Algemene Rekenkamer

Digitalisering aan de grens

Cybersecurity van het grenstoezicht door de Koninklijke Marechaussee op Schiphol

2020

Vooraf

Nederland is met de rest van de wereld sinds begin dit jaar in de greep geraakt van het coronavirus – SARS-CoV-2, dat de ziekte COVID19 veroorzaakt. De maatregelen die sinds maart zijn genomen, hebben grote impact gehad op het dagelijks leven van alle Nederlanders. Ook op de werkvloer van de Algemene Rekenkamer zijn deze maatregelen voelbaar.

Dit onderzoek is medio 2019 begonnen. Het beschrijft de situatie vóór de komst van corona naar Nederland. Toen in Nederland de maatregelen tegen het coronavirus van kracht werden en het kabinet alle aandacht moest richten op crisisbeheersing, viel dat samen met het moment waarop wij onze bevindingen voorlegden aan de verantwoordelijke ministers. Daarbij gaat het om conclusies over feiten die in 2019 plaatsvonden. Die conclusies veranderen niet vanwege de ernstige ontwikkelingen in 2020. Onder deze moeilijke omstandigheden waren de betrokken ministers desondanks in de gelegenheid te reageren op onze conclusies en aanbevelingen. Dit illustreert dat ons democratisch systeem, waarvan de onafhankelijke controle van de Algemene Rekenkamer deel uitmaakt, blijft functioneren. Zelfs onder de uitzonderlijke omstandigheden van het voorjaar van 2020.

De tekst in dit document is vastgesteld op 10 april 2020. Dit document is op 20 april 2020 aangeboden aan de Tweede Kamer.

Luchthaven Schiphol is een internationale hub. Voor het grenstoezicht worden grote hoeveelheden persoongegevens van reizigers van over de hele wereld verwerkt.

Inhoud

1 Samenvatting

Schiphol is met bijna 80 miljoen passagiers per jaar niet alleen de belangrijkste luchthaven van Nederland maar ook een belangrijke toegangspoort tot Europa / de Europese Unie (EU). De Koninklijke Marechaussee (KMar) controleert reizigers die op luchthaven Schiphol de Schengenzone binnenkomen of verlaten. Hierbij verwerkt de KMar persoonsgegevens van passagiers van over de hele wereld. Het betreft onder meer informatie over nationaliteit, reisroute, reisgezelschap en in sommige gevallen strafrechtelijke gegevens. Met dit grenstoezicht draagt de KMar bij aan veiligheid en grip op immigratie. Het belang van IT bij het grenstoezicht is groot en groeiende. Digitalisering maakt het grenstoezicht grondiger en sneller, maar creëert tegelijkertijd een afhankelijkheid en nieuwe risico's.

Cyberaanvallen -bijvoorbeeld in de vorm van digitale sabotage, spionage en criminaliteit- bedreigen de continuïteit van het grenstoezicht en de vertrouwelijkheid van de verwerkte gegevens. Als de IT-systemen uitvallen, kan de KMar de grenscontrole niet uitvoeren. Een ander risico is dat buitenlandse veiligheidsdiensten cyberspionage inzetten om de gegevens van (specifieke) reizigers in te zien. Maar cyberaanvallen zouden ook ingezet kunnen worden om bijvoorbeeld informatie te manipuleren, zodat gezochte personen makkelijker de grens kunnen passeren.

Het grenstoezicht wordt de komende jaren onder andere door initiatieven van de EU en Royal Schiphol Group N.V. (hierna: Schiphol N.V.) verder gedigitaliseerd. Aan de vooravond van nog grootschaliger inzet van technologie hebben we daarom onderzocht hoe het grenstoezicht op Schiphol beschermd is tegen cyberaanvallen.

Ons onderzoekt spitst zich toe op de drie primaire en IT-intensieve processen van het grenstoezicht:

1. de controles op aankomende passagiers gedurende hun vlucht;
2. de controles bij de KMar-balies op Schiphol;
3. de controles bij de *self service passport control* op Schiphol.

Elk van deze processen wordt ondersteund door een eigen IT-systeem. De minister van Defensie is verantwoordelijk voor de cybersecurity van de systemen die de eerste twee processen ondersteunen. De minister van Justitie en Veiligheid (JenV) draagt de verantwoordelijkheid voor het IT-systeem voor het derde proces.

Uit ons onderzoek blijkt dat de werking van de cybersecuritymaatregelen in de praktijk nog te wensen overlaat. Het Ministerie van JenV maakt voor de cybersecurity van het grenstoezicht gebruik van expertise en IT-infrastructuur van het Ministerie van Defensie en Schiphol N.V. Binnen het Ministerie van Defensie is de expertise aanwezig om een hoog niveau van cybersecurity te waarborgen. De organisatie zet deze in de praktijk niet altijd in conform afspraken en eigen richtlijnen. In het licht van alle komende technologische ontwikkelingen beoordelen we het huidige niveau van cybersecurity op het grenstoezicht als onvoldoende en niet toekomstbestendig.

Het Ministerie van Defensie heeft een vastgesteld cybersecuritybeleid. Onderdeel daarvan is dat de beveiliging van de belangrijkste IT-systemen moet zijn goedgekeurd vóór de systemen gebruikt mogen worden. Dit beleid is van toepassing op de twee systemen van het grenstoezicht van het Ministerie van Defensie. Daarnaast is besloten dat het systeem waar het Ministerie van JenV eigenaar van is deze goedkeuring ook moet krijgen. Uit ons onderzoek blijkt dat het IT-systeem van de balie en het selfservicesysteem operationeel zijn zonder de vereiste goedkeuring. Daardoor is niet vastgesteld dat ze veilig zijn. Specialisten kunnen cyberaanvallen snel detecteren door IT-systemen continu te monitoren. Het Ministerie van Defensie en Schiphol N.V. beschikken beiden over dergelijke detectiecapaciteit in de vorm van een Security Operations Center (SOC). De IT-systemen die het grenstoezicht ondersteunen zijn zelf niet op de detectiecapaciteit van deze SOC's aangesloten. Hierdoor bestaat het risico dat cyberaanvallen op deze IT-systemen niet of te laat worden opgemerkt.

Bij het IT-systeem waarvan het Ministerie van JenV eigenaar is, zijn meerdere publieke en private partijen betrokken. Een gezamenlijke beveiligingstest verliep hierdoor moeizaam en had als resultaat dat een kleiner deel getest werd dan de partijen van plan waren. Ook bij de goedkeuring van de beveiliging van het systeem zijn de verschillende betrokken partijen van elkaar afhankelijk.

In ons onderzoek bleek dat het IT-systeem voor de balie en het pre-assessmentsysteem nog niet onderworpen waren aan de voorgeschreven beveiligingstests. Voor het selfservicesysteem gold dat in beperkte mate. Zonder regelmatige beveiligingstesten blijven kwetsbaarheden in IT-systemen bestaan. Deze kunnen misbruikt worden bij een cyberaanval. Voor dit onderzoek is een beveiligingstest gedaan op pre-assessmentsystemen, dat nog niet getest was. Uit die test kwamen 11 kwetsbaarheden aan het licht waaronder het gebruik van zwakke wachtwoorden en de mogelijkheid e-mails te versturen uit naam van willekeurige Defensiemedewerkers. Door de kwetsbaarheden te combineren zou een

aanvaller het systeem kunnen binnendringen en de werking kunnen beïnvloeden. Het Ministerie van Defensie heeft inmiddels maatregelen genomen waardoor een dergelijke aanval niet meer mogelijk is.

Het Ministerie van Defensie heeft uitgebreide procedures voor het afhandelen van IT-verstoringen en crisissituaties. Onderdeel daarvan zijn specifieke procedures voor verstoringen die worden veroorzaakt door een cyberaanval. Het Ministerie van Defensie oefent met cybercrisissituaties. Het ontbreekt echter aan voorbereiding aan de hand van concrete scenario's, zoals een aanval met gijzelsoftware (*ransomware*) waarbij losgeld wordt geëist. Ook is er geen cyberoefening gedaan voor het grenstoezicht. Hierdoor is onzeker of de reactie vanuit het Ministerie van Defensie op een cyberaanval in de praktijk van het grenstoezicht effectief is.

Aanbevelingen

Om de cybersecurity van het grenstoezicht door de KMar op Schiphol te vergroten, doen we aanbevelingen aan de verantwoordelijke bewindspersonen.

We bevelen de minister van Defensie aan:

- Zorg dat voor het IT-systeem van de balie zo spoedig mogelijk de benodigde beveiligingsmaatregelen worden genomen zodat de goedkeuringsprocedure conform het Defensiebeveiligingsbeleid kan worden afgerond.
- Sluit de twee IT-systemen van het grenstoezicht waar het Ministerie van Defensie voor verantwoordelijk is zo snel mogelijk aan op de detectiecapaciteit van het SOC van het Ministerie van Defensie en geef hierbij de hoogste prioriteit aan het als 'kritiek' benoemde systeem voor pre-assessment.

We bevelen de minister van JenV aan:

- Zorg dat het selfservicesysteem de goedkeuringsprocedure conform het Defensiebeveiligingsbeleid zo spoedig mogelijk doorloopt, waarbij Schiphol N.V. alle beveiligingseisen implementeert en blijft implementeren en het systeem goedkeuring verkrijgt van de beveiligingsautoriteit van het Ministerie van JenV.
- Overdenk opnieuw of met de voorgenomen overdracht van het selfservicesysteem aan Schiphol N.V. de cybersecurity afdoende gewaarborgd is.
- Zorg dat het selfservicesysteem zo snel mogelijk op de detectiecapaciteit van het SOC van Schiphol N.V. wordt aangesloten.

We bevelen de minister van Defensie en de minister van JenV gezamenlijk aan:

- Onderwerp de drie grenstoezichtsystemen zo snel mogelijk, conform het Defensie-beveiligingsbeleid, aan jaarlijkse beveiligingstesten en borg de opvolging van aanbevelingen.
- Laat het Ministerie van Defensie en het Ministerie van JenV in samenwerking met alle relevante ketenpartijen oefenen met het beheersen van crises als gevolg van een cyberaanval op de drie IT-systemen van het grenstoezicht op Schiphol.

2 Over dit onderzoek

2.1 Wat is er aan de hand?

Cybersecurity is het geheel aan maatregelen om schade door verstoring, uitval of misbruik van IT te voorkomen en, indien er toch schade is ontstaan, deze te herstellen (NCTV, 2018). Doelbewuste pogingen om langs digitale weg schade aan IT te veroorzaken, zoals het verspreiden van *malware* of hacken van systemen, vatten we samen onder het begrip cyberaanvallen.

De continuïteit van vitale processen, zoals de levering van elektriciteit en het mobiele telefoonnetwerk, is van groot belang voor Nederland.[1] Deze processen zijn sterk gedigitaliseerd en dus kwetsbaar voor cyberaanvallen. In het *Cybersecuritybeeld Nederland 2019* waarschuwt de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) voor de mogelijke gevolgen van deze afhankelijkheid van IT. Volgens de NCTV is er sprake van een permanente dreiging van cyberaanvallen en ligt maatschappelijke ontwrichting op de loer (NCTV, 2019). De Wetenschappelijke Raad voor het Regeringsbeleid (WRR) concludeerde dat de voorbereiding op digitale ontwrichting te weinig aandacht krijgt (WRR, 2019). De Algemene Rekenkamer doet onderzoek naar informatiebeveiliging binnen het Rijk en onderzoekt daarbij de weerbaarheid tegen cyberaanvallen van vitale processen binnen de rijksoverheid.[2] Zo constateerden we in 2019 dat de cybersecurity van vitale waterwerken van Rijkswaterstaat extra aandacht behoefde (Algemene Rekenkamer, 2019a).

Het grenstoezicht door de Koninklijke Marechaussee (KMar) op Schiphol is het vitale proces dat centraal staat in dit onderzoek. De KMar is één van de krijgsmachtonderdelen van het Ministerie van Defensie. Grenstoezicht is van vitaal belang voor de veiligheid en stabiliteit van Nederland. Tegelijkertijd wil de KMar zoveel mogelijk voorkomen dat het toezicht leidt tot grote vertragingen op de luchthaven en daardoor (vitale) economische belangen schaadt. Ook moeten burgers erop kunnen rekenen dat hun persoonsgegevens veilig worden verwerkt.

Risico's van cyberaanvallen op het grenstoezicht

Schiphol is met bijna 80 miljoen passagiers per jaar niet alleen de belangrijkste luchthaven van Nederland, maar ook een belangrijke toegangspoort tot Europa / de Europese Unie (EU) en de tweede *hub* van Europa.[3] Voor het grenstoezicht verwerkt de KMar persoonsgegevens van passagiers van over de hele wereld. Het betreft onder meer informatie over nationaliteit, reisroute, reisgezelschap en in sommige gevallen strafrechtelijke gegevens. Verschillende incidenten illustreren dat aanvallers het op deze gegevens gemunt hebben.

Zo zijn bij cyberaanvallen op de Amerikaanse grenscontroleautoriteit en luchtvaartmaatschappijen persoonlijke gegevens van miljoenen passagiers buitgemaakt.[4] Het grenstoezicht kan door het belang voor Schiphol en de grote hoeveelheden persoonsgegevens een interessant doelwit zijn voor hackers.

Een eerste mogelijke cyberaanval zou gericht kunnen zijn op het verstoren van de beschikbaarheid van het grenstoezicht. Als de IT-systemen van het grenstoezicht onbruikbaar worden, kan de KMar het grenstoezicht niet uitvoeren. Dit zorgt voor lange wachtrijen op Schiphol, vertraging en annulering van vluchten met economische en maatschappelijke schade als gevolg. Bij uitval van systemen kan de KMar door overmacht moeten besluiten de controles tijdelijk te versoepelen. Op dat moment vergroot de cyberaanval bijvoorbeeld het risico op illegale migratie. In juni 2019 was de KMar door een technische storing – niet zijnde een cyberaanval – genoodzaakt de controles op de grens ruim een uur te versoepelen.

Een ander scenario is een aanval op de vertrouwelijkheid van de IT-systemen. Volgens het Nationaal Cyber Security Centrum (NCSC) is de dreiging van cyberspionage door buitenlandse veiligheidsdiensten permanent en groeiende (NCTV & NCSC, 2019). Zij zijn mogelijk geïnteresseerd in de reisbewegingen van diplomaten, onderdrukte minderheden of politieke tegenstanders en kunnen proberen systemen binnen te dringen om deze informatie te bemachtigen. Ook de Militaire Inlichtingen en Veiligheidsdienst (MIVD) heeft ons bevestigd dat veiligheidsdiensten uit het buitenland interesse kunnen hebben in gegevens van reizigers die bij het grenstoezicht op Schiphol verwerkt worden. Schiphol is als internationale hub een interessant doelwit.

Een derde risico is een geavanceerde cyberaanval die zich zou kunnen richten op het manipuleren van informatie. Het grenstoezicht is afhankelijk van de betrouwbaarheid (‘integriteit’) van de gebruikte informatie. Als een aanvaller er bijvoorbeeld in slaagt informatie op opsporingslijsten te manipuleren, kunnen gezochte personen makkelijker ongemerkt de grens passeren.

