Algemene Rekenkamer

Cyber security of border controls operated by Dutch border guards at Amsterdam Schiphol Airport

2020

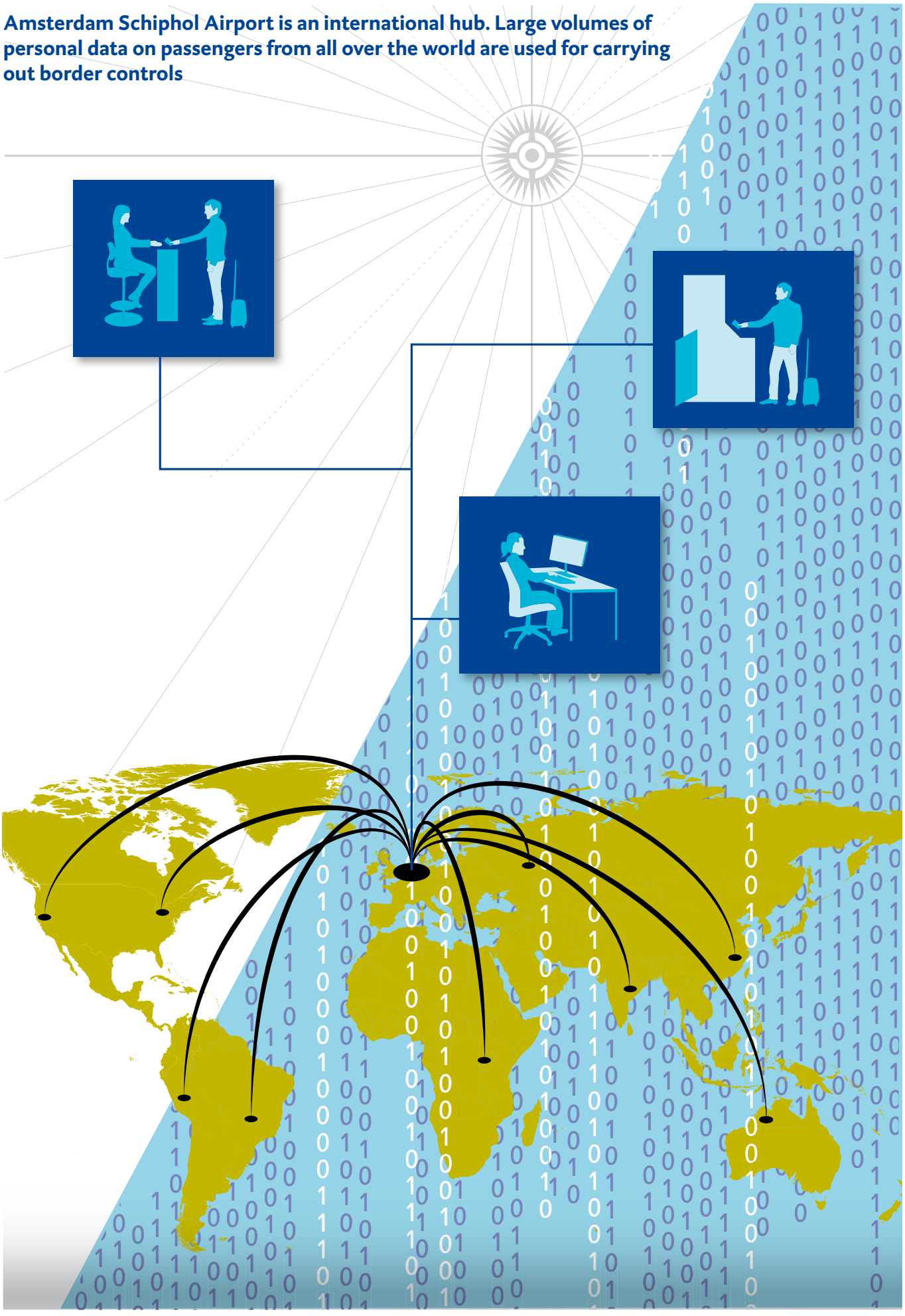
Preface

Along with the rest of the world, the Netherlands has been firmly in the grip of the coronavirus (SARS-CoV-2, which causes the disease known as COVID-19) since the beginning of the year. The measures taken by the Dutch government since March have had a huge impact on the daily lives of everyone in the country. The same applies to us: we, too, are feeling their effects.

This audit was launched in the middle of 2019. It describes the situation before the coronavirus had reached the Netherlands. We presented our audit findings to the responsible ministers precisely at the time when the measures to combat the spread of the coronavirus came into effect and the Dutch government was compelled to direct all its energy at managing the crisis. Our findings and conclusions relate to events that occurred in 2019, and have not been altered by the grave developments that have followed in 2020. Despite the difficult circumstances, the ministers concerned were able to respond to our conclusions and recommendations, thus illustrating how the Dutch democratic system, including the independent audits performed by the Court of Audit, continues to operate – even in the exceptional circumstances prevailing in the spring of 2020.

