderdeel van de besluitvorming van overdracht van het SSPC systeem aan Schiphol. De daadwerkelijke implementatietijd om het SSPC systeem op een SOC aan te sluiten is afhankelijk van fundamentele aanpassingen aan het SSPC systeem en de fysieke ICT infrastructuur.

Jaarlijkse beveiligingstesten van de software

Als onderdeel van de goedkeuringsprocedure van het SSPC systeem zijn vorig jaar door een onafhankelijke partij beveiligingstesten uitgevoerd op de doorontwikkelde softwareversie. Deze software is nog niet operationeel geïmplementeerd. Door middel van penetratietesten (systeembeveiligingstesten) zijn risico's en kwetsbaarheden van de software inzichtelijk gemaakt. Hierna zijn gerichte verbeteringen doorgevoerd die de beveiliging versterken en kwetsbaarheden mitigeren. Middels een tweede penetratietest is vervolgens zeker gesteld dat de meest risicovolle bevindingen zijn opgelost. Momenteel vinden acceptatietesten van deze verbeterde softwareversie plaats. Na het succesvol afronden van deze testen, kan de nieuwe software geïmplementeerd worden op het SSPC systeem op Schiphol. De beveiligingstesten zullen periodiek herhaald worden en zijn onderdeel van de goedkeuringsprocedure van het Defensiebeveiligingsbeleid.

Overdracht van SSPC aan Schiphol

Momenteel vinden gesprekken plaats over de overdracht van het SSPC systeem van het Ministerie van Justitie en Veiligheid aan Schiphol. Naar verwachting worden afspraken over de gevolgen van de overdracht en het eigenaarschap afgerond in Q3 2021. Een overdracht verandert niets aan de bestaande wettelijke verantwoording inzake de uitvoering van het grenstoezicht. Het Ministerie van JenV is en blijft beleidsverantwoordelijk voor de uitvoering van het grenstoezicht door de grensautoriteiten. Het Ministerie van Defensie is en blijft verwerkingsverantwoordelijk van de data in de systemen van de Koninklijke Marechaussee. De overdracht vindt plaats binnen de functionele eisen, het beveiligingsbeleid en de Algemene Beveiligingseisen Defensieopdrachten (ABDO).

Individuele aanbevelingen aan het Ministerie van Defensie

Afronden goedkeuringsprocedure

Een van de aanbevelingen aan het Ministerie van Defensie was om te zorgen dat in het IT-systeem (Border Control System, BCS) van de grensbalie zo spoedig mogelijk de benodigde beveiligingsmaatregelen worden genomen zodat de goedkeuringsprocedure conform het Defensiebeveiligingsbeleid kan worden afgerond. De huidige planning is om dit in Q4-2021 afgerond te hebben. De andere aanbeveling is om de twee IT-systemen van het grenstoezicht zo snel mogelijk aan te sluiten op de detectiecapaciteit van het SOC van het Ministerie van Defensie en daarbij de hoogste prioriteit te geven aan het als «kritiek» benoemde systeem voor pre-assessment. Het Ministerie van Defensie is bezig met een standaardisatie traject om IT-systemen standaard gekoppeld te krijgen op het SOC. Het streven is om beide IT-systemen van het grenstoezicht, dus BCS en API3, zo snel mogelijk gekoppeld te krijgen op het SOC.

Vervolg

In deze brief ben ik ingegaan op de belangrijkste maatregelen waarmee ik, in samenwerking tussen publieke partners en de private partner Schiphol,

opvolging zal geven aan de aanbevelingen van de ARK gericht op een veilig en toekomstbestendig grenstoezicht. Ik zal de implementatie van de verbetermaatregelen nauwlettend volgen en uw Kamer nader berichten over de verdere voortgang.

De Minister van Justitie en Veiligheid,
F.B.J. Grapperhaus