De potentiële risico’s van cyberaanvallen worden in de toekomst groter. Met de plannen van Schiphol N.V. voor biometrische grenspassage en Europese ontwikkelingen voor een entry-exit systeem om in- en uitreizen van personen die tijdelijk in de Schengenzone mogen verblijven te registreren, ontstaan nieuwe (biometrische) gegevensverzamelingen en onderlinge koppelingen. Kans op en impact van een cyberaanval nemen daarmee toe.

Belang van IT bij grenstoezicht groot en groeiende

Om de balans tussen veiligheid en mobiliteit te bewaren maakt de KMar steeds meer gebruik van IT bij de grens. Dat maakt het grenstoezicht grondiger en sneller, maar ook afhankelijker van een goede werking van de automatisering. De EU, Schiphol N.V. en de KMar willen het grenstoezicht op Schiphol de komende jaren nog verder digitaliseren:

- Met het EU-programma *Smart Borders* is in 2020 een systeem voorzien voor registratie van alle in- en uitreizende personen.[5]
- In 2021 moet het *European Travel Information and Authorisation System* (ETIAS) operationeel zijn: een Europees systeem voor reisautorisatie vergelijkbaar met het Amerikaanse *Electronic System for Travel Authorization* (ESTA).
- In de EU wordt samengewerkt aan het uitbreiden en uniformeren van digitale informatiesystemen bij de grens, zoals visa-systemen en opsporingsregisters.
- Onder de noemer *Seamless Flow* experimenteert Schiphol N.V. momenteel met biometrische grenspassage. Op termijn is het doel om na eenmalige registratie van biometrische kenmerken alle controlepunten op de luchthaven te kunnen passeren, waaronder de grensdoorlaatposten van de KMar.[6]
- De KMar is voornemens de bestaande IT-systemen bij het grenstoezicht uit te breiden met nieuwe functionaliteit, bijvoorbeeld om extra digitale controles op de echtheid van reisdocumenten te doen.

De IT van het grenstoezicht is dus sterk in ontwikkeling. De digitaliseringsambities voor de komende jaren stellen de bij het grenstoezicht betrokken partijen voor een grote opgave, ook op het gebied van cybersecurity. Ze leiden immers tot meer en grotere IT-systemen, een groeiend aantal digitale koppelingen en extra verwerking van persoonsgegevens. Zowel de kans op als de impact van een cyberaanval op het grenstoezicht nemen daarmee toe.

2.2 Wie is politiek verantwoordelijk?

Wet beveiliging netwerk en -informatiesystemen

De Wet beveiliging netwerk- en informatiesystemen (Wbni) stelt eisen aan de IT-beveiliging van processen die van vitaal belang zijn voor de Nederlandse samenleving. De Wbni onderkent 'een veilige en vlotte vlucht- en vliegtuigafhandeling voor wat betreft de luchthaven Schiphol' als 'essentiële dienst'. De KMar is in de Wbni aangewezen als een van de aanbieders van deze dienst. Ook Schiphol N.V. is genoemd als aanbieder. Volgens de nota van toelichting bij het besluit is de KMar aangewezen als een van de aanbieders omdat verstoring van het grenstoezicht op Schiphol kan leiden tot passagiersopstoppingen en uitval van het vliegverkeer.

Aanbieders van een essentiële dienst moeten op grond van de Wbni maatregelen nemen om beveiligingsrisico's op hun IT-systemen te beheersen, beveiligingsincidenten te voorkomen en de gevolgen ervan te beperken. Daarnaast moeten zij beveiligingsincidenten met aanzienlijke gevolgen voor de verleende dienst melden bij de minister van Justitie en Veiligheid (JenV).

Zowel de minister van Defensie als de minister van JenV dragen politieke verantwoordelijkheid voor de KMar en het grenstoezicht. De minister van JenV stelt de wettelijke kaders voor het grenstoezicht (gezag). De minister van Defensie stelt mensen en middelen beschikbaar waarmee de KMar haar taken uitvoert (beheer). Bij de cybersecurity van de IT-systemen zien we ook dat beide bewindspersonen betrokken zijn. Het Ministerie van Defensie is eigenaar van twee van de drie IT-systemen waardoor de minister van Defensie verantwoordelijk is voor een adequaat niveau van cybersecurity. Het Ministerie van JenV is eigenaar van het derde systeem. Bij dat systeem ligt die verantwoordelijkheid dus bij de minister van JenV.

2.3 Wat hebben we onderzocht?

We hebben onderzoek gedaan naar de maatregelen die de ministers van Defensie en JenV treffen om de systemen van het grenstoezicht door de KMar op luchthaven Schiphol te beschermen tegen cyberaanvallen. Daarbij hebben we specifiek gekeken naar de maatregelen om cyberaanvallen snel op te kunnen merken ('detectie') en de werkwijze om de gevolgen van een cyberaanval in te dammen ('respons'). Ook hebben we onderzocht of de maatregelen in de praktijk werken. We beantwoorden de volgende onderzoeksvragen:

1. Hoe ziet de context van het grenstoezicht door de KMar op Schiphol eruit, welke processen kent het grenstoezicht en welke IT is hieraan ondersteunend?
2. Welke preventieve cybersecuritymaatregelen zijn er genomen rondom de IT van het grenstoezicht?
3. Welke detectiemaatregelen zijn er, en zijn deze voldoende?
4. Hoe werken deze detectiemaatregelen in de praktijk en bieden ze voldoende bescherming?
5. Welke responsscenario's zijn er voor cyberincidenten, en zijn die voldoende?
6. Hoe werken de responsscenario's in de praktijk en is dat voldoende?

De eerste onderzoeksvraag beantwoorden we in hoofdstuk 3. Onderzoeksvraag 2 komt aan bod in hoofdstuk 4. In hoofdstuk 5 gaan we in op onderzoeksvragen 3 en 4. Hoofdstuk 6 is gewijd aan onderzoeksvragen 5 en 6. In hoofdstuk 7 volgen de conclusies en aanbevelingen. In hoofdstuk 8 volgt ten slotte de reactie van de ministers en het nawoord van de Algemene Rekenkamer.

Afbakening

Bij aanvang van het onderzoek hebben we onderzocht welke processen een rol spelen bij het grenstoezicht. Op basis daarvan bakenden we ons onderzoek af tot drie KMar-processen (zie § 3.1 en § 3.2). In de eerste plaats vinden in die drie processen de primaire controles op grote groepen passagiers plaats, waardoor verstoring door een cyberaanval de meeste impact zal hebben. Ten tweede zijn dit sterk gedigitaliseerde processen, waardoor de afhankelijkheid van IT groot is. Overige processen bij het grenstoezicht, zoals het mobiele toezicht door de KMar op Schiphol of tweedelijnscontroles op de authenticiteit van documenten, hebben we niet onderzocht.

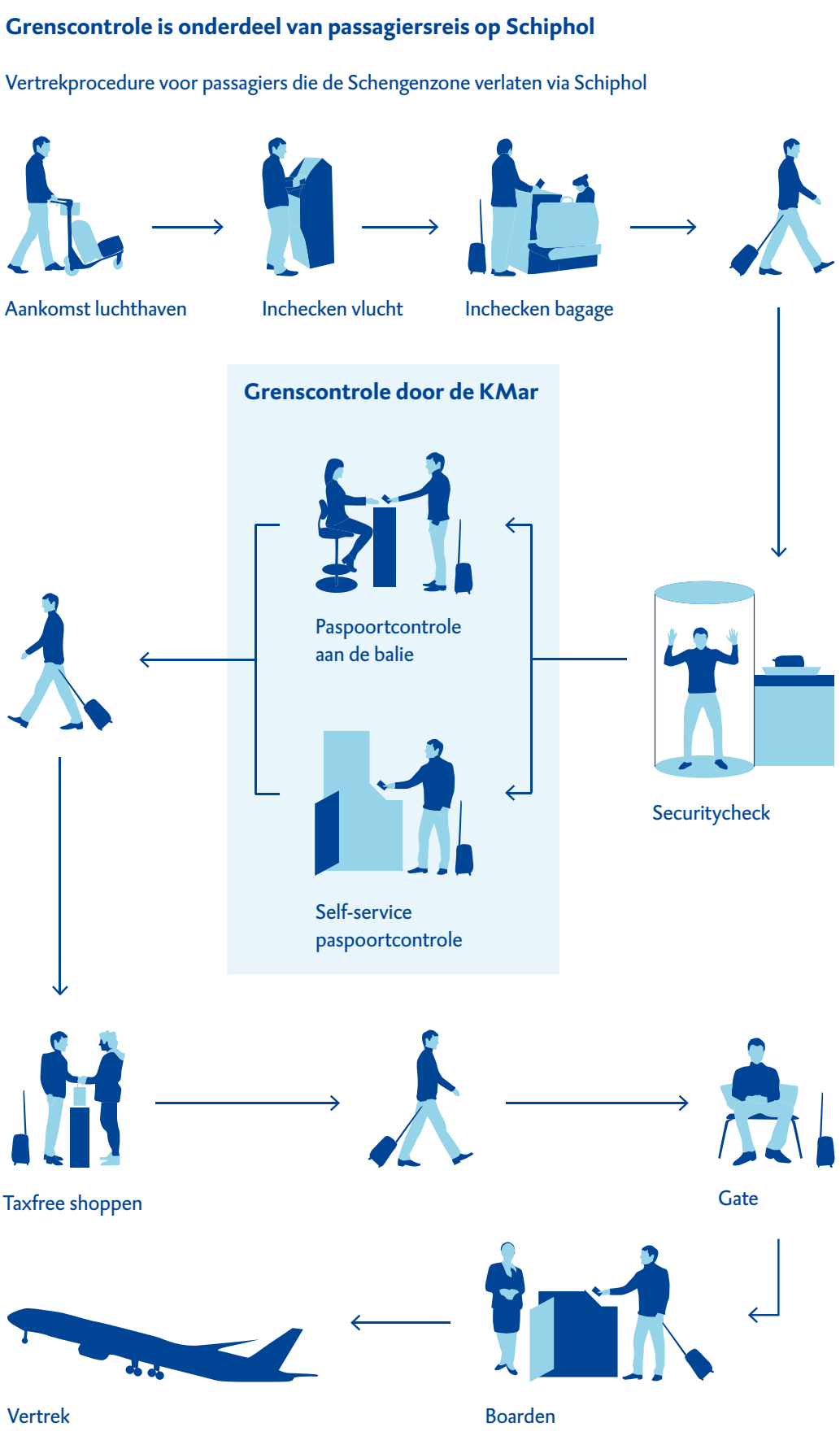
Vervolgens zijn we nagegaan welke IT-systemen deze drie processen ondersteunen (zie § 3.3). Elk van de processen bleek ondersteund door een eigen IT-systeem. Deze IT-systemen hebben we nader onderzocht. De generieke IT-voorzieningen zoals het netwerk en de besturingssystemen hebben we daarbij buiten beschouwing gelaten. De drie systemen zijn onderzocht tot aan de koppelvlakken met andere systemen, zoals bijvoorbeeld het politie-systeem met strafrechtelijke gegevens dat bij het grenstoezicht door de KMar geraad-pleegd wordt.

2.4 Hoe hebben we het onderzoek uitgevoerd?

Voor het beantwoorden van de onderzoeksvragen bestudeerden we in de periode juli tot en met november 2019 interne documenten bij het Ministerie van Defensie en het Ministerie van JenV. Ook legden we werkbezoeken af aan de KMar op Schiphol en voerden we gesprekken met betrokkenen. Hierbij keken we naar de opzet van de maatregelen en voorbeelden van de werking in de praktijk. Op ons initiatief hebben we voor dit onderzoek samen met specialisten van het Ministerie van Defensie de weerbaarheid van één van de drie IT-systemen in de praktijk getoetst met een beveiligingstest. Als normenkader voor ons onderzoek hanteerden we het cybersecurity-raamwerk van het *National Institute of Standards and Technology* (NIST). In de methodologische verantwoording in bijlage 1 staat meer informatie over onze aanpak.

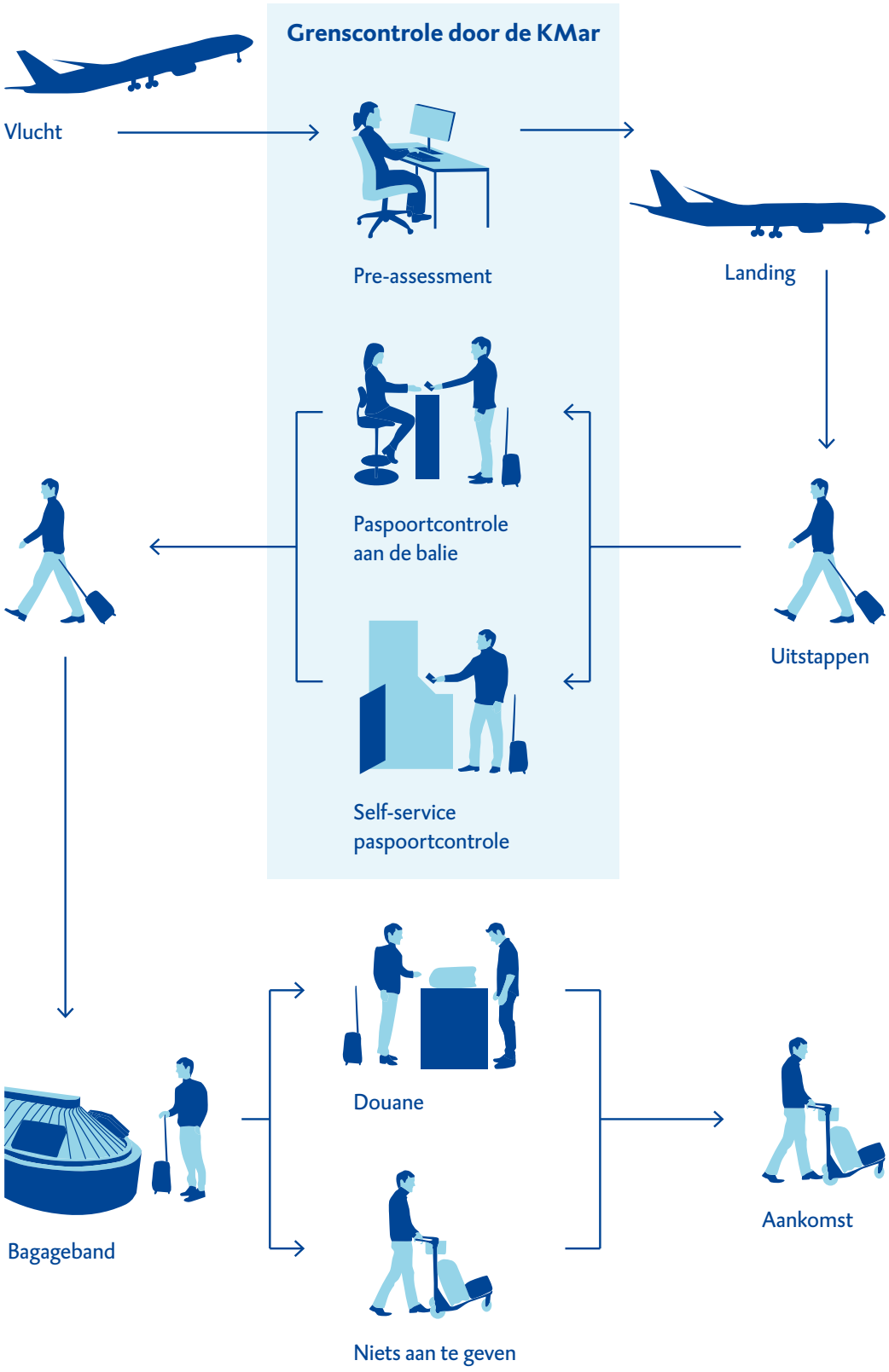
3 Proces van het grenstoezicht op Schiphol

In 1985 tekende Nederland met België, Luxemburg, Duitsland en Frankrijk het eerste verdrag van Schengen. Het verdrag creëerde de Schengenzone, waarbinnen inwoners van de deelnemende landen vrij kunnen reizen. De Schengenzone is in de loop der jaren flink uitgebreid. Binnen de Schengenzone zijn grenscontroles bij grensdoorlaatposten op luchthavens verleden tijd voor onderdanen van Schengenlanden en EU-lidstaten. De Koninklijke Marechaussee (KMar) controleert op Schiphol alleen passagiers op vluchten vanuit of naar een land buiten de Schengenzone. Figuur 1 en figuur 2 geven schematisch weer wanneer deze passagiers op hun reis te maken krijgen met grenstoezicht.