Original title:
Algemene Rekenkamer (2020). *Digitalisering aan de grens; Cybersecurity van het grens-toezicht door de Koninklijke Marechaussee op Schiphol.*

Amsterdam Schiphol Airport is an international hub. Large volumes of personal data on passengers from all over the world are used for carrying out border controls



Inhoud

1 Summary

Handling almost 80 million passengers every year, Amsterdam Schiphol Airport is not just the Netherlands' main airport, it is also a vital gateway to Europe and the European Union (EU). Passengers entering or leaving the Schengen Area via Amsterdam Schiphol Airport are checked by border guards from the *Koninklijke Marechaussee* (the Dutch Royal Military Constabulary). For the purpose of these border controls, the border guards process personal data in relation to passengers from all over the world. Such data include information on nationality, itinerary, travel companions and also (in some cases) on criminal records. The aim of carrying out these checks is to safeguard national security and control immigration. IT plays an important – an increasingly prominent – role in these border controls. While automation helps both to speed up border controls and to make them more thorough, at the same time it creates a dependency and poses new risks.

Cyber attacks, for example in the shape of digital sabotage, espionage and cyber crime, threaten the continuity of border controls and the confidentiality of the data processed. If IT systems fail, the Dutch border guards can no longer carry out border checks. Another risk is that foreign intelligence services may use cyber espionage as a means of gaining access to personal information, either on passengers in general or on individuals. However, cyber attacks could also be used in order to manipulate information, for example, to make it easier for people on wanted lists to cross the border.

Border controls are set to undergo further automation in the coming years, in part as a result of plans adopted by the EU and Royal Schiphol Group N.V. (referred to in the remainder of this report as 'Schiphol N.V.'). On the eve of an even more widespread use of technology, we therefore set out to examine how border controls at Amsterdam Schiphol Airport are protected against cyber attacks.

Our audit centred on the three primary, IT-intensive processes used by the border guards:
1. in-flight checks of incoming passengers;
2. checks performed at the manned passport-control desks at Amsterdam Schiphol Airport;
3. checks performed at self-service passport gates at Amsterdam Schiphol Airport.

Each of these processes is supported by its own dedicated IT system. The Minister of Defence is responsible for the cyber security of the systems used for the first two of the processes listed above. The Minister of Justice and Security is responsible for the IT system used by the third process.

Our audit showed that the cyber security procedures adopted are not as effective in practice as they could be. For the purpose of safeguarding the cyber security of border controls, the Ministry of Justice and Security makes use of the expertise and IT infrastructure of the Ministry of Defence and Schiphol N.V. Although the Ministry of Defence possesses the expertise needed to guarantee a high level of cyber security, the Ministry does not always make use of this expertise in practice in accordance with the arrangements made and with its own guidelines. In the light of all the impending technological developments, we believe that the current level of cyber security in relation to the border controls is neither adequate nor future-proof.

The Ministry of Defence has adopted a policy on cyber security. One of the aspects of this policy is that the most important IT systems must have their security features approved before they are taken into use. This policy applies to the two border control systems for which the Ministry of Defence is responsible. It was also decided that the system for which the Ministry of Justice and Security is the owner requires the same approval. Our audit team found that the IT systems used for the manned passport-control desks and the self-service passport gates are both operational despite not having obtained the necessary approvals. This means that there are no guarantees that they are safe.
IT specialists can quickly detect any cyber attacks by monitoring IT systems on a continuous basis. Both the Ministry of Defence and Schiphol N.V. have the necessary detection capacity in the form of a Security Operations Centre (SOC). The IT systems used for the border controls are not connected to the detection capacity of these SOCs. As a result, there is a risk of cyber attacks directed against these IT systems either not being detected or not being detected in time.

Multiple public-sector and private-sector parties are involved in the IT system owned by the Ministry of Justice and Security. This led to problems with a joint security test, which resulted in the test being more limited in scope than had originally been planned. The same applies to the way in which the system's security features are approved: here too, all the various parties are dependent on each other.

We found that neither the IT system used for the manned passport-control desks nor the system used for pre-assessments had yet been subjected to the requisite security tests. The same applied to a limited extent to the self-service system. Vulnerabilities in IT systems cannot be eradicated without regular security tests. Hackers perpetrating cyber attacks can take advantage of such vulnerabilities. For the purpose of this audit, a security test was performed on the system used for pre-assessments, which had not yet been tested. The test revealed 11 vulnerabilities, including the use of weak passwords and the

possibility of emails being sent with random Ministry of Defence officials being named as the sender. By taking advantage of a combination of these vulnerabilities, an attacker would be able to penetrate the system and manipulate its operation. The Ministry of Defence has now taken action to prevent such an attack.

The Ministry of Defence has adopted a wide range of procedures for dealing with IT failures and crisis situations. These include specific procedures for operational disruptions caused by a cyber attack. Although the Ministry of Defence practises with cyber crisis situations, it has not prepared for any specific scenarios, such as a ransomware attack in which the attacker demands the payment of a ransom. Similarly, no cyber exercises have been conducted in relation to border controls. This means that there is no way of knowing whether the Ministry's response to a cyber attack mounted against border controls would indeed be effective in practice.

Recommendations

We have formulated a number of recommendations for the responsible ministers in order to enhance the cyber security of the border controls carried out by the border guards at Amsterdam Schiphol Airport.

We urge the Minister of Defence to:

- ensure that the requisite security procedures are adopted as swiftly as possible in relation to the IT system used for the manned passport-control desks, so that the approval procedure can be completed in accordance with the Ministry's security policy;
- connect the two IT systems used for the border controls for which the Ministry of Defence is responsible as swiftly as possible to the detection capacity of the Ministry's SOC, and to give priority to the pre-assessment system (classified as 'critical') in this respect.

We urge the Minister of Justice and Security to:

- ensure that the self-service system is subjected as swiftly as possible to the approval procedure prescribed by the Ministry of Defence's security policy, that Schiphol N.V. adopts, both now and in the future, all the requisite security procedures, and that the system is approved by the security authority at the Ministry of Justice and Security;
- reconsider whether the planned transfer of ownership of the self-service system to Schiphol is accompanied by adequate cyber security safeguards;
- connect the self-service system as swiftly as possible to the detection capacity of Schiphol N.V.'s SOC.

We urge the Minister of Defence and the Minister of Justice and Security to act jointly in:

- subjecting the three IT systems used for border controls as swiftly as possible to annual security testing in accordance with the Ministry of Defence's security policy, and in ensuring that recommendations are implemented;
- ensuring that the Ministry of Defence and the Ministry of Justice and Security work together with all relevant partners in the supply chain in conducting exercises in managing crises caused by a cyber attack directed against the three IT systems used for the border controls at Amsterdam Schiphol Airport.

2 About this audit

2.1 What is the problem?

Cyber security is the term used to denote a wide variety of measures for preventing damage being caused by the disruption, breakdown or misuse of IT facilities and for repairing any damage thus caused (National Coordinator for Security and Counterterrorism, 2018). All deliberate attempts to damage IT systems by digital means (such as by using malware or by hacking into IT systems) are grouped together under the umbrella term of 'cyber attacks'.

The continuity of critical processes such as the electricity supply and the operation of the mobile phone network is of vital importance to the Netherlands.[1] The fact that these processes are highly computerised means that they are highly vulnerable to cyber attacks. Writing in a publication entitled *Cybersecuritybeeld Nederland 2019* ('The status of cyber security in the Netherlands in 2019'), the National Coordinator for Security and Counterterrorism warned about the potential consequences of this dependency on IT.
The National Coordinator believed that there was a permanent threat of cyber attacks, with the disruption of society looming as a potential consequence (National Coordinator for Security and Counterterrorism, 2019). The Dutch Scientific Council for Government Policy concluded in 2019 that not enough thought had been given to preparations for digital disruption (Scientific Council for Government Policy, 2019). For our part, when auditing information security at central government, we look specifically at the capability of resisting cyber attacks directed against critical government processes.[2] In 2019, for example, we concluded that there was scope for improving the cyber security of the country's critical water structures (Netherlands Court of Audit, 2019a).

The border controls operated by the border guards from the *Koninklijke Marechaussee* (the Dutch Royal Military Constabulary) at Amsterdam Schiphol Airport are the critical process at the centre of this audit. The border guards are part of the Dutch armed forces and as such fall under the Ministry of Defence. Border controls are of critical importance for the security and stability of the country. At the same time, the border guards are keen to ensure that these controls do not lead to long delays at the airport and thus damage the country's critical economic interests. Moreover, citizens must feel safe in the knowledge that their personal data are processed in a safe way.

Risks of cyber attacks directed against border controls
Handling almost 80 million passengers every year, Amsterdam Schiphol Airport is not just the country's main airport, it is also a vital gateway to Europe and the European Union (EU)

and Europe's second biggest transport hub.[3] In order to carry out border controls, the border guards make use of personal data on passengers from all over the world. Such data include information on nationality, itinerary, travel companions and also (in some cases) on criminal records. A number of incidents in the past bear witness to the fact that attackers are interested in obtaining this type of data. For example, the personal data of millions of passengers were stolen in cyber attacks directed against the US border protection agency and US airlines.[4] Due to the importance of Amsterdam Schiphol Airport and the large volume of personal data involved, the border controls could well form an attractive target for hackers.

The first possibility is that of a cyber attack aimed at disrupting border controls. The border guards cannot carry out border controls if the IT systems supporting the controls are disabled. The result would be long queues forming at Amsterdam Schiphol Airport and flights being delayed or cancelled, resulting in damage to the economy and the disruption of society. In the event of an IT failure, the border guards might have to relax border controls for a time, due to circumstances beyond their control. This is the point at which a cyber attack could raise the risk of illegal immigration, for example. In June 2019, a technical problem (not a cyber attack) forced the border guards to relax border controls for over an hour.

Another scenario involves an attack mounted against the confidentiality of the IT systems. According to the National Cyber Security Centre (NCSC), there is a permanent and growing threat of cyber espionage perpetrated by foreign intelligence services (National Coordinator for Security and Counterterrorism and National Cyber Security Centre, 2019). The latter may be interested in tracking the movements of diplomats, members of repressed minorities or political opponents, and they may attempt to penetrate systems in order to gain access to such information. The Dutch Military Intelligence and Security Service confirmed that foreign intelligence services may indeed be interested in obtaining passenger data processed during border controls at Amsterdam Schiphol Airport. It status as an international hub makes Amsterdam Schiphol Airport an attractive target.

A third risk is of a sophisticated cyber attack aimed at manipulating information. The fact is that border controls depend on the reliability, or 'integrity', of the data used. If an attacker succeeds, for example, in manipulating the contents of lists of wanted persons, this could make it easier for wanted persons to get past the border undetected.
The potential risks associated with cyber attacks will intensify in the future. The plans announced by Schiphol N.V. for performing biometric border checks and the EU's development of an entry-exit system for recording border crossings by travellers with

permission to reside temporarily in the Schengen Area will generate new data sets, including biometric data sets, and new interlinkages. Not only will this create a higher risk of cyber attacks, it will also ensure that they will have a more powerful impact if they materialise.