Figuur 1 *Grenstoezicht bij vertrek vanaf Schiphol*

Aankomstprocedure voor passagiers die de Schengenzone binnenkomen via Schiphol



Figuur 2 *Grenstoezicht bij aankomst op Schiphol*

3.1 Controles vóór aankomst: pre-assessment

De KMar doet de eerste controles op aankomende passagiers terwijl hun vlucht onderweg is naar Schiphol. Luchtvaartmaatschappijen zijn verplicht om direct na het opstijgen passagiersgegevens bij de KMar aan te leveren.

Via pre-assessment controleert de KMar voor aankomst van een vlucht of er passagiers zijn die extra gecontroleerd moeten worden

Figuur 3 *Pre-assessment*

De KMar voert met die gegevens tijdens de vlucht een pre-assessment uit. Daarbij controleert de KMar bijvoorbeeld alvast of aankomende passagiers op justitiële opsporingslijsten staan of, op basis van hun profiel, iets met mensensmokkel te maken hebben. Het doel van de pre-assessment is om alvast aan de grensdoorlaatposten op Schiphol door te geven welke passagiers (extra) gecontroleerd moeten worden. Zo verloopt het grenstoezicht daar sneller en effectiever.

3.2 Controles bij de grensdoorlaatpost: balie en Self Service Passport Control

Passagiers die aankomen uit of vertrekken naar een land buiten de Schengenzone passeren op Schiphol een grensdoorlaatpost van de KMar. Bij grensdoorlaatposten voor aankomende passagiers kan de KMar extra aandacht geven aan bepaalde passagiers, op basis van informatie uit het pre-assessment. De KMar voert bij de grensdoorlaatpost grenstoezicht uit via grenswachters achter een balie of geautomatiseerd via *Self Service Passport Control* (SSPC).

Bij de grensdoorlaatpost op Schiphol voert de KMar grenstoezicht uit aan de balie, en volledig geautomatiseerd via Self Service Passport Control

Paspoortcontrole balie Selfservice

Figuur 4 *Paspoortcontrole bij de balie en via selfservice*

Reizigers die niet onder het vrije Europese verkeer vallen of jonger dan 16 jaar zijn, zijn in principe verplicht om langs de balie te gaan.[7] Andere passagiers mogen kiezen tussen balie of selfservice. Bij alle passagiers wordt de identiteit en geldigheid van hun reisdocumenten vastgesteld. Ook wordt gekeken of ze voorkomen op opsporingslijsten en of hun reisdocument geregistreerd staat als vermist of gestolen. In het geval van aankomende passagiers zijn dat dubbele controles: ze zijn namelijk ook al in het pre-assessment uitgevoerd. Bij selfservice zijn de controles volledig geautomatiseerd. De selfservicepoortjes worden overzien door een KMar-grenswacht maar de reizigers scannen zelf hun paspoort en het systeem controleert op basis van biometrie hun identiteit. De KMar-grenswacht kan, als er iets niet in orde is, de passagier meenemen voor een nadere controle.

Bij de balie scant de KMar-grenswacht het paspoort handmatig. Daarbij kan de grenswacht nog nader onderzoek doen, bijvoorbeeld door vragen te stellen over het doel en de duur van de reis. Ook kan de grenswacht besluiten vragen te stellen aan meereizende minderjarigen. Tijdens ons werkbezoek aan Schiphol constateerden we hoe nauwgezet en snel de KMar-medewerkers bij de grensdoorlaatpost grote aantallen passagiers moeten controleren en hoe belangrijk de IT-ondersteuning daarbij is.

3.3 IT-systemen van het grenstoezicht

De drie belangrijkste processen van het grenstoezicht (pre-assessment, selfservice en de balie) werken elk met een eigen IT-systeem. Die van het pre-assessment en de balie zijn eigendom van het Ministerie van Defensie. Het selfservicesysteem SSPC is eigendom van

het Ministerie van Justitie en Veiligheid (JenV). In 2016 is een project gestart om het bestaande systeem door te ontwikkelen met een nieuwe softwareversie. Bij dit technisch ingewikkelde project zijn verschillende publieke en private partijen betrokken. Naast het Ministerie van JenV (als eigenaar) spelen ook Schiphol N.V. en het Ministerie van Defensie (gezamenlijk beheer), een externe softwareleverancier, sub-leveranciers en de KMar (als gebruiker) een rol.

De partijen hebben niet altijd dezelfde belangen. De nieuwe software is cruciaal voor het toekomstige *Seamless Flow* (zie § 2.1). Schiphol N.V. en de softwareleverancier willen de nieuwe software graag zo snel mogelijk implementeren. Zij zien *Seamless Flow* als een belangrijk innovatief project. De KMar wil echter primair dat het selfservicesysteem stabiel en veilig genoeg is. Tot nu toe voldoet de nieuwe software nog niet aan de beveiligingseisen van het Ministerie van Defensie (zie § 4.1.2) en vindt de KMar de nieuwe software nog onvoldoende stabiel. Wij zien hier een risico dat het belang van veiligheid van het self-servicesysteem ondergeschikt raakt aan dat van de snelle uitrol van *Seamless Flow*.

De uitrol van de nieuwe software zou oorspronkelijk al in 2016 gereed zijn maar is vertraagd. Dit komt onder andere doordat de betrokken partijen veel moeten afstemmen vanwege hun uiteenlopende belangen. Het Ministerie van JenV en de betrokken partijen willen hier iets aan doen. Zo wil het Ministerie van JenV met een nieuwe integrale planning de beperkt beschikbare capaciteit en afhankelijkheden bij de verschillende partijen beter op elkaar afstemmen. Volgens de laatste planning is de nieuwe software halverwege 2020 gereed, waarna deze kan worden uitgerold. De nieuwe software mag alleen worden gebruikt als deze voldoet aan de beveiligingseisen die het Ministerie van Defensie aan IT-systemen stelt. Dit komt nader aan de orde in § 4.1.

Het is de bedoeling dat het eigenaarschap van het selfservicesysteem wordt overgedragen aan Schiphol N.V. Op dat moment ligt de verantwoordelijkheid voor de cybersecurity bij Schiphol N.V. en heeft de minister van JenV alleen nog een beleidsmatige rol: bijvoorbeeld bij het stellen van normen voor de betrouwbaarheid van de biometrische controle. Wij hebben geconstateerd dat er geen wettelijke beperkingen gelden voor het overdragen van IT-eigenaarschap bij vitale overheidstaken zoals grenstoezicht aan partijen met commerciële belangen. De Wet beveiliging netwerken en infrastructuur (Wbni) en het toezicht daarop moeten borgen dat de onderliggende IT van essentiële diensten voldoende weerbaar is tegen cybersecuritydreigingen. Gezien het aantal betrokken partijen en de verschillende belangen in een zich ontwikkelende technische omgeving, vinden we het belangrijk dat de cybersecurity gewaarborgd is bij de voorgenomen overdracht naar Schiphol N.V.

4 Preventieve cybersecuritymaatregelen grenstoezicht

In dit hoofdstuk gaan we in op de preventieve cybersecuritymaatregelen rond het grenstoezicht. We hebben ons gefocust op het Ministerie van Defensie omdat de Koninklijke Marechaussee (KMar) op grond van de Wet beveiliging netwerk- en informatiesystemen (Wbni) is aangewezen als essentiële dienstverlener voor het grenstoezicht. We toetsen in vier paragrafen achtereenvolgens in hoeverre het Ministerie van Defensie bij het grenstoezicht:

1. op basis van risico's beveiligingsmaatregelen voor IT-systemen opstelt en realiseert (§ 4.1),
2. verantwoordelijkheden belegt en overlegstructuren inricht rondom cybersecurity (§ 4.2),
3. inzicht en overzicht heeft van de IT-systemen van het grenstoezicht, hun technische kenmerken en onderlinge relaties (§ 4.3),
4. afhankelijkheden met externe partijen beheerst (§ 4.4).

4.1 Cybersecurityeisen IT-systemen van het grenstoezicht

Van twee van de drie IT-systemen van het grenstoezicht is door de eigenaren ervan niet vastgesteld dat ze afdoende beveiligd zijn tegen cyberaanvallen. Het systeem voor de balie en de selfservice hebben de goedkeuringsprocedure van het Ministerie van Defensie om dit vast te stellen niet geheel doorlopen. Daardoor is het onzeker of deze twee systemen voldoende weerbaar zijn tegen cyberaanvallen.

4.1.1 Ministerie van Defensie kent een goedkeuringsprocedure voor IT-systemen

Het op basis van risico's beveiligen van IT-systemen is van belang om cybersecurityrisico's zo klein mogelijk te houden, zonder onnodige maatregelen te nemen. Binnen de Defensieorganisatie mogen belangrijke IT-systemen pas in gebruik worden genomen wanneer is vastgesteld dat ze voldoende weerbaar zijn tegen cyberaanvallen. Hierbij geldt een goedkeuringsprocedure van vier stappen:

1. Vaststellen van het benodigde niveau van betrouwbaarheid.
2. Vaststellen van de beveiligingseisen en -maatregelen op basis van het benodigde niveau van betrouwbaarheid.
3. Treffen van de beveiligingsmaatregelen.
4. Geven van goedkeuring voor ingebruikname van het IT-systeem ('accreditatie').

Defensie schat cybersecurityrisico's in op basis van dreigingsinformatie

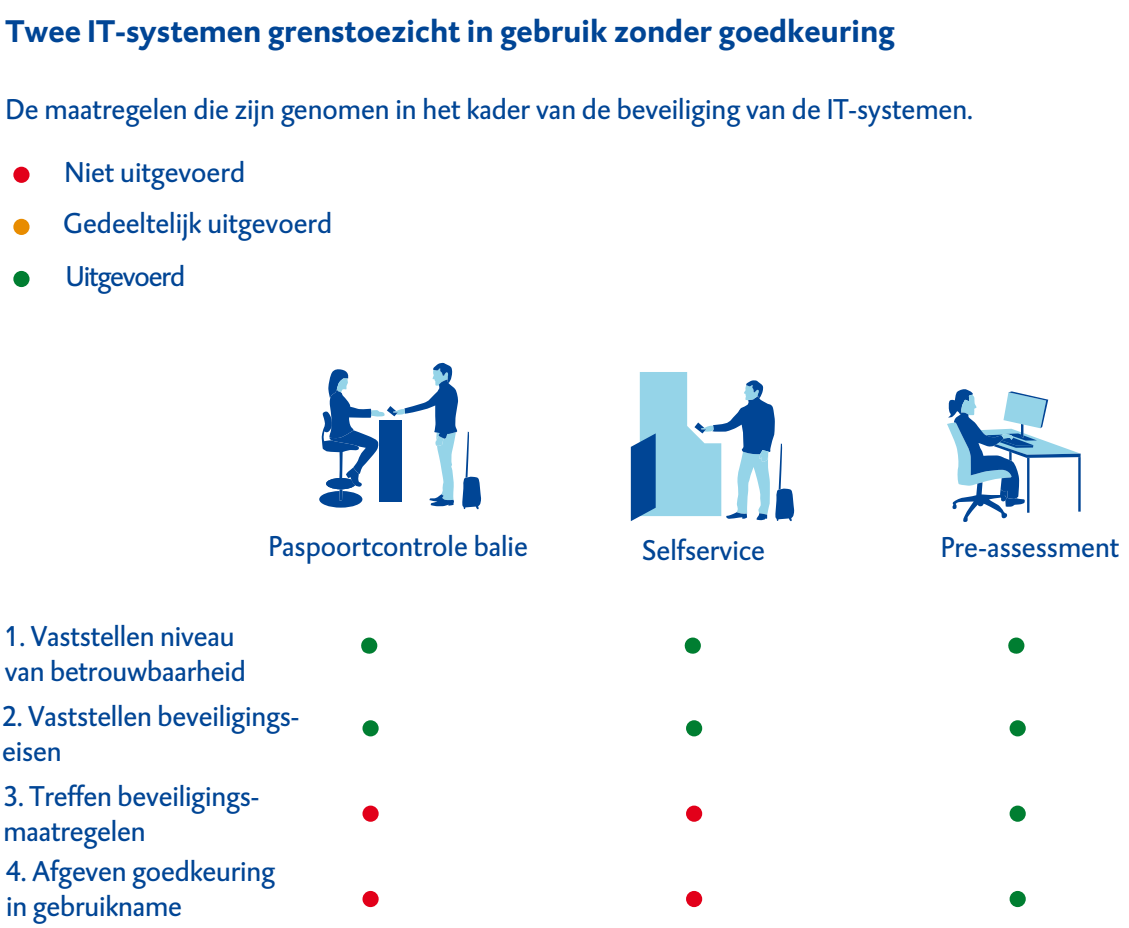
Het Ministerie van Defensie betrekt vanuit verschillende bronnen cybersecurity-dreigingsinformatie en weegt de risico's daarvan op een gestructureerde wijze. Dit is belangrijk omdat het helpt om efficiënt om te gaan met middelen en voldoende (maar geen onnodige) beveiligingsmaatregelen te nemen. Belangrijke informatiebronnen om de dreiging van cyberaanvallen mee in te schatten zijn:

- de Militaire Inlichtingen en Veiligheidsdienst (MIVD),
- het Nationaal Cyber Security Centrum (NCSC)[8] ,
- partners in externe samenwerkingsverbanden (zie § 4.2.2).