Prominent and growing role of IT in relation to border controls

In order to maintain the right balance between security and mobility, more and more use is made of IT in operating border controls. While this both speeds up border controls and enables them to be more thorough, it does make them more reliant on the effectiveness of computer systems. The EU, Schiphol N.V. and the border guards are planning to further automate the border controls at Amsterdam Schiphol Airport in the years to come:

- Under the EU's Smart Borders programme, a system for recording all entries and exits is due to become operational in 2020.[5]
- The European Travel Information and Authorisation System (ETIAS) is due to become operational in 2021. This is comparable with the ESTA (Electronic System for Travel Authorization) system in the US.
- EU member states are seeking to extend and harmonise digital border information systems, such as visa systems and lists of wanted persons.
- Schiphol N.V. is currently experimenting with biometric border checks as part of a project known as Seamless Flow. The ultimate objective is for passengers to be able to pass all airport checkpoints, including those operated by the border guards, once their biometric identifiers have been recorded.[6]
- The border guards are planning to add new features to the IT systems currently used for border controls, such as an extra digital check of the authenticity of travel documents.

In other words, the IT systems used for border controls are in the midst of a process of rapid development. The plans for further automating the border controls in the coming years form a big challenge for the parties involved in many different areas, including cyber security. This is because they will result in the creation of more and bigger IT systems, more digital interlinkages, and a larger volume of personal data that needs processing. The consequence is both a greater risk of a cyber attack directed at the border controls, and a more powerful impact if such an attack does indeed materialise.

2.2 Who bears political responsibility?

The Network and Data System Security Act

The Network and Data System Security Act lays down certain requirements that must be satisfied by the IT security of processes deemed critical to Dutch society. The Act recognises 'the safe and swift handling of flights and aircraft at Amsterdam Schiphol Airport' as an

'essential service'. The Act designates the border guard corps as one of the suppliers of this essential service, alongside Schiphol N.V. According to the explanatory memorandum accompanying the subsequent decree, the border guards were designated as one of the suppliers in the knowledge that any disruption of the border controls at Amsterdam Schiphol Airport could lead to massive passenger congestion and the cancellation of flights. Under the Network and Data System Security Act, suppliers of an essential service are obliged to take steps to manage the security risks associated with their IT systems, prevent security incidents and limit their impact. They are also required to report to the Minister of Justice and Security any security incidents that have a major impact on their ability to deliver the service in question.

Both the Minister of Defence and the Minister of Justice and Security bear political responsibility for the border guards and for border controls. As the responsible authority, the Minister of Justice and Security sets the legal framework for border controls. The Minister of Defence has a managerial responsibility for giving the border guards the people and resources they need in order to perform their duties. Both ministers are involved in the cyber security of the IT systems. The Ministry of Defence is the owner of two of the three IT systems, which means that the Minister of Defence is responsible for ensuring an adequate level of cyber security. The Ministry of Justice and Security is the owner of the third system, which means that the Minister of Justice and Security is responsible for its cyber security.

2.3 What did we audit?

We audited the measures taken by the Minister of Defence and the Minister of Justice and Security to protect the IT systems supporting the border controls operated by the border guards at Amsterdam Schiphol Airport against cyber attacks. We looked specifically at the procedures adopted for detecting any cyber attack as swiftly as possible, and at the way in which the minsters seek to contain the effects of such an attack, i.e. their response. We also sought to ascertain whether the measures are effective in practice. These were our main audit questions:

1. What is the context of the border controls operated by the border guards at Amsterdam Schiphol Airport? What processes are involved? What IT systems are used to support the border controls?
2. What preventive cyber security measures have been taken in relation to the IT systems used for the border controls?
3. What measures have been taken for detecting cyber attacks and are these adequate?
4. How do these detection measures operate in practice? Do they offer sufficient protection?

5. What response scenarios have been developed for cyber incidents? Are they adequate?
6. How do the response scenarios operate in practice? Are they adequate?

The first audit question is answered in Chapter 3. The second audit question is discussed in chapter 4. The third and fourth audit questions are addressed in chapter 5, while chapter 6 goes into the fifth and sixth audit questions. Our conclusions and recommendations are set out in chapter 7. Finally, chapter 8 contains the ministers' responses and our own afterword.

Audit scope

We began the audit by looking at all the various processes that play a role in border controls. Based on the results of this analysis, we decided to limit our audit to three processes used by the border guards (see sections 3.1 and 3.2). There were two reasons for this. Firstly, these three processes all involve primary checks of large groups of passengers, which means that any disruption caused by a cyber attack will have a relatively powerful impact. Secondly, they are all highly computerised, and hence heavily dependent on IT. We did not examine other processes involved in the operation of border controls, such as mobile checks performed by the border guards at Amsterdam Schiphol Airport or second-line checks of the authenticity of documents.

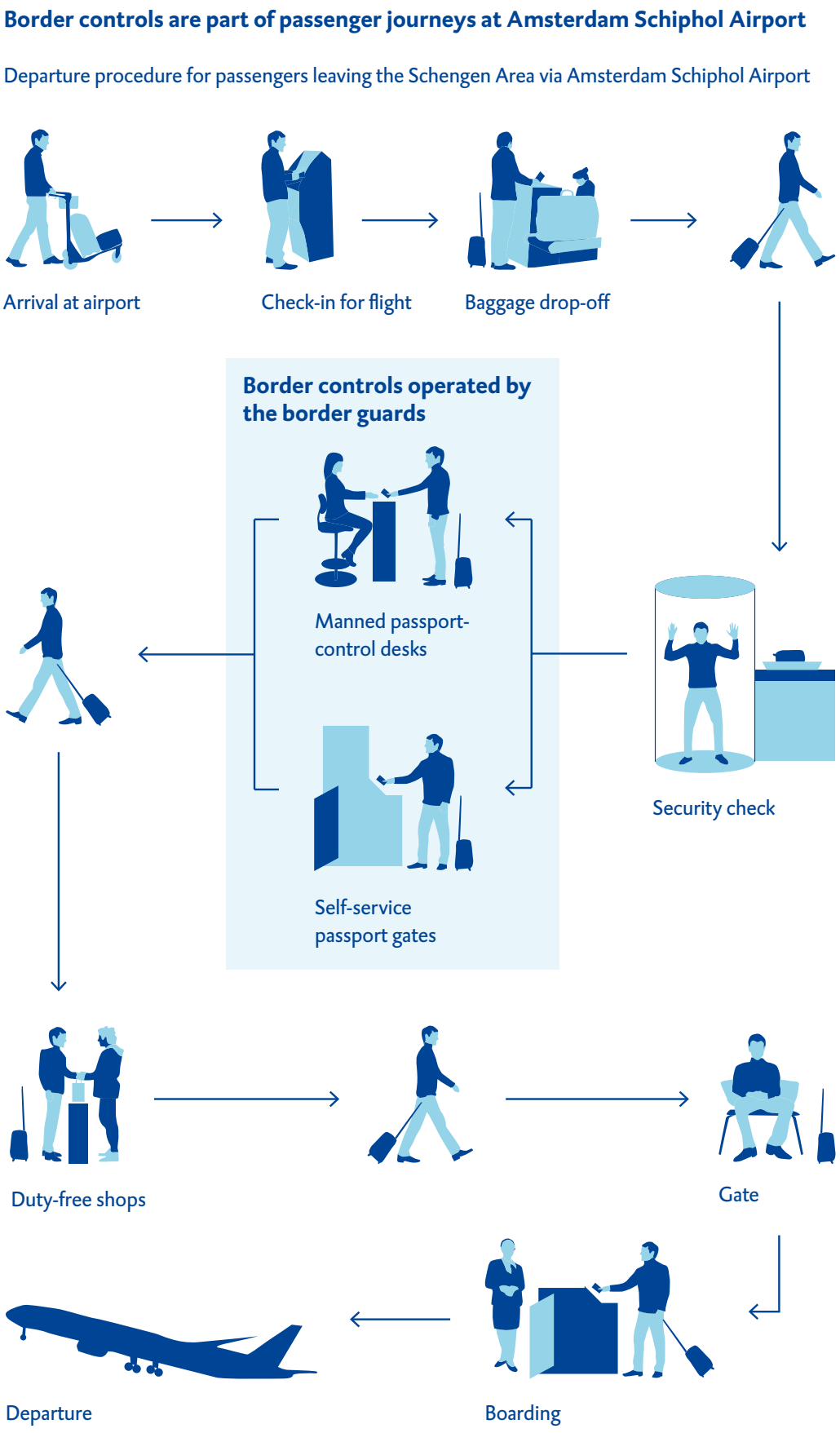
We then sought to establish which IT systems are used in support of these three processes (section 3.3). We found that each of the processes was supported by its own IT system. We proceeded to take a closer look at these systems, disregarding generic IT facilities such as the network and the operating systems. We analysed the three IT systems up to their interfaces with other systems, such as the police database containing criminal records, which the border guards consult during border controls.

2.4 How did we perform the audit?

In order to answer the audit questions, we studied internal documents at the Ministry of Defence and the Ministry of Justice and Security between July and the end of November 2019. We also made a number of working visits to the border guards at Amsterdam Schiphol Airport and interviewed a number of individuals involved in the border controls. We were interested both in the nature of the measures adopted and in how they worked in practice. At our own initiative, and with the aid of specialist staff from the Ministry of Defence, we tested the practical resilience of one of the three IT systems by subjecting it to a security test. Our audit criteria were taken from the cyber security framework published by the US National Institute of Standards and Technology (NIST). See Appendix 1 for further information on the audit methods.