Het Ministerie van Defensie gebruikt de verzamelde dreigingsinformatie op verschillende manieren, bijvoorbeeld in het Defensie-daderprofiel: een document dat verschillende soorten tegenstanders beschrijft en inzicht biedt in hun motieven en werkwijzen, waaronder gebruik van cyberaanvallen. De dreigingsinformatie wordt ook gebruikt bij het vaststellen van het benodigde niveau van betrouwbaarheid binnen de goedkeuringsprocedure van IT-systemen.

4.1.2 Twee IT-systemen grenstoezicht in gebruik zonder goedkeuring

Uitkomst van ons onderzoek is dat twee IT-systemen van het grenstoezicht de goedkeuringsprocedure niet volledig hebben doorlopen. Voor het systeem bij de KMar-balie is goedkeuring vereist vanuit het Defensiebeveiligingsbeleid. Het IT-systeem voor selfservice op Schiphol valt niet onder het Defensiebeveiligingsbeleid, het Ministerie van JenV is immers eigenaar. Voor dit systeem is echter afgesproken dat de goedkeuringsprocedure conform het Defensiebeveiligingsbeleid moet worden doorlopen. Het is onzeker of de systemen bij de balie en selfservice afdoende beschermd zijn tegen cyberaanvallen omdat niet is vastgesteld in hoeverre de benodigde beveiligingsmaatregelen zijn getroffen.



Figuur 5 *Goedkeuringsprocedure IT-systemen grenstoezicht*

IT-systeem pre-assessment

De goedkeuringsprocedure voor het systeem voor pre-assessment is doorlopen en de meeste maatregelen zijn geïmplementeerd. Maar de goedkeuring voor ingebruikname van het IT-systeem is afgegeven zonder dat beveiligingstesten zijn uitgevoerd en zonder dat het IT-systeem aangesloten is op de detectiecapaciteit van het Defensie SOC om cyberaanvallen snel te detecteren (zie hoofdstuk 5). Beide maatregelen waren wel door Defensie-experts geadviseerd.

IT-systeem bij de balie

Het IT-systeem bij de balie is opgebouwd uit bestaande en nieuwe componenten. Voor gebruik van de bestaande componenten heeft het Ministerie van Defensie eerder goedkeuring afgegeven. Het Ministerie van Defensie heeft besloten het systeem bij de balie als nieuw informatiesysteem te beschouwen. Begin 2019 is de goedkeuringsprocedure voor ingebruikname gestart. Er is vastgesteld wat het niveau van betrouwbaarheid behoort te zijn en welke beveiligingsmaatregelen daarbij horen, maar deze maatregelen moeten nog

worden uitgevoerd. Hiervoor was ten tijde van het onderzoek nog geen planning bekend. Het IT-systeem is operationeel zonder dat de goedkeuringsprocedure is afgerond. Hierdoor loopt de samenleving het risico dat het baliesysteem kwetsbaar is voor cyberaanvallen. De Algemene Rekenkamer heeft in eerder onderzoek in 2019 al gewezen op het feit dat binnen Defensie belangrijke IT-systemen operationeel zijn zonder de vereiste goedkeuring (Algemene Rekenkamer, 2019b).

IT-systeem Self Service Passport Control

Als benoemd in § 3.3 kent het project dat een nieuwe softwareversie voor het selfservice-systeem realiseert vele betrokkenen met verschillende verantwoordelijkheden. Voorop staat dat het Ministerie van JenV eigenaar is van de nu operationele software en verantwoordelijk is voor de cybersecurity van dit systeem. Begin 2017 heeft de KMar geadviseerd voor het selfservicesysteem de goedkeuringsprocedure voor IT-systemen te doorlopen conform het Defensie-beveiligingsbeleid. Belangrijke reden hiervoor was dat de KMar de wettelijke verwerkingsverantwoordelijke is van persoonsgegevens die met het systeem verwerkt worden. Door de goedkeuringsprocedure te doorlopen zijn er meer garanties dat deze verwerking veilig plaatsvindt.

In het voorjaar van 2019 is gestart met het doorlopen van de goedkeuringsprocedure. De beveiligingsmaatregelen zijn inmiddels vastgesteld. Schiphol N.V. gaat deze maatregelen, als toekomstig eigenaar, uitvoeren. De Defensie-organisatie geeft hierbij advies en ondersteuning. Uiteindelijk zal de beveiligingsautoriteit van het Ministerie van JenV de formele toestemming voor ingebruikname afgeven.

Schiphol N.V. controleerde in het najaar van 2019 de naleving van 52 beveiligingseisen. Aan 23 eisen werd nog niet voldaan. Aan 8 eisen was gedeeltelijk voldaan, maar nog niet in voldoende mate. Aan 21 eisen werd volgens Schiphol N.V. voldaan, maar dit was nog niet door het Ministerie van Defensie geverifieerd.

Het Ministerie van JenV heeft tweemaal een tijdelijke goedkeuring afgegeven voor het selfservicesysteem. De opgestelde verbeterplannen bij deze tijdelijk goedkeuringen zijn nooit gerealiseerd. Sinds 1 juni 2018 is de laatste tijdelijke goedkeuring verlopen. De software is dus sindsdien operationeel zonder garantie dat aan de benodigde beveiligingseisen wordt voldaan. Zonder (tijdelijke) goedkeuring is niet duidelijk hoe groot de risico's hierbij zijn en of deze aanvaardbaar zijn of actie vereisen. Gezien de risico's op kwetsbaarheden voor cyberaanvallen is dit naar onze opvatting onbegrijpelijk.

4.2 Cybersecurity en de Defensie-organisatie

Binnen de Defensie organisatie zijn de taken voor cybersecurity duidelijk belegd. Ook is er een goed gedocumenteerd cybersecuritybeleid aanwezig en bestaan er overlegstructuren waarin interne en externe partijen afstemmen. Dit helpt het Ministerie van Defensie cybersecurityrisico's te beheersen.

4.2.1 Cybersecuritybeleid aanwezig en verantwoordelijkheden belegd

In de IT- en cybersecuritystrategie van het Ministerie van Defensie is oog voor de opkomende dreiging van cyberaanvallen. De cybersecuritystrategie benoemt specifiek de groeiende digitale risico's bij het grenstoezicht. De strategie is vertaald in het Defensie-beveiligingsbeleid: een gestructureerde set procedures en instructies die gezamenlijk beschrijven hoe er met cybersecurity moet worden omgegaan en wie waarvoor verantwoordelijk is.

In de Hoofddirectie Bedrijfsvoering (HDBV) zijn enkele sleutelrollen op gebied van IT en cybersecurity belegd: de Defensie-beveiligingsautoriteit (BA), de Chief Information Officer (CIO) en de Chief Information Security Officer (CISO). Ook was er ten tijde van dit onderzoek binnen HDBV een *CIO-office* van ongeveer 17 medewerkers in oprichting waar CIO en CISO onderdeel van uitmaken.

De commandant van de KMar is verantwoordelijk voor de operationele uitvoering van de grenstoezichtstaken binnen de kaders die de HDBV stelt. De commandant wordt hierbij ondersteund door een beveiligingscoördinator (BC). Deze zorgt als adviseur dat de centraal vastgelegde kaders ook decentraal worden nageleefd. De BC werd ten tijde van het onderzoek ondersteund door twee stafadviseurs met specifieke kennis van cybersecurity.

Het Joint IV Commando (JIVC) is de IT-leverancier van het Ministerie van Defensie. Het onderdeel heeft als taak de ontwikkeling en het beheer van alle IT-middelen. Onder het JIVC valt het Defensie Cyber Security Commando (DCSC) dat zich bezig houdt met defensieve cybertaken zoals preventie en detectie van cyberaanvallen (zie hoofdstuk 5). Het DCSC bestaat uit twee onderdelen met een adviserende rol:

- Het *Security Intelligence Operations Center*, SIOC (49 medewerkers)
- Het Defensie *Computer Emergency Response Team*, DefCERT (38 medewerkers).

4.2.2 Afstemming over cybersecurity vindt georganiseerd plaats

Vanwege de afhankelijkheden binnen het grenstoezicht en snelle technologische ontwikkelingen is overleg en kennisdeling op het gebied van cybersecurity belangrijk. Binnen Defensie zelf zijn een *Cyber Governance Board* (CBG) en een *IT-Governance Board*

(ITGB) opgezet. Aan beide overleggen nemen de verschillende krijgsmachtonderdelen (waaronder de KMar) en relevante IT-verantwoordelijken deel. In deze overleggen wordt bijvoorbeeld gesproken over de uitwerking van de Defensie-cyberstrategie, de veiligheid van IT-infrastructuur en de toepassing van cryptografie. Van beide overleggen hebben wij verslagen en stukken ingezien, waaruit blijkt dat ze actief zijn en afgesproken activiteiten worden opgepakt.

De KMar voert het grenstoezicht op Schiphol uit in een omgeving met verschillende externe partijen zoals vrachtvervoerders, particuliere beveiligers en de Douane. Op het gebied van cybersecurity neemt de KMar daarom deel in het Airport- Information Sharing and Analysis Centre (Airport-ISAC) en het Platform Beveiliging Publieke en Private Veiligheid Schiphol (BPVS). Uit stukken en verslagen blijkt dat de deelnemende partijen actief kennis uitwisselen, bijvoorbeeld over hoe wordt omgegaan met telefoons en laptops bij buitenlandse dienstreizen van medewerkers van het Ministerie van Defensie.

4.3 Inzicht in IT-middelen

Binnen de Defensie-organisatie is het centrale overzicht van de IT-systemen voor het grenstoezicht nog niet op het gewenste niveau. Het hebben van een overzicht van de IT-systemen, hun kenmerken en onderlinge relaties is belangrijk. Met het overzicht kan het Ministerie van Defensie bij een cyberaanval of ontdekte digitale kwetsbaarheid snel inzicht in de impact verkrijgen en gericht reageren. Bij het Ministerie van Defensie is dit inzicht momenteel nog niet centraal, volledig en actueel aanwezig.

Het Ministerie van Defensie streeft naar centrale overzichten van alle IT-applicaties en diensten van het grenstoezicht. De overzichten geven inzicht in de onderlinge relaties tussen applicatie en diensten. Ook tonen ze technische details over de systemen en informatie over het soort informatie dat ermee verwerkt wordt (bijvoorbeeld vertrouwelijke informatie of bijzondere categorieën van persoonsgegevens). De informatie wordt uit verschillende onderliggende administraties verzameld via koppelingen. De centrale overzichten voor het grenstoezicht zijn in 2019 in gebruik genomen en waren tijdens ons onderzoek nog in ontwikkeling. We zien de volgende problemen:

- Niet alle koppelingen met onderliggende administraties zijn gelegd, waardoor niet alle beschikbare informatie centraal wordt getoond. Hierdoor ontbreekt nog informatie in het centrale beeld.
- Sommige informatie op de overzichten is niet eenduidig omdat er niet-vergelijkbare informatie onder dezelfde noemer wordt weergegeven. Hierdoor kan verwarring ontstaan over de juistheid van informatie.

- De werkafspraken over de overzichten en onderliggende administraties zijn nog in ontwikkeling. Zo waren verantwoordelijkheden op onderdelen nog aan individuen gekoppeld in plaats van aan (persoonsonafhankelijke) rollen. Hierdoor loopt Defensie het risico dat de overzichten niet goed onderhouden worden.

Bij het reageren op een IT-incident of calamiteit (al dan niet veroorzaakt door een cyber-aanval) kunnen de overzichten gebruikt worden om de impact te bepalen. Het belang daarvan bleek in 2018 bij een grote verstoring in een belangrijk generiek IT-onderdeel van het Ministerie van Defensie die ook het grenstoezicht raakte. In het evaluatieverslag van de respons op deze verstoring staat dat het ingewikkeld was om vast te stellen welke IT-onderdelen en dienstverlening daadwerkelijk geraakt werden door de verstoring. In de evaluatie wordt daarom aanbevolen om software aan te schaffen om kenmerken en onderlinge verbanden van de IT-infrastructuur centraal in vast te leggen.

4.4 Beheersen afhankelijkheden externe partijen

De IT-systemen van het grenstoezicht worden (deels) door externe leveranciers ontwikkeld. Via de Algemene Beveiligingseisen Defensieopdrachten (ABDO) stelt het Ministerie van Defensie eisen aan de (cyber)veiligheid van bedrijven waar ze mee samenwerkt. De MIVD is verantwoordelijk voor het autoriseren van potentiële leveranciers. Zo heeft de leverancier van de software voor selfservice een ABDO-autorisatie. Een van de punten die daarbij is afgedwongen, is dat de (buitenlandse) leverancier geen toegang op afstand heeft tot de productie-omgeving in Nederland.

Het grenstoezicht is daarnaast afhankelijk van de beschikbaarheid van externe registraties en diensten voor de controles bij pre-assessment, balie en selfservice. Voor de belangrijke afhankelijkheden bestaan afspraken met de leverancier van de gegevens over de beschikbaarheid en ondersteuning bij storingen. Om de restrisico's verder te verkleinen, heeft de KMar een lokale digitale kopie van opsporingsregisters voor het geval deze niet live geraadpleegd kunnen worden. Deze kopie is uiteraard minder actueel dan de eigenlijke registers maar dekt de risico's volgens ons afdoende af.

5 Detectie van cyberaanvallen en kwetsbaarheden

In dit hoofdstuk gaan we in op het opsporen van kwetsbaarheden in IT-systemen van het grenstoezicht en het snel detecteren van (mogelijke) cyberaanvallen. We toetsen in twee paragrafen achtereenvolgens in hoeverre het Ministerie van Defensie bij het grenstoezicht:

- cyberaanvallen detecteert door het gedrag van IT-systemen te monitoren (§ 5.1) en
- kwetsbaarheden opspoort met beveiligingstests (§ 5.2).

Bij de beveiligingstest staan we stil bij twee casussen: een beveiligingstest op het selfservicesysteem (§ 5.3) en een test, uitgevoerd in het kader van dit onderzoek, op het systeem voor pre-assessment (§ 5.4).

5.1 Cyberaanvallen detecteren met monitoring op afwijkend gedrag

Het Ministerie van Defensie beschikt over de mogelijkheid om cyberaanvallen snel te detecteren. De IT-systemen van het grenstoezicht zijn echter niet op deze detectiecapaciteit aangesloten. Daardoor is er een risico dat cyberaanvallen op deze systemen niet of niet snel genoeg opgemerkt worden door het Ministerie van Defensie.

5.1.1 Ministerie van Defensie heeft de middelen om cyberaanvallen snel te detecteren

Het Ministerie van Defensie is in staat IT-systemen op afwijkend gedrag te monitoren om zo (mogelijke) cyberaanvallen snel te detecteren, de impact vast te stellen en indien nodig maatregelen te treffen. Afwijkend gedrag van IT-systemen, zoals het genereren van grote hoeveelheden dataverkeer of een reeks mislukte inlogpogingen, kunnen duiden op een cyberaanval. Het is daarom van belang het gedrag van IT-systemen te monitoren op dit soort afwijkingen.