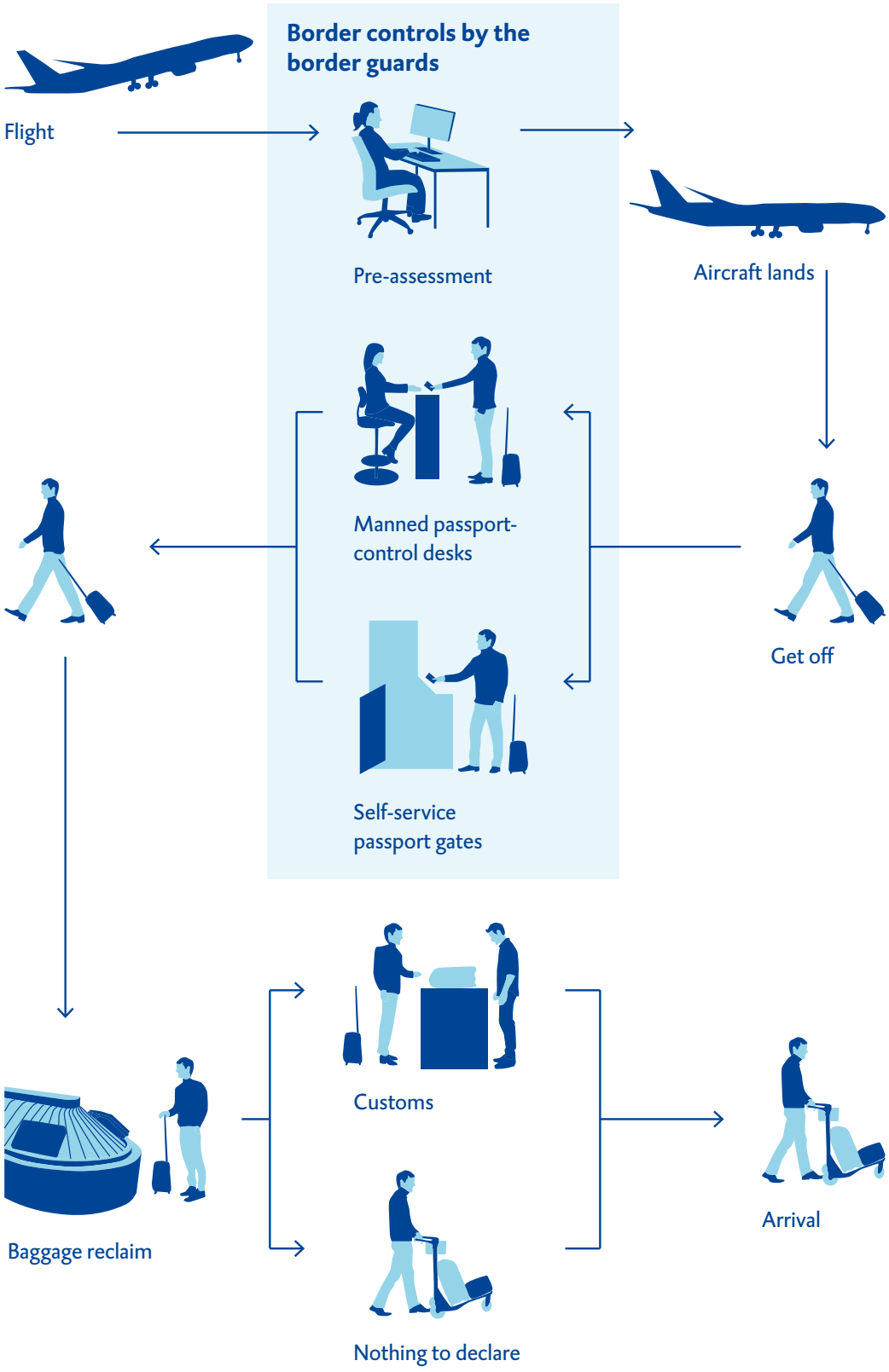
3 The border control process at Amsterdam Schiphol Airport

The Netherlands signed the first Schengen Agreement with Belgium, Luxembourg, Germany and France in 1985. The Agreement created the Schengen Area, an area in which the residents of the signatory countries are allowed to travel without any restrictions. The Schengen Area has been considerably expanded over the years. Residents of the Schengen countries and EU member states are no longer required to undergo border controls at border crossing points in airports in the Schengen Area. At Amsterdam Schiphol Airport, the border guards only check passengers travelling on flights to or from a country outside the Schengen Area. Figures 1 and 2 show the points at which these passengers encounter border controls.



Figuur 1 *Border controls for passengers departing from Amsterdam Schiphol Airport*

Arrival procedure for passengers entering the Schengen Area via Amsterdam Schiphol Airport



Figuur 2 *Border controls for passengers arriving at Amsterdam Schiphol Airport*

3.1 Border controls prior to entry: pre-assessment

The border guards carry out an initial check of incoming passengers while their flight is still in the air. Airlines are obliged to submit their passenger data to the border guards immediately after take-off.

The border guards use pre-assessments to check, before a flight arrives, whether any of the passengers on board need to be subjected to extra checks

Pre-assessment

Figuur 3 *Pre-assessment*

The border guards use these data to perform what is known as a 'pre-assessment' while the plane is in the air. They check, for example, whether any of the passengers appear on lists of wanted persons or have a profile that indicates that there might be a connection with people smuggling. The aim of a pre-assessment is to let the staff manning the border crossing points at Amsterdam Schiphol Airport know whether any passengers need to be checked or given an extra check, as the case may be. The pre-assessment speeds up border controls and makes them more effective.

3.2 Controls at border crossing points: manned passport-control desks and self-service passport gates

At Amsterdam Schiphol Airport, passengers entering the Netherlands from or leaving the Netherlands for a non-Schengen country pass a border crossing point manned by border guards. At crossing points for arrivals, the border guards may decide to pay extra attention to certain passengers, using information they have obtained from the pre-assessment. The checks at border crossing points take the form either of manual passport checks performed by border guards manning passport-control desks or of automated checks with the aid of self-service passport gates.

Border controls at border crossing points at Amsterdam Schiphol Airport take place either at manned passport-control desks or using fully automated self-service passport gates

Manned passport-control desks

Self-service passport gates

Figuur 4 *Passport control at manned passport-control desks and self-service passport gates*

In principle, passengers who are not covered by the rules on the free movement of persons in the EU or who are younger than 16 are obliged to pass through the manned passport-control desks.[7] Other passengers are entitled to choose between the manned desks and the self-service passport gates. In all cases, a check is made of each passenger's identity and the validity of their travel documents. A check is also made to ascertain whether their name appears on a list of wanted persons and whether their travel document is recorded as either missing or stolen. Where arrivals are concerned, this is in fact a double check, i.e. the same check is also performed as part of the pre-assessment. In the case of the self-service passport gates, the checks are fully automated. Although a border guard is on duty to supervise the gates, passengers scan their passports themselves and the system then uses biometrics to check their identity. If there is a problem, the duty guard can take the passenger in question aside for a more detailed check.

The guard at the manned passport-control desk scans the passport manually. He or she may decide to question the passenger, for example about the purpose or duration of his or her trip. The guard may also decide to question any minors travelling with the passenger. During our working visit to Amsterdam Schiphol Airport, we saw how carefully and quickly the border guards are required to check large numbers of passengers at the border crossing points and how important IT support is in this connection.

3.3 IT systems used for border controls

Each of the three main border control processes, i.e. the pre-assessments, the self-service passport gates and the manned passport-control desks, has its own IT system. The systems used for the pre-assessments and the manned passport-control desks are owned by the Ministry of Defence. The system supporting the self-service passport gates is owned by the Ministry of Justice and Security. A project was launched in 2016 for upgrading the existing system by installing a new version of the software. A number of public-sector and private-sector parties are involved in this technically complex project. Among those playing a role alongside the Ministry of Justice and Security as the owner are Schiphol N.V. and the Ministry of Defence (who are jointly responsible for management), an external software supplier, sub-contractors and the border guards as the user.

The parties do not all share the same interests. The new software is crucial to the Seamless Flow of the future (see section 2.1). Schiphol N.V. and the software supplier regard Seamless Flow as a key innovational project and are keen to implement the new software as soon as possible. The border guards, on the other hand, want first and foremost to be sure that the self-service system is stable and sufficiently secure. To date, the new software has failed to meet the security requirements laid down by the Ministry of Defence (see section 4.1.2), and the border guards do not believe that it is sufficiently stable. There is a risk here of the security of the self-service system becoming subordinate to the desire to roll-out Seamless Flow as quickly as possible.

The roll-out of the new software was originally slated for back in 2016, but has been delayed. This is due in part to the need for the parties involved in the project, given their divergent interests, to consult each other on all sorts of matters. The Ministry of Justice and Security and the parties involved in the project are keen to do something about this. For example, the Ministry of Justice and Security would like to adopt a new, all-encompassing timetable so as to make more effective use of the limited capacity available to the parties and coordinate their interdependencies. According to the latest timetable, the new software should be ready to be rolled-out by mid-2020. The new software may be used only if it meets the security requirements for IT systems as laid down by the Ministry of Defence. These are discussed in detail in section 4.1.

The idea is for the ownership of the self-service system to be transferred to Schiphol N.V. Schiphol N.V. is currently responsible for cyber security matters, with the Minister of Justice and Security involved only in a policy-making role, for example in setting standards for the reliability of biometric checks. We found that there are no legal restrictions on

transferring IT ownership in relation to critical government tasks such as border controls to commercial parties. The presence of the Network and Data System Security Act and its enforcement should ensure that the IT systems underlying essential services are sufficiently capable of resisting any cyber security threats. In the light of the number of parties involved and the wide range of interests at play in a changing technical environment, we believe it is important for cyber security to be guaranteed in relation to the planned transfer of ownership to Schiphol N.V.

4 Preventive cyber security procedures relating to border controls

This chapter discusses the preventive cyber security procedures relating to border controls. Our focus is on the Ministry of Defence given that, under the Network and Data System Security Act, the corps of border guards is designated as an essential service-provider in relation to border controls. In the four sections of this chapter, we assess whether, in relation to border controls, the Ministry of Defence:

1. prepares and adopts security procedures for IT systems on the basis of a risk assessment (section 4.1);
2. delegates responsibilities and creates consultative mechanisms for cyber security (section 4.2);
3. has a clear picture of the IT systems underlying border controls, their technical features and their interrelationships (section 4.3);
4. manages the dependencies with external parties (section 4.4).

4.1 Cyber security requirements applying to IT systems underlying border controls

In the case of two of the three IT systems used for border controls, the owners have not established that they are adequately protected against cyber attacks. The IT systems supporting the manned passport-control desks and the self-service passport gates have not completed the Ministry of Defence's approval procedure as is required to confirm that they are secure. As a result, there is no guarantee that these two systems are sufficiently capable of resisting cyber attacks.

4.1.1 The Ministry of Defence has an approval procedure for IT systems

The risk-driven protection of IT systems is an important means of minimising cyber security risks without taking any unnecessary action. The rule at the Ministry of Defence is that key IT systems may be taken into use only once it has been established that they are sufficiently capable of resisting cyber attacks. This involves following a four-stage approval procedure:

1. identify the requisite level of reliability;
2. define security requirements and procedures based on the requisite level of reliability;
3. adopt security procedures;
4. approve the implementation of the IT system ('accreditation').