Het Security Intelligence Operations Center van Defensie

Organisaties beleggen het detecteren van afwijkend gedrag in IT-systemen over het algemeen bij een specialistische afdeling: een *Security Operations Center* (SOC). Het SOC van het Ministerie van Defensie heet SIOC (*Security Intelligence Operations Centre*). Het SIOC heeft de kennis en middelen om afwijkend gedrag te detecteren (hierna: detectiecapaciteit).

Het SIOC maakt gebruik van zogenaamde *security information and event management software*, kortweg SIEM. Het SIEM van het Ministerie van Defensie monitort geautomatiseerd of er sprake is van afwijkend gedrag bij de aangesloten IT-systemen.

5.1.2 Systemen grenstoezicht niet aangesloten op het SIOC

De IT-systemen van het grenstoezicht waarvoor het Ministerie van Defensie verantwoordelijk is, zijn niet individueel aangesloten op detectiecapaciteit van het SIOC. Het selfservicesysteem waar het Ministerie van JenV verantwoordelijk voor is, is ook niet aangesloten op detectiecapaciteit van een SOC. Het is ons niet duidelijk geworden waarom deze systemen niet aangesloten zijn. Schiphol N.V. beschikt over een SOC en zal het selfservicesysteem, zodra zij eigenaar zijn, wel gaan monitoren.

De besturingssystemen waar het Ministerie van Defensie gebruik van maakt, zijn wel aangesloten op de detectiecapaciteit. Hetzelfde geldt voor het koppelvlak waarmee de systemen van het grenstoezicht met de buitenwereld communiceren. Hierdoor is de kans groot dat een cyberaanval van buitenaf op de systemen van het grenstoezicht snel wordt opgemerkt. Doordat de drie grenstoezichtsystemen niet zijn aangesloten op de detectiecapaciteit van het SIOC is de kans kleiner dat het Ministerie van Defensie een directe aanval van binnenuit snel opmerkt. Daarmee ontbreekt bij het Ministerie van Defensie een adequate maatregel om dit type aanval op een vitaal proces tijdig te signaleren. Dit aanvalsscenario is door ons getest in een beveiligingstest voor dit onderzoek (zie § 5.4).

Het SIOC heeft een planning waarin staat welke (onderdelen van) IT-systemen het SIOC tussen het vierde kwartaal 2019 en het vierde kwartaal 2020 gaat aansluiten op de detectiecapaciteit van het SIOC. In die planning zijn de drie IT-systemen van het grenstoezicht niet opgenomen. Dit terwijl het Ministerie van Defensie in haar Cyber Strategie 2018 al specifiek de risico's van de gedigitaliseerde grensprocessen noemde.[9]

Het is naar ons oordeel zorgwekkend dat het IT-systeem voor pre-assessment niet is aangesloten op de detectiecapaciteit van het SIOC en dat het blijkens de planning ook niet snel aangesloten wordt. Aansluiting was namelijk één van de vastgestelde beveiligingsmaatregelen uit de goedkeuringsprocedure van dat systeem (zie § 4.1.1). Bovendien staat het systeem vermeld op de lijst met kritieke IT-systemen van het Ministerie van Defensie, waarmee het wordt beschouwd als essentieel voor de inzet van Defensie-eenheden.

5.1.3 Nog geen verbetercyclus voor detectieprocessen

We constateren dat het Ministerie van Defensie een begin heeft gemaakt met het evalueren en verbeteren van de detectieprocessen. Er is nog geen sprake van een planmatige werkwijze op basis waarvan Defensie de processen verder kan ontwikkelen en verbeteren.

Het SIOC heeft procesbeschrijvingen rond de detectiecapaciteit vastgelegd. Het Ministerie van Defensie kan ze daardoor evalueren en indien nodig effectiever en efficiënter maken.

Het SIOC zit nog in het beginstadium van het evalueren van de detectieprocessen om deze effectiever te laten werken. Bij het afhandelen van een melding vanuit het SIEM evalueert het SIOC in hoeverre het SIEM goed gewerkt heeft. Zo kan het SIOC de configuratie bijstellen als het SIEM veel onterechte meldingen afgeeft. Zolang de drie systemen van het grenstoezicht niet zijn aangesloten op de detentiecapaciteit van het SIOC, zijn er echter geen meldingen om te evalueren.

5.2 Kwetsbaarheden opsporen met beveiligingstesten

De Defensie-organisatie beschikt over de kennis en kunde om IT-beveiligingstesten uit te voeren. In het Defensiebeveiligingsbeleid staat dat deze testen jaarlijks moeten plaatsvinden. In de praktijk bleken twee van de drie IT-systemen nog nooit getest op beveiliging. Het derde IT-systeem van selfservice was eenmaal getest, met een veel beperktere scope dan gepland. Hierdoor bestaat het risico dat aanvallers misbruik maken van onopgemerkte kwetsbaarheden in de drie IT-systemen.

5.2.1 Het Ministerie van Defensie heeft kennis en middelen om beveiligingstesten te doen

Het Ministerie van Defensie beschikt met het Defensie *Computer Emergency Response Team* (DefCERT) over een interne partij met de juiste technische kennis en middelen voor beveiligingstesten. Het is voor cybersecurity belangrijk dat organisaties actief kwetsbaarheden, zoals bijvoorbeeld gebruik van zwakke wachtwoorden of verouderde software, opsporen via periodieke beveiligingstesten.

Het Ministerie van Defensie onderschrijft het belang van beveiligingstesten. In het beveiligingsbeleid van het Ministerie van Defensie is de volgende passage opgenomen: *"Informatiesystemen worden jaarlijks gecontroleerd op technische naleving van beveiligingsnormen en risico's ten aanzien van de feitelijke veiligheid. Dit kan bijvoorbeeld door (geautomatiseerde) kwetsbaarheidsanalyses of pentesten."*

Beveiligingstesten: kwetsbaarheden vinden en uitbuiten

Beveiliging is een van de aspecten van IT-systemen die getest moeten worden om de kwaliteit ervan te waarborgen. In een beveiligingstest onderzoeken testers hoe kwetsbaar een IT-systeem is voor misbruik en/of hoe effectief de beveiligingsmaatregelen zijn. Een belangrijk onderscheid[10] in beveiligingstesten is dat tussen:

- kwetsbaarheidsanalyses, waarmee onderzocht wordt welke kwetsbaarheden het systeem kent die een aanvaller mogelijk uit kan buiten en
- pentesten, waarmee geprobeerd wordt kwetsbaarheden uit te buiten ten koste van de beschikbaarheid, integriteit (betrouwbaarheid) of vertrouwelijkheid van het IT-systeem.

In beveiligingstesten gevonden kwetsbaarheden worden gekoppeld aan een risicocategorie, afhankelijk van de kans dat de kwetsbaarheid wordt misbruikt en de impact van misbruik. Defensie hanteert de categorieën 'laag', 'gemiddeld', 'hoog' en 'kritiek', waarbij 'kritiek' een eenvoudig uit te buiten kwetsbaarheid is die grote gevolgen kan hebben.

Beveiligingstesten door DefCERT

Binnen Defensie is de afdeling DefCERT de aangewezen partij voor de uitvoering van beveiligingstesten. DefCERT biedt in opdracht verschillende soorten beveiligingstesten aan zoals documentatiereviews, advies bij nieuwe projecten en kwetsbaarheids- en pentesten, waarbij fysieke beveiliging ook een onderdeel kan zijn. DefCERT stelt voor een opdracht een team samen uit adviseurs en analisten. Wij hebben voor ons onderzoek gesproken met medewerkers van DefCERT en rapporten en plannen van aanpak voor beveiligingstesten ingezien. Ook hebben we DefCERT zien opereren in de voor dit onderzoek uitgevoerde beveiligingstest. Hieruit blijkt dat DefCERT een professionele en kundige partij is voor het uitvoeren van beveiligingstesten.

Kwetsbaarheidsanalyses door SIOC

Het SIOC doet vanuit de detectiecapaciteit (zie § 5.1) ook kwetsbaarheidsanalyses (*vulnerability scans*) op aangesloten IT-systemen. Daarbij controleert het SIOC bijvoorbeeld geautomatiseerd of belangrijke updates zijn gedaan en virusscanners actief zijn. De drie IT-systemen van het grenstoezicht zijn echter niet aangesloten op het SIOC. Voor deze systemen doet het SIOC dus geen kwetsbaarheidsanalyses.

5.2.2 Beveiligingstesten grenstoezicht beperkt in opzet en qua opvolging

Hoewel het Ministerie van Defensie in het beveiligingsbeleid jaarlijkse beveiligingstesten voorschrijft, blijkt dat deze testen in de praktijk in zeer beperkte mate plaatsvinden. Ook laat de opvolging van de aanbevelingen te wensen over.

Wij hebben onderzocht in hoeverre beveiligingstesten in de praktijk ook plaatsvinden op de drie IT-systemen van het grenstoezicht. Hierbij bleek dat alleen voor het systeem van selfservice beveiligingstesten waren uitgevoerd. In 2018 voerde een partij in opdracht van het Ministerie van JenV een beveiligingsanalyse uit op de nieuwe software van het self-servicesysteem. Dit was een documentenanalyse waarbij alle technische documenten van het selfservicesysteem beoordeeld zijn op beveiligingsaspecten. Uit het rapport dat wij hebben ingezien blijkt dat in deze analyse geen kritieke risico's naar voren kwamen.[11] Daarnaast heeft DefCERT in 2018 een beveiligingstest op de software van het selfservice-systeem uitgevoerd. We bespreken deze test als casus in § 5.3.

Op de IT-systemen van het pre-assessment en de balie zijn de (conform het Defensie-beveiligingsbeleid voorgeschreven) beveiligingstesten nog nooit gedaan. Voor dit onderzoek hebben wij een beveiligingstest geïnitieerd op het IT-systeem van het pre-assessment. Deze test is uitgevoerd door DefCERT. Opzet en resultaten van de test zijn als casus opgenomen in § 5.4.

5.3 Casus beveiligingstest op Self Service Passport Control

Opzet en uitvoering door DefCERT en betrokken partijen
In 2018 voerde DefCERT in opdracht van het Ministerie van Defensie een beveiligingstest uit op het systeem van *Self Service Passport Control* (SSPC). Aanleiding was de nieuwe versie van de software die het selfserviceproject realiseert. Het ontwerpen en uitvoeren van de beveiligingstest verliep moeizaam door de noodzakelijke afstemming met de vele partijen in het selfserviceproject, het beperkte inzicht vooraf en de beperkte capaciteit bij de betrokken partijen. De partijen stelden gezamenlijk de scope van de test en een plan van aanpak vast. Tijdens de uitvoeringsfase van de test kon DefCERT:

- een IT-onderdeel van Schiphol N.V. niet conform plan testen omdat Schiphol N.V. een risico zag voor de continuïteit van de luchthaven,
- een specifieke koppeling niet testen omdat het Ministerie van Justitie en Veiligheid de medewerking hiervoor vlak voor aanvang van de test introk,
- niet de nieuwste softwareversie testen omdat de ontwikkelaars gedurende de test verder werkten aan de nieuwe software. De nieuwste software is dus nooit getest, terwijl dit juist de aanleiding van de test was.

Gevonden kwetsbaarheden, conclusies en aanbevelingen van DefCERT
DefCERT concludeerde dat er met de aangepaste en flink beperkte scope geen kwetsbaarheden van het kritieke niveau in de software naar voren waren gekomen. Er werden in totaal 12 kwetsbaarheden gevonden, waaronder 1 met de risicocategorie 'hoog', 7 'gemiddeld' en 3 'laag'. Voorbeelden van (inmiddels opgeloste) kwetsbaarheden waren het gebruik van eenvoudige wachtwoorden en niet bijgewerkte software. Om aanbevelingen te doen over de gehele status van het selfserviceproject en de definitieve implementatie van de nieuwe versie achtte DefCERT echter extra onderzoek nodig. Voor de overdracht van het selfservicesysteem aan Schiphol N.V. (zie § 3.3) is een akkoord vanuit het Ministerie van Defensie noodzakelijk. Hierin speelt het advies vanuit DefCERT een belangrijke rol.

Opvolging van bevindingen en aanbevelingen
Het hoofd van DefCERT heeft de eindrapportage met de gevonden kwetsbaarheden en aanbevelingen aangeboden aan de interne opdrachtgever van de test. Voor het opvolgen van de aanbevelingen waren verschillende betrokken partijen verantwoordelijk. In 2019 heeft DefCERT de bevindingen uit het onderzoek uit 2018 opnieuw getest om te controleren of de risico's waren weggenomen. DefCERT testte 10 van de 12 gevonden kwetsbaarheden uit 2018 opnieuw, daarbij bleken:

- van 3 kwetsbaarheden de aanbevelingen opgevolgd,
- van 7 kwetsbaarheden de aanbevelingen niet opgevolgd en de risico's door het Ministerie van JenV tijdelijk geaccepteerd.

Van de 7 niet opgevolgde kwetsbaarheden heeft 1 kwetsbaarheid de risicocategorie 'hoog' en 3 de risicocategorie 'gemiddeld'. Deze hebben alle te maken met de toegangsbeveiliging en gebruikersrechten bij het selfservicesysteem. DefCERT geeft aan dat de geadviseerde termijnen voor opvolgen van de aanbevelingen niet is opgevolgd. De 7 nog op te volgen aanbevelingen liggen bij Schiphol N.V. en de softwareleverancier. Het Ministerie van JenV is als eigenaar verantwoordelijk dat dit gebeurt.

5.4 Casus beveiligingstest op IT-systeem pre-assessment door de Algemene Rekenkamer

Opzet en uitvoering door Algemene Rekenkamer en DefCERT
De Algemene Rekenkamer heeft voor dit onderzoek een beveiligingstest geïnitieerd op het IT-systeem van pre-assessment. De test is uitgevoerd door DefCERT. Hoewel het Defensie-beveiligingsbeleid jaarlijkse testen voorschrijft, was op het systeem van pre-assessment nog nooit een beveiligingstest gedaan door het Ministerie van Defensie. Uitgangspunt van de test vormde de *insider threat*: een cyberaanval via een Defensie-medewerker die toegang heeft tot het netwerk van het Ministerie van Defensie, maar niet geautoriseerd is voor het systeem voor pre-assessment. We wilden juist dit scenario toetsen omdat daarmee belangrijke hordes voor een aanvaller, zoals toegang tot het netwerk van het Ministerie van Defensie of toegang tot een fysieke Defensielocatie, genomen zijn. Tegelijkertijd is een cyberaanval via een Defensiemede-werker niet onrealistisch: het Ministerie van Defensie heeft circa 60.000 medewerkers en een 'interne dader' is ook specifiek als dreiging benoemd in het Defensiebeveiligingsbeleid. Wij wilden onderzoeken of het voor iemand binnen de organisatie mogelijk was ongeautoriseerd toegang te krijgen tot het IT-systeem van pre-assessment, en vervolgens de werking van het systeem te manipuleren en/of (persoons)gegevens in te zien of aan te passen.

DefCERT heeft op initiatief van de Algemene Rekenkamer samen met andere betrokkenen binnen het Ministerie van Defensie een plan van aanpak voor deze beveiligingstest geschreven. Onderdeel van de test waren zowel een kwetsbaarheidstest (het zoeken naar kwetsbaarheden) als een penetratietest (kwetsbaarheden proberen te misbruiken). DefCERT voerde de test in november 2019 uit op een locatie van het Ministerie van Defensie. De resultaten van de test zijn gelijktijdig en ongefilterd met zowel de Algemene Rekenkamer als het Ministerie van Defensie gedeeld.

Bevindingen, conclusies en aanbevelingen van DefCERT
De test is conform het plan van aanpak uitgevoerd. DefCERT heeft in de test 11 kwetsbaarheden aangetroffen in het IT-systeem van pre-assessment. Geen daarvan was 'kritiek', 5 waren 'hoog', 3 'gemiddeld' en 3 'laag'. Voorbeelden van (inmiddels opgeloste) kwetsbaarheden waren;

- Het gebruik van een standaard wachtwoord dat via de (met Google te vinden) gebruikers handleiding van het systeem te achterhalen was.
- De mogelijkheid om beheerrechten toe te kennen en daarmee controle over een server in het centrale beheerplatform van het Ministerie van Defensie te krijgen. Op dit platform zijn honderden (waaronder ook kritieke) applicaties van het Ministerie van Defensie aangesloten.
- Het versturen van e-mails uit naam van willekeurige Defensie-medewerkers, zoals bijvoor-beeld de Commandant der Strijdkrachten. Dergelijk e-mails kunnen er, doordat de ontvanger de afzender denkt te kennen, betrouwbaar uitzien en gebruikers verleiden op malafide hyperlinks te klikken.
- Het gebruik van oude softwarepakketten (waarvan één sinds 2016 niet meer ondersteund werd) en waar dus ook geen beveiligingsupdates meer voor verschijnen.

Een belangrijke conclusie was dat DefCERT aangaf enkele kwetsbaarheden te kunnen combineren om toegang te verkrijgen tot het systeem van pre-assessment en de werking van het systeem te beïnvloeden. In dit scenario zou een aanvaller passagiersgegevens kunnen inzien. Het zou via een complexe aanval ook mogelijk zijn om voor een *false negative* te zorgen: dat wil zeggen dat het systeem aangeeft dat een passagier niet op een opsporingslijst staat terwijl dit wel het geval is. De risico's van een *false negative* in het pre-assessment worden beperkt doordat de KMar bij de grensdoorlaatpost opnieuw controleert of passagiers op opsporingslijsten staan. De geautomatiseerde controle of een passagier op basis van zijn kenmerken (zoals reisroute, nationaliteit en reisgezelschap) in een risicoprofiel past, doet de KMar echter uitsluitend in het pre-assessment. Door een *false negative* zou een passagier die bijvoorbeeld aan het profiel van een mensensmokkelaar voldoet minder snel opgemerkt worden. Het aanvalsscenario is niet in de praktijk gebracht, ook omdat het daarvoor nodig was Defensiemedewerkers te misleiden (*social engineering*), wat in het plan van aanpak was uitgesloten. Dat het scenario denkbaar en uitvoerbaar was, staat echter vast.

Reactie van het Ministerie van Defensie op de bevindingen en aanbevelingen beveiligingstest

De beveiligingsautoriteit van het Ministerie van Defensie heeft op basis van het rapport van DefCERT opdracht gegeven de bevindingen op te lossen. Enkele bevindingen met een hoge prioriteit zijn direct opgelost. Hierdoor was het door DefCERT gesignaleerde aanvalsscenario niet meer uitvoerbaar. Voor het oplossen van de andere bevindingen heeft Defensie een planning opgesteld. Alle acties om bevindingen met een hoge prioriteit op te lossen zijn daarbij gepland in het eerste kwartaal van 2020. Medio februari 2020 waren circa de helft van deze acties afgerond waardoor in totaal 4 van de 5 bevindingen met een hoge prioriteit waren opgelost door het Ministerie van Defensie.

6 Reactie op cyberincidenten en -crises

Dit hoofdstuk gaat in op hoe het Ministerie van Defensie reageert op incidenten en crises als gevolg van een cyberaanval. We toetsen achtereenvolgens in hoeverre er:

- procedures zijn vastgelegd voor een reactie op incidenten en crisissituaties als gevolg van een cyberaanval, of deze volledig zijn en hoe ze in de praktijk werken (§ 6.1),
- in de praktijk geoefend wordt met incidenten en crisissituaties als gevolg van een cyberaanval (§ 6.2).

Een cyberincident is een relatief kleine, geïsoleerde verstoring van het reguliere proces, veroorzaakt door een kwaadwillende derde. We spreken van een cybercrisis zodra er een langdurige en/of complexe IT-verstoring optreedt als gevolg van een cyberaanval. Een cyberincident kan zich ontwikkelen tot een cybercrisis: bijvoorbeeld in het geval van *ransomware* die zich vanaf één computer over een computernetwerk verspreidt.

Cyberincidenten en -crises in de praktijk

Het was in ons onderzoek niet mogelijk om te onderzoeken hoe het Ministerie van Defensie en de KMar hebben gereageerd op een daadwerkelijk cyberincident of -crisis, aangezien deze gedurende ons onderzoek nog niet hadden plaatsgevonden op het grenstoezicht op Schiphol. Wel was er in 2019 een grootschalige IT-storing die illustratief is voor de impact die een digitale verstoring kan hebben op de luchthavenprocessen.

In juni 2019 was het door een IT-storing niet mogelijk om te controleren of de reizigers op opsporingslijsten stonden. Hierdoor ontstonden lange wachtrijen bij de grensdoorlaatpost waardoor grote groepen reizigers hun vlucht dreigden te missen en de andere luchthavenprocessen werden verstoord. In dergelijke situaties kan de KMar, binnen de Schengenafspraken, een uitzondering maken en grote groepen passagiers met minimale controle de grens te laten passeren. Dat was in juni 2019 gedurende ruim een uur het geval. Dit is een onwenselijke situatie die de KMar altijd probeert te voorkomen, maar waar de KMar gezien alle andere belangen tijdens een crisis soms voor moet kiezen.

6.1 Procedures voor cyberincidenten en –crises

Het Ministerie van Defensie beschikt over procedures waarin staat hoe te reageren op IT-verstoringen. Hierbinnen bestaat een apart proces voor verstoringen die veroorzaakt worden door een cyberaanval. Het ontbreekt nog aan scenario's voor specifieke cyberaanvallen, zoals met gijzelsoftware. Hierdoor zien we een risico dat bij de reactie te zeer geïmproviseerd moet worden.

6.1.1 Algemene procedures IT-verstoringen zijn aanwezig

Het Ministerie van Defensie heeft uitgebreide procedures voor hoe te handelen bij een IT-verstoring. Hierdoor kunnen medewerkers terugvallen op vaste procedures en actieplannen in een onzekere en onvoorspelbare situatie. Zo wordt de grip op de situatie verstevigd en kan de Defensie-organisatie stapsgewijs aan een oplossing werken.

Defensie heeft in de procedures voor incidenten en crises doelen gesteld over hoe snel verstoringen opgelost moeten zijn. Als een systeem te lang verstoord is of er sprake is van dataverlies, zijn er procedures om op te schalen van incident naar calamiteit en mogelijk zelfs naar het crisisniveau. De rollen, taken en verantwoordelijkheden die hier bij horen zijn allemaal uitgeschreven. Ook is helder hoe de communicatie over het probleem moet verlopen en zijn er methodes om de oorzaak van het probleem te analyseren. Na afloop van een grote verstoring vindt een evaluatie plaats. Uit deze evaluaties volgen maatregelen die genomen moeten worden om te voorkomen dat hetzelfde probleem zich nog een keer voordoet.

6.1.2 Specifieke procedure voor cyberincidenten

Het Joint IV Commando (JIVC) van het Ministerie van Defensie heeft een specifieke procedure voor de reactie op een cyberincident. Die procedure moet in werking treden wanneer in de afhandeling van een incident conform de algemene procedures blijkt dat het wordt veroorzaakt door een cyberaanval. Dat de specifieke procedure bestaat, werd ons overigens pas laat in het onderzoek helder. De verschillende JIVC-medewerkers die we in eerste instantie spraken, hebben ons hier desgevraagd niet op gewezen. Blijkbaar is dit niet algemeen bekend bij het Ministerie van Defensie. Ook staat er in de algemene procedure geen expliciete verwijzing naar de specifieke procedure. Het Ministerie van Defensie geeft aan dat de bij de verstoring betrokken calamiteitenmanager verantwoordelijk is om de cyberprocedure op te starten.

In de specifieke procedure zijn geen cyberscenario's benoemd. Dit terwijl een cyberincident een organisatie voor geheel eigen dilemma's kan stellen. Bijvoorbeeld in de situatie dat systemen besmet zijn met *ransomware* en de aanvallers losgeld eisen.[12] In een gesprek met Schiphol N.V. bleek dat binnen de luchthaven specifiek op dit punt bij een crisisoefening discussie ontstond omdat er geen richtlijnen voor waren.

Andere specifieke situaties doen zich voor bij ongeautoriseerde toegang tot passagiersdata, bijvoorbeeld door cyberspionage. Het is belangrijk vooraf procedures vast te stellen over hoe te handelen in dit soort cybercrisissituaties. Bijvoorbeeld rondom het doen van een

melding bij de Autoriteit Persoonsgegevens (AP) en het informeren van personen wiens gegevens zijn ingezien.

Bij het grenstoezicht zijn verschillende publieke en private partijen betrokken. Bij het vooraf opstellen van procedures kunnen onduidelijkheden en conflicterende belangen aan het licht komen. Bijvoorbeeld tussen het commerciële belang en het veiligheidsbelang. Het is verstandig deze vooraf te bespreken en op te helderen, zodat tijdens een daadwerkelijke cybercrisis duidelijk is hoe de partijen moeten handelen en wat ze van elkaar mogen verwachten.

6.2 Praktijkoefeningen met cybersecurityincidenten en -crises

Ter voorbereiding op een cybercrisis organiseert het Ministerie van Defensie oefeningen. Ook neemt het Ministerie van Defensie deel aan door anderen georganiseerde oefeningen, bijvoorbeeld van de NAVO of het Nationaal Cyber Security Centrum (NCSC). De KMar is zich bewust van haar belangrijke rol en de mogelijke impact van een IT-verstoring op het grenstoezicht. De brigade Grensbewaking van de KMar doet elk kwartaal mee aan een crisissimulatie op Schiphol. Een cybercrisis is nog geen oefenscenario geweest en staat ook nog niet in de planning.

Het grenstoezicht van de KMar op Schiphol is onderdeel van een keten van publieke en private partijen waarbinnen continu afwegingen worden gemaakt tussen veiligheid en mobiliteit. Wanneer de grenscontrole verstoord is, kan dit impact hebben op de hele luchthaven. Een cyberaanval is een reëel risico dat de KMar en Schiphol N.V. hoogst-waarschijnlijk voor nieuwe dilemma's zal plaatsen. Wij vinden het daarom een risico dat dit scenario in de praktijk nog niet geoefend is. Bovendien kunnen zonder oefening procedures ook niet geëvalueerd en verbeterd worden.

7 Conclusies en aanbevelingen

IT speelt een cruciale rol bij het grenstoezicht op de luchthaven Schiphol. Dit belang neemt in de nabije toekomst verder toe. Uit ons onderzoek naar de cybersecurity van het grenstoezicht blijkt dat de werking van de cybersecuritymaatregelen in de praktijk nog te wensen overlaat, terwijl de benodigde kennis en procedures wel voorhanden zijn.

De risico's hiervan worden groter naarmate het gebruik van IT bij het grenstoezicht groeit. In het licht van alle technologische ontwikkelingen in de komende jaren beoordelen we het huidige niveau van cybersecurity op het grenstoezicht door de KMar op Schiphol als onvoldoende en dus niet toekomstbestendig.

Bij het grenstoezicht zijn verschillende publieke en private partijen betrokken. De partijen hebben niet altijd dezelfde belangen. Bij het selfservicesysteem zien we dat Schiphol N.V. belang heeft bij snelle doorontwikkeling terwijl de KMar als gebruiker in de eerste plaats belang hecht aan een stabiel en veilig systeem. Daarnaast is er veel afstemming nodig tussen betrokken partijen. Een gezamenlijke beveiligingstest van het selfservicesysteem verliep hierdoor moeizaam en had een kleinere scope dan beoogd. Ook bij het voldoen aan de gestelde beveiligingseisen van het selfservicesysteem zijn de partijen van elkaar afhankelijk. Het risico is dat het belang van cybersecurity ondergeschikt raakt aan de (commerciële) belangen van luchthavenoperaties.

Het grenstoezicht zal de komende jaren verder digitaliseren. De complexiteit en de afhankelijkheid van IT zal groeien met een toename van het aantal systemen, verbindingen en gegevensverzamelingen. Deels komt de digitalisering voort uit afspraken in Europees verband. Voor *Seamless Flow* is Schiphol N.V. een drijvende kracht. Schiphol neemt in de toekomst ook de rol van eigenaar van het selfservicesysteem over van het Ministerie van JenV. Met deze toekomst in gedachte is het zaak om nu een afdoende niveau van cybersecurity te waarborgen. Wij zien dat de benodigde kennis en kunde aanwezig is binnen het Ministerie van Defensie. Onze aanbevelingen komen dan ook vooral neer op daadwerkelijk doen wat al mogelijk is. Het is onbegrijpelijk dat dit tot op heden nog niet is gedaan.

Maatregelen voor beveiliging IT-systemen grenstoezicht nauwelijks genomen

De maatregelen die zijn genomen in het kader van de beveiliging van de IT-systemen.

- Niet uitgevoerd
- Gedeeltelijk uitgevoerd
- Uitgevoerd

Paspoortcontrole balie

Selfservice

Pre-assessment

	Paspoortcontrole balie	Selfservice	Pre-assessment
Eigenaar	Defensie	JenV	Defensie
Goedkeuring voor gebruik afgegeven	●	●	●
Beveiligingstesten uitgevoerd	●	●	●*
Aangesloten op detectiecapaciteit	●	●	●

* op initiatief van de Algemene Rekenkamer is deze beveiligingstest in het kader van het onderzoek alsnog uitgevoerd.

Figuur 6 *Genomen cybersecuritymaatregelen voor IT-systemen grenstoezicht*

7.1 Goedkeuring voor twee IT-systemen grenstoezicht ontbreekt

In het Defensiebeveiligingsbeleid staat dat er beveiligingsmaatregelen worden vastgesteld voor IT-systemen op basis van risicoanalyses. Belangrijke IT-systemen mogen pas in gebruik worden genomen als deze maatregelen zijn genomen. Het IT-systeem van het Ministerie van Defensie dat de KMar bij de balie op Schiphol gebruikt is echter operationeel zonder de vereiste goedkeuring. Dit wil niet zeggen dat dit systeem onveilig is, maar wel dat niet is zekergesteld dat dit wél zo is.