Ministry of Defence bases cyber security risk assessments on information about cyber threats

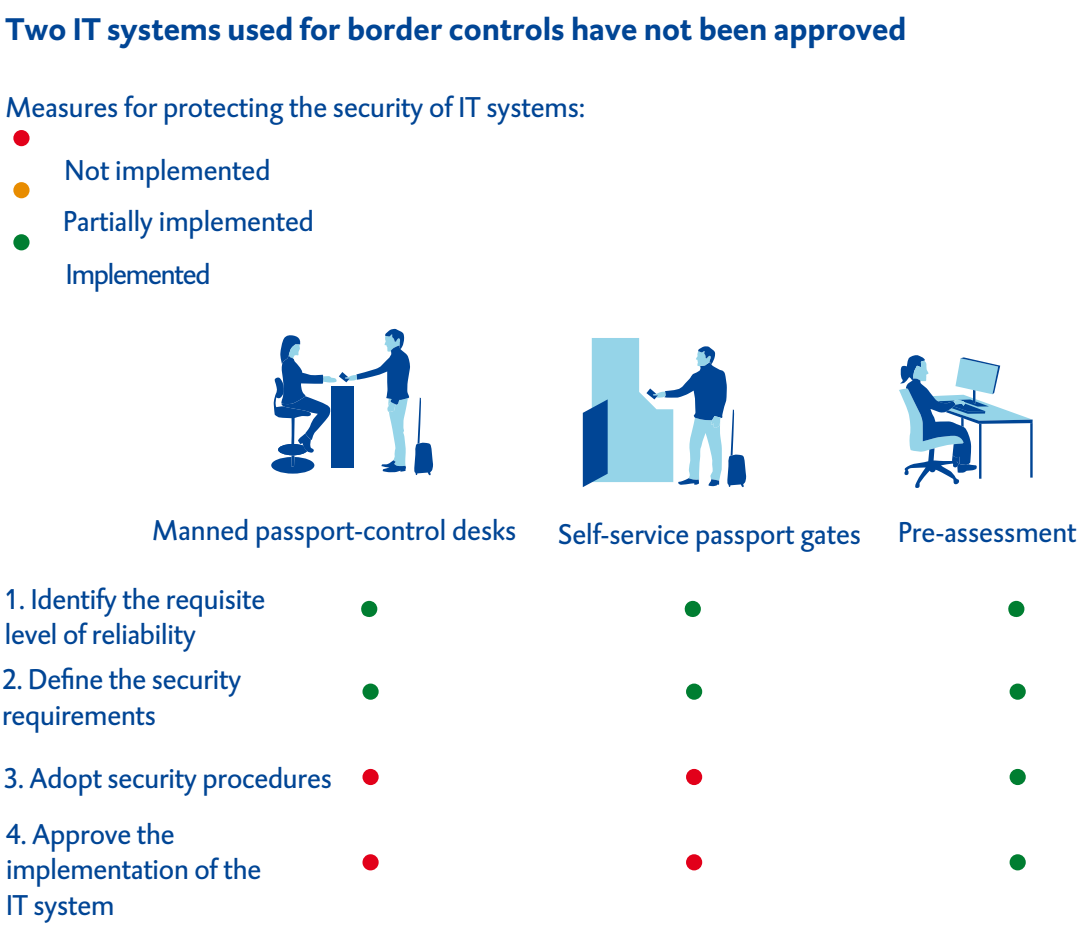
After obtaining information on cyber security threats from a variety of sources, the Ministry of Defence makes a systematic assessment of the risks. This is important as it helps to ensure that efficient use is made of resources and that adequate (but not unnecessary) security procedures are adopted. The main sources of information for assessing the threat of cyber attacks are:

- the Military Intelligence and Security Service;
- the National Cyber Security Centre (NCSC);[8]
- external partners (see section 4.2.2).

The Ministry of Defence uses the information it collects on cyber threats in a number of different ways, for example in order to compile a 'perpetrator profile'. This is a document that describes various types of adversaries and contains information on their motives and working methods, including the use of cyber attacks. The information on cyber threats is also used in setting the requisite level of reliability as part of the approval procedure for IT systems.

4.1.2 Two IT systems used for border controls have not been approved

We found that two IT systems used for border controls had not fully completed the approval procedure. The IT system used for the manned passport-control desks needs to be approved in accordance with the Ministry of Defence's security policy. The IT system used for the self-service passport gates is owned by the Ministry of Justice and Security and is therefore not subject to the Ministry of Defence's security policy. However, it has been agreed that this system must pass the approval procedure in accordance with the Ministry of Defence's security policy. As it is not clear whether the necessary security procedures have been adopted, it is equally unclear whether the systems used for the manned passport-control desks and the self-service passport gates are adequately protected against cyber attacks.



Figuur 5 *The approval procedure for IT systems used for border controls*

The IT system used for pre-assessments

The IT system used for the pre-assessments has completed the approval procedure and the majority of the relevant security procedures have been implemented. However, even though the system was given the go-ahead to be taken into use, no security tests were carried out and the system was not connected to the detection capacity of the Ministry of Defence's Security Operations Centre for the rapid detection of cyber attacks (see chapter 5). Both these measures were recommended by experts from the Ministry of Defence.

The IT system used for the manned passport-control desks

The IT system used for the manned passport-control desks consists of both new and existing components. Having previously approved the use of the existing components, the Ministry of Defence decided to regard the IT system underlying the manned passport-control desks as a new computer system. The approval procedure for the use of the system began early in 2019. Although decisions were taken on the requisite level of reliability and the appropriate security procedures, the latter have yet to be implemented. No timetable

had been drawn up for this at the time of our audit. The IT system is now being used despite the fact that the approval procedure has not been completed. As a result, there is now a risk to society that the computer system supporting the manned passport-control desks may be vulnerable to cyber attacks. We already pointed out in a previous audit report published in 2019 that a number of key IT systems used by the Ministry of