Het Ministerie van JenV heeft tot taak het selfservicesysteem bij de grensdoorlaatpost te organiseren. Er is afgesproken dat ook daar de goedkeuringsprocedure wordt doorlopen conform het beleid van het Ministerie van Defensie. Ook dit systeem is operationeel zonder dat de vastgestelde cybersecuritymaatregelen zijn genomen. Ook hier geldt dat er zo onzekerheid is over de weerbaarheid van het systeem tegen cyberaanvallen.

We bevelen de minister van Defensie aan:

1. Zorg dat voor het IT-systeem van de balie zo spoedig mogelijk de benodigde beveiligingsmaatregelen worden genomen zodat de goedkeuringsprocedure conform het Defensiebeveiligingsbeleid kan worden afgerond.

We bevelen de minister van JenV aan:

2. Zorg dat het selfservicesysteem de goedkeuringsprocedure conform het Defensie-beveiligingsbeleid zo spoedig mogelijk doorloopt, waarbij Schiphol N.V. alle beveiligingseisen implementeert en blijft implementeren en het systeem goedkeuring verkrijgt van de beveiligingsautoriteit van het Ministerie van JenV.
3. Overdenk opnieuw of met de voorgenomen overdracht van het selfservicesysteem aan Schiphol N.V. de cybersecurity afdoende gewaarborgd is.

7.2 Systemen grenstoezicht niet aangesloten op Security Operations Centers

Het risico bestaat dat cyberaanvallen op de drie IT-systemen van het grenstoezicht niet of te laat worden opgemerkt. Slechts een deel van de cyberaanvallen op het grenstoezicht zijn direct waar te nemen omdat de drie IT-systemen niet direct zijn aangesloten op de detectiecapaciteit van een Security Operations Center (SOC). Dit geldt zowel voor de twee systemen van het Ministerie van Defensie als voor het selfservicesysteem van het Ministerie van JenV.

Met detectie kan een SOC in de gaten houden of IT-systemen digitaal aangevallen worden. Binnen het Ministerie van Defensie is een SOC opgezet onder de naam SIOC. Ook Schiphol N.V. beschikt over een SOC. Het hebben van een SOC is een belangrijke randvoorwaarde voor een adequate cybersecurity-aanpak. De systemen van het grenstoezicht zijn echter niet zelf aangesloten op deze detectiecapaciteit. Omliggende IT, zoals koppelvlakken en besturingssystemen, zijn hier wel op aangesloten. Dit is een risico omdat zo een directe aanval op de systemen niet snel kan worden gedetecteerd door een SOC. Eén van de IT-systemen (dat voor pre-assessment) is door het Ministerie van Defensie zelf aangemerkt als 'kritiek systeem' maar staat niet in de aansluitplanning van het SIOC.

We bevelen de minister van Defensie aan:

4. Sluit de twee IT-systemen van het grenstoezicht waar het Ministerie van Defensie voor verantwoordelijk is zo snel mogelijk aan op de detectiecapaciteit van het SOC van het Ministerie van Defensie en geef hierbij de hoogste prioriteit aan het als 'kritiek' benoemde systeem voor pre-assessment.

We bevelen de minister van JenV het volgende aan:

5. Zorg dat het selfservicesysteem zo snel mogelijk op de detectiecapaciteit van het SOC van Schiphol N.V. wordt aangesloten.

7.3 Onvoldoende beveiligingstesten op IT-systemen grenstoezicht

In de praktijk voerden het Ministerie van Defensie en het Ministerie van JenV nauwelijks tot geen beveiligingstesten uit op de drie IT-systemen van het grenstoezicht. Dit terwijl jaarlijkse beveiligingstesten als verplichte beveiligingsmaatregel volgen uit het Defensie-beveiligingsbeleid. De wel uitgevoerde test was beperkt en de aanbevelingen zijn slechts gedeeltelijk opgevolgd.

Het Ministerie van Defensie beschikt met het organisatieonderdeel DefCERT over een partij die beveiligingstesten kan uitvoeren. In de praktijk zijn er echter weinig tot geen beveiligingstesten uitgevoerd op de drie IT-systemen van het grenstoezicht. Zo waren voor het IT-systeem van pre-assessment en de balie nog geen beveiligingstesten uitgevoerd. Een beveiligingstest op het selfservicesysteem duurde lang en had uiteindelijk een beperktere scope dan gepland. Ook werden de aanbevelingen van DefCERT beperkt opgevolgd en duurde opvolging lang: een jaar na de test op de software bleken slechts 3 van de 10 bevindingen die opnieuw werden getest opgevolgd. Hierdoor bestaat het risico dat onbekende kwetsbaarheden in de systemen blijven bestaan die misbruikt kunnen worden voor cyberaanvallen.

Een door de Algemene Rekenkamer geïnitieerde beveiligingstest in november 2019 op het systeem voor pre-assessment bracht 11 verschillende kwetsbaarheden aan het licht. Door deze kwetsbaarheden gecombineerd te benutten, was een cyberaanval mogelijk waarmee een aanvaller passagiersgegevens zou kunnen inzien en de werking van het systeem kon beïnvloeden. Het Ministerie van Defensie heeft hierop direct maatregelen genomen zodat een dergelijke aanval nu onmogelijk is. De resultaten van de test onderstrepen het belang van beveiligingstesten.

We bevelen de ministers van Defensie en JenV het volgende aan:

6. Onderwerp de drie grenstoezichtsystemen zo snel mogelijk, conform het Defensie-beveiligingsbeleid, aan jaarlijkse beveiligingstesten en borg de opvolging van aanbevelingen.

7.4 Reactie op cyberincidenten

Het Ministerie van Defensie heeft uitgebreide procedures over hoe te handelen bij een IT-verstoring. Daarbinnen is er ook een specifieke procedure voor een reactie op een cyberincident. Alle betrokken partijen moeten op dat moment als keten functioneren. Of de procedures in geval van een cyberaanval op het grenstoezicht in de praktijk goed werken, is nog niet aangetoond met een oefening. Hierdoor bestaat het risico dat de partijen gezamenlijk in een crisissituatie niet adequaat reageren op een cyberaanval. Een cyberaanval op het grenstoezicht kan specifieke kenmerken en gevolgen hebben waar nu nog geen voorbereidingen voor zijn getroffen. In het geval van *ransomware* is het bijvoorbeeld van belang dat vooraf is nagedacht over het eventueel betalen van losgeld. Dergelijke scenario's zijn niet expliciet benoemd in de processen. Door te oefenen raken partijen op elkaar ingespeeld en worden belangentegenstellingen expliciet. Zo gaat in een crisissituatie hieraan geen tijd verloren en hoeft er minder te worden geïmproviseerd.

We bevelen de ministers van Defensie en JenV het volgende aan:

7. Laat het Ministerie van Defensie en het Ministerie van JenV in samenwerking met alle relevante ketenpartijen oefenen met het beheersen van crises als gevolg van een cyberaanval op de drie IT-systemen van het grenstoezicht op Schiphol.

8 Reactie ministers en nawoord Algemene Rekenkamer

De ministers van Defensie en Justitie en Veiligheid (JenV) hebben op 27 maart 2020 gereageerd op ons rapport. Hieronder is deze reactie opgenomen. We sluiten af met ons nawoord.

8.1 Reactie minister van Defensie en minister van JenV

Met veel belangstelling hebben wij kennis genomen van het rapport 'Digitalisering aan de Grens'. Gezien het toenemende belang van IT is cybersecurity een belangrijk maatschappelijk thema. We moeten ons voorbereiden op geavanceerde digitale dreigingen en de mogelijke gevolgen. Wij hebben daarom veel aandacht voor dit onderwerp. Dagelijks werken er binnen Defensie en J&V vele professionals aan het veilig maken en houden van het grenstoezicht.

Er zijn diverse maatregelen van kracht om de risico's en gevolgen van een cyberaanval op de IT-systemen te beperken. In het geval de IT-systemen op Schiphol om wat voor reden ook uitvallen, zal het grenstoezicht nog steeds handmatig plaatsvinden.

In lijn met uw rapport onderkennen wij dat gezien het toenemende gebruik van IT-systemen bij het grenstoezicht op Schiphol verdere verbeteringen gewenst zijn en onderschrijven uw aanbevelingen. Tegelijkertijd is de opgave op het gebied van cybersecurity groot en het IT-landschap voor het grenstoezicht dynamisch. Op veel van de aanbevelingen zetten we reeds stappen. Of we aan alle aanbevelingen kunnen voldoen binnen de door u aanbevolen termijnen of frequentie kunnen we daarom niet op voorhand garanderen.

Hieronder gaan wij verder in op uw aanbevelingen, beschrijven wij welke acties er worden genomen en welke overwegingen daaraan ten grondslag liggen.

Aanbevelingen

Afronden goedkeuringsprocedure (aanbeveling 1 en 3)
U beveelt aan zo snel als mogelijk de benodigde beveiligingsmaatregelen te treffen en de goedkeuringsprocedure af te ronden voor het systeem in de balie en het selfservicesysteem.

Het systeem in de balie heeft in 2016 voor het laatst de goedkeuringsprocedure doorlopen. Sindsdien zijn geen grote wijzigingen opgetreden in het ontwerp van het systeem, waardoor op basis van de resultaten uit 2016 een goede analyse valt te maken of het systeem

veilig is. Defensie schat op basis van deze analyse in dat de risico's laag en acceptabel zijn. Momenteel worden aanpassingen gedaan in het systeem en extra beveiligingsmaatregelen getroffen om de beschikbaarheid van het systeem in de toekomst beter te kunnen garanderen. Om dit proces niet te vertragen is besloten de goedkeuringsprocedure, die in 2019 van start is gegaan, te voltooien zodra de benodigde wijzigingen zijn doorgevoerd.

Voor het selfservicesysteem geldt dat de te treffen beveiligingsmaatregelen zijn geïdentificeerd en dat de inzet is deze maatregelen zo snel mogelijk te implementeren. Daarna kan de goedkeuringsprocedure worden afgerond.

Aansluiten op detectiecapaciteit (aanbeveling 2 en 5)
U beveelt aan de onderzochte IT-systemen zo snel als mogelijk aan te sluiten op de detectiecapaciteit van Defensie en Schiphol. Defensie heeft in 2017 een eigen Security Operations Center (SOC) opgericht om gevraagde en ongevraagde detectie op de IT-systemen van Defensie uit te kunnen voeren. Niet alle systemen kunnen tegelijkertijd op het SOC worden aangesloten, hierin is voor een stapsgewijze benadering gekozen. Daarbij wordt voorrang gegeven aan de IT-systemen die voor Defensie de hoogste prioriteit hebben. Momenteel geldt dat andere kritieke systemen, met een hogere urgentie, voorrang krijgen. Het netwerk waarop de systemen in de balie en bij het pre-assessment zich bevinden is aangesloten op het SOC. Daarmee wordt reeds een deel van de risico's ondervangen. Om ook de overige risico's te kunnen ondervangen worden de individuele systemen op termijn aangesloten.

Het selfservicesysteem wordt inmiddels aangesloten op de detectiecapaciteit van het SOC van Schiphol. Dit is onderdeel van de beveiligingsmaatregelen die worden getroffen in het kader van de goedkeuringsprocedure.

Beveiligingstesten (aanbeveling 6)
U beveelt aan om jaarlijks een beveiligingstest uit te voeren op de onderzochte systemen. Voor de 14 kritieke systemen van Defensie, waar het systeem voor het pre-assessment onderdeel van uitmaakt, is besloten dat zij elke drie jaar opnieuw de goedkeuringsprocedure moeten doorlopen. Het uitvoeren van een beveiligingstest en het borgen van de aanbevelingen die daaruit voort komen maken een onderdeel uit van deze cyclus. Het grote aantal systemen, de beperkte personele capaciteit om te kunnen testen en de tijd die benodigd is om alle bevindingen te kunnen opvolgen maken dat het verhogen van deze frequentie op korte termijn niet haalbaar is.

Bovenstaande cyclus geldt niet voor het selfservicesysteem. Op zo kort mogelijke termijn wordt een nieuwe beveiligingstest uitgevoerd op dit systeem. De resultaten zullen gebruikt worden voor het verder verbeteren van de veiligheid. Het streven is om vanaf 2021 het self-servicesysteem jaarlijks te testen.

Oefenen met cyberaanval (aanbeveling 7)
U beveelt aan om te oefenen met het beheersen van crises als gevolg van een cyberaanval op Schiphol. In overleg met de relevante ketenpartners zullen wij bespreken op welke termijn een dergelijke oefening georganiseerd kan worden.

Overdracht selfservicesysteem aan Schiphol (aanbeveling 4)
U beveelt aan om de voorgenomen overdracht van het eigenaarschap van het selfservice-systeem van het ministerie van Justitie en Veiligheid naar Schiphol te overdenken. Alvorens te besluiten tot overdracht van het eigenaarschap van het systeem aan Schiphol zal worden bekeken hoe de veiligheid het meest effectief kan worden gewaarborgd. Dit sluit aan op het goedkeuringsproces volgens het Defensieveiligheidsbeleid dat momenteel wordt doorlopen. Het voltooien van de goedkeuringsprocedure en het blijvend voldoen aan de beveiligingseisen is een voorwaarde voor een overdracht van het systeem aan Schiphol.

Tot slot
We danken de Algemene Rekenkamer voor het onderzoek en de aanbevelingen. Uw onderzoek vormt een belangrijke bijdrage aan de discussie over de kansen en risico's van digitalisering.

8.2 Nawoord Algemene Rekenkamer

De minister van Defensie en de minister van JenV erkennen dat het toenemende gebruik van IT verbetering van de cybersecurity van het grenstoezicht noodzakelijk maakt. Ze wijzen op de diverse cybersecuritymaatregelen die van kracht zijn. Bij uitval zal het grenstoezicht volgens de ministers bovendien nog steeds handmatig plaatsvinden. Wij merken op dat die terugvaloptie van handmatige grenscontroles zal leiden tot vertraging en kans op fouten bij de grenscontroles.
De ministers geven aan dat niet alle aanbevelingen direct en volledig opgevolgd kunnen worden. Met een planning kunnen de ministers transparant maken op basis waarvan prioriteiten zijn gesteld en welke risico's daarbij geaccepteerd worden. Wij pleiten ervoor dat de ministers de Kamer in ieder geval informeren over de goedkeuringsprocedures en aansluiting van de 14 kritieke Defensiesystemen op het SOC van het Ministerie van Defensie.

Wat betreft de beveiligingstesten baart het ons grote zorgen dat zelfs de 14 kritieke Defensiesystemen niet vaker dan eens per drie jaar aan een beveiligingstest kunnen worden onderworpen. Dit is tevens in afwijking van het Defensie-beveiligingsbeleid, dat jaarlijkse testen voorschrijft. Gedurende een jaar kunnen nieuwe kwetsbaarheden, dreigingen en aanvalsscenario's ontstaan. Het is belangrijk om de weerbaarheid van IT-systemen te blijven controleren. De kwetsbaarheden die in de test voor dit onderzoek naar voren kwamen, zoals het gebruik van verouderde software, onderstrepen het belang van jaarlijks testen. Het voornemen van de ministers om het selfservicesysteem wel jaarlijks te testen valt hierbij te prijzen.

Wij volgen de voortgang op onze aanbevelingen op de voet en zullen hierover rapporteren indien wij dat nodig achten.

Bijlage 1 Methodologische verantwoording

Onderzoeksvragen

In dit onderzoek stonden 6 onderzoeksvragen centraal

1. Hoe ziet de context van het grenstoezicht door de Koninklijke Marechaussee op Schiphol eruit, welke processen kent het grenstoezicht en welke IT is hieraan ondersteunend?
2. Welke preventieve cybersecuritymaatregelen zijn er genomen rondom de IT van het grenstoezicht?
3. Welke detectiemaatregelen zijn er, en zijn deze voldoende?
4. Hoe werken deze detectiemaatregelen in de praktijk en bieden ze voldoende bescherming?
5. Welke responsscenario's zijn er voor cyberincidenten, en zijn ze voldoende?
6. Hoe werken de responsscenario's in de praktijk en is dat voldoende?

Normen

Als normenkader bij de beantwoording van onderzoeksvragen 2 tot en met 6 hanteerden we het cybersecurityraamwerk van het *National Institute of Standards and Technology* (NIST). Het NIST is onderdeel van het Amerikaanse Ministerie van Economische Zaken. Hun raamwerk voor cybersecurity wordt wereldwijd veel gebruikt en heeft relaties met beveiligingsstandaarden en -modellen als ISO 27001 en COBIT. Het NIST-raamwerk onderscheidt vijf hoofdfuncties, waaronder de voor ons onderzoek extra relevante functies 'detectie' en 'respons'. De categorieën binnen de hoofdfuncties hebben we gebruikt als hulpmiddel om de diversiteit aan inspanningen op het gebied van cybersecurity bij het grenstoezicht inzichtelijk te maken. Ons uiteindelijke oordeel over de cybersecurity van het grenstoezicht is niet uitsluitend gebaseerd op het al dan niet voldoen aan de specifieke normen binnen het NIST-raamwerk. Het oordeel is kwalitatief, gevormd op basis van onze bevindingen in brede zin die we per categorie bij het grenstoezicht hebben gedaan. Om het rapport toegankelijk te houden, hebben we de Engelse namen van de NIST-categorieën vermeden. Bijlage 2 geeft een overzicht van de gebruikte NIST-categorieën en hun plek in het rapport.

Onderzoeksactiviteiten

Op basis van de gehanteerde NIST-categorieën hebben we via de Ministeries van Defensie en JenV gesprekspartners en -onderwerpen geselecteerd. Vervolgens hebben we relevante stukken opgevraagd en interviews afgenomen. Naar aanleiding van de interviews hebben we informatie gecontroleerd aan de hand van aanvullende documenten.

Voor het onderzoek hebben we werkbezoeken afgelegd aan de KMar op Schiphol en de locatie waar het pre-assessment plaatsvindt. Daarnaast hebben een beveiligingstest geïnitieerd op een van de systemen van het grenstoezicht. Specialisten van het Ministerie van Defensie (DefCERT) hebben op het door ons geselecteerde systeem en de door ons voorgedragen uitgangssituatie de weerbaarheid van dat systeem in de praktijk getoetst met een beveiligingstest. De resultaten van die test zijn ongefilterd en gelijktijdig met het Ministerie van Defensie en ons gedeeld. Na ons onderzoek hebben we onze bevindingen voorgelegd aan het Ministerie van Defensie en het Ministerie van JenV. Het ambtelijk commentaar hierop hebben we meegenomen bij het schrijven van dit rapport.

Casuïstiek

Omdat er nog geen cyberaanvallen zijn waargenomen op het grenstoezicht konden we een dergelijk praktijkgeval niet evalueren. Wel hebben we gebruik gemaakt van een evaluatie van een grote IT-verstoring (niet veroorzaakt door een cyberaanval) en een eerder door DefCERT uitgevoerde beveiligingstest op de selfservicesoftware. Het scenario voor de beveiligingstest op het systeem van pre-assessment in het kader van dit onderzoek is gebaseerd op een eigen risico-inschatting.

Bijage 2 Normen waaraan we toetsen

Onderstaande tabel geeft de gehanteerde categorieën uit het *Cybersecurity Framework* van het NIST weer, met een Nederlandse vertaling (tussen haken). Bij elke categorie is aangegeven wat onze belangrijkste verwachtingen waren bij het toetsen en in welke paragraaf onze bevindingen zijn opgenomen.

Tabel 1 *Overzicht van belangrijkste verwachtingen per NIST-categorie*

NIST-categorie	Belangrijkste verwachtingen	§
Governance (Besturing)	Samenhangend cybersecuritybeleid, duidelijke verantwoordelijkheden, interne en externe afstemming.	4.2
Information Protection Processes and Procedures (Processen voor IT-beveiliging)	Gebruik van beveiligingsprincipes en -maatregelen om, afhankelijk van het risico, te hanteren bij het bouwen en configureren van systemen.	4.1
Protective Technology (Beveiligingstechnologie)	Inzet van technische maatregelen tegen cyberaanvallen.	4.1
Risk Assessment (Risico-inschatting)	Dreigingsanalyses op basis van verschillende bronnen en gebruik van de analyses om het benodigde niveau van maatregelen te bepalen.	4.1
Asset Management (Beheren bedrijfsmiddelen)	Inzicht en overzicht in de (kenmerken van) IT-middelen en gebruik van dit inzicht voor cybersecurity-analyses.	4.2
Supply Chain Risk Management (Beheersen ketenrisico's)	Zicht op ketenafhankelijkheden, afspraken en controles om risico's te beperken.	4.4
Anomalies and Events (Afwijkingen en gebeurtenissen)	Inzicht in de normale werking van IT-systemen en indicatoren (events) die kunnen duiden op een cyberaanval.	5.1
Security Continuous Monitoring (Voortdurende monitoring beveiliging)	Voortdurende monitoring van IT-systemen op cybersecurity-events met gebruik van een SIEM en regelmatig uitgevoerde beveiligingstesten.	5.1 5.2
Detection Processes (Detectieprocessen)	Inzicht in de werking van de detectieprocessen en het verbeteren ervan op basis van evaluaties.	5.1
Response Planning (Planning respons)	Processen voor de reactie op een cyberincident of een crisis waarin betrokken partijen, rollen, verantwoordelijkheden en doelen zijn vastgelegd.	6.1
Communications (Communicatielijnen)	Coördinatie van respons-activiteiten en afstemming tussen interne en externe betrokkenen in de keten.	6.1
Analysis (Analyse)	Vastgestelde werkwijze voor analyses op een incident of crisis, als basis voor een adequate reactie.	6.1
Mitigation (Afwenden)	Vastgestelde activiteiten voor types cyberaanvallen om een crisis te bestrijden en terug te keren naar de normale situatie.	6.1
Improvements (Verbeteringen)	Oefeningen en evaluaties van cyberincidenten/-crises en voorstellen om de respons te verbeteren.	6.1 6.2

Bijlage 3 Lijst van afkortingen en Engelstalige begrippen

ABDO	Algemene Beveiligingseisen voor Defensieopdrachten
AIVD	Algemene Inlichtingen- en Veiligheidsdienst
AP	Autoriteit Persoonsgegevens
BPVS	Beveiliging Publieke en Private Veiligheid Schiphol
Cybersecurity	Het geheel aan maatregelen om schade door verstoring, uitval of misbruik van ICT te voorkomen en, indien er toch schade is ontstaan, het herstellen hiervan.
Dark web	Een besloten deel van het internet dat men niet vindt met normale browsers en zoekmachines. Het staat vooral bekend als een plek waar criminelen hun zaken doen.
DCSC	Defensie Cyber Security Commando
DefCERT	Defensie Computer Emergency Response Team
EES	Entry-Exit Systeem
ESTA	Electronic System for Travel Authorization
ETIAS	European Travel Information and Authorisation System
False negative	Een uitslag van een test die ten onrechte negatief is
Hacken	Actie om in of bij een computer, netwerk, hardware of software te komen. Als men dat ongevraagd of zonder geldige reden doet, is zo'n actie illegaal.
Insider Threat	Dreiging die zijn oorsprong heeft binnen de organisatie. Er is sprake van een insider threat als een (oud)-medewerker of leverancier zijn positie misbruikt voor kwaadwillende activiteiten.
ISAC	Information Sharing and Analysis Centre
JenV	Justitie en Veiligheid
JIVC	Joint IV-Commando
KMar	Koninklijke Marechaussee
Malware	Kwaadaardige software die aanvallers op een digitaal systeem zetten om er op afstand bij te kunnen, het te vernielen of informatie te stelen. Malware is een samentrekking van het Engelse malicious software.
MIVD	Militaire Inlichtingen- en Veiligheidsdienst
NCTV	Nationaal Coördinator Terrorismebestrijding en Veiligheid
NCSC	Nationaal Cyber Security Centrum
NIST	National Institute of Standards and Technology
Pentest	Penetratietest, een 'proefhack' waarmee een organisatie de digitale beveiliging in de praktijk test
Ransomware	Gijzelsoftware waarmee een aanvaller IT-systemen/bestanden blokkeert en losgeld eist om ze te deblokkeren
Seamless Flow	Een nieuw systeem dat op basis van gezichtsherkenningstechnologie het passagiersproces op Schiphol van check-in tot boarding tot een gestroomlijnd geheel moet maken.
SIEM	Security Information and Event Management software
SIOC	Security Intelligence Operations Centre
SOC	Security Operations Centre
SSPC	Self Service Passport Control

Bijlage 4 Literatuur

Publicaties

Algemene Rekenkamer (2019a). *Digitale Dijkverzwaring, cybersecurity van vitale waterwerken*. Den Haag: eigen beheer.

Algemene Rekenkamer (2019b). *Rapport bij het jaarverslag 2017 Ministerie van Defensie (X)*. Den Haag: eigen beheer.

Cyberveilig Nederland (2019). Cybersecurity Woordenboek (2019) *Van cybersecurity naar Nederlands*. Den Haag: eigen beheer.

Ministerie van Defensie (2017). *Introductiebundel Defensie*. Den Haag: eigen beheer.

NCTV (2018). *Nederlandse Cybersecurity Agenda, Nederland digitaal veilig*. Den Haag: eigen beheer.

NCTV & NCSC (2019). *Cybersecuritybeeld Nederland 2019*. Den Haag: eigen beheer.

Wetenschappelijke Raad voor het Regeringsbeleid (2019). *Voorbereiden op digitale ontwrichting*. Den Haag: eigen beheer.

Wet en regelgeving

Besluit beveiliging netwerk- en informatiesystemen. Besluit van 30 oktober 2018, houdende regels ter uitvoering van de Wet beveiliging netwerk- en informatiesystemen.

Comptabiliteitswet 2016. Wet van 22 2017, houdende regels inzake het beheer, de informatievoorziening, de controle en de verantwoording van de financiën van het Rijk, inzake het beheer van publieke liquide middelen buiten het Rijk en inzake het toezicht op het beheer van publieke liquide middelen en publieke financiële middelen buiten het Rijk.

Uitvoeringswet Algemene verordening gegevensbescherming.

Verordening (EG) nr.562/2006 van het Europees Parlement en de Raad van 15 maart 2006 tot vaststelling van een communautaire code betreffende de overschrijding van de grenzen door personen (Schengengrenscode).

Wet beveiliging netwerk- en informatiesystemen. Wet van 17 oktober 2018, houdende regels ter implementatie van richtlijn (EU) 2016/1148.

Bijlage 5 Eindnoten

1. Voor een overzicht van vitale proces wordt veel verwezen naar de lijst die de Nationaal Coördinator Terrorisme bestrijding en Veiligheid hanteert. Een van de processen daarop is 'vlucht- en vliegtuigafhandeling', waar het grenstoezicht op luchthavens onderdeel van maakt.
2. Algemene Rekenkamer, Staat van de Rijksverantwoording 2018, blz. 39
3. Zie voor meer informatie het *ACI Europe Airport Industry Connectivity Report 2019*.
4. In juni 2019 werd bekend dat bij een cyberaanval op de Amerikaanse grenscontrole-autoriteit informatie van reizigers was buitgemaakt. Deze informatie, waaronder foto's van reizigers, bleek later beschikbaar op het dark web. In oktober 2018 waren bij een hack op luchtvaartmaatschappij Cathay Pacific de persoonlijke gegevens van 9,4 miljoen passagiers buitgemaakt, waaronder paspoort- en creditcardgegevens. Een maand eerder waren bij British Airways informatie van 380.000 transacties van passagiers gestolen.
5. Dit systeem staat bekend onder de naam Entry/Exit System (EES).
6. Zie voor meer informatie bijvoorbeeld https://magazines.defensie.nl
7. We schetsen slechts de hoofdlijnen van de grensprocedures. Voor het self-servicesysteem geldt bijvoorbeeld dat onderdanen van bepaalde landen (waaronder de Verenigde Staten en Japan) bij vertrek wel gebruik maken van SSPC, mits hun paspoort daar geschikt voor is.
8. Het NCSC levert organisaties op verzoek beveiligingsadviezen over nieuwe kwetsbaarheden in hard- en software. Daarnaast biedt het NCSC een wekelijks overzicht van alle verzonden beveiligingsadviezen en mediaberichten over cybersecurity in die week.
9. Pagina 11 van de Defensie Cyber Strategie 2018.
10. Dit onderscheid wordt ook gemaakt in de Baseline Informatiebeveiliging Overheid (BIO).
11. We hebben in ons onderzoek nog andere uitgevoerde testen op de IT van het grenstoezicht aangetroffen maar deze zijn niet direct te beschouwen als beveiligingstesten. Deze testen hebben wel te maken met de kwaliteit van de software maar gaan niet specifiek in op cybersecurity. Zo zijn er functionele testen uitgevoerd om vast te stellen of systemen werken conform eisen vanuit de Internationale Burgerluchtvaartorganisatie (ICAO). Ook vinden er periodiek onderzoeken naar de broncode van het selfservicesysteem en het gezichtsvergelijkingsalgoritme plaats.
12. Het gebruik van gijzelsoftware neemt de afgelopen jaren toe. Eind 2019 werd Maastricht University getroffen door een aanval met dergelijke *ransomware*. Hierbij is losgeld betaald aan de aanvallers om versleutelede gegevens te kunnen ontsleutelen.

Voorlichting

Afdeling Communicatie
Postbus 20015
2500 EA Den Haag
telefoon (070) 342 44 00
voorlichting@rekenkamer.nl
www.rekenkamer.nl

Omslag

Ontwerp: Corps Ontwerpers
Foto: Ton Koene/Alamy Stock Photo

Den Haag, april 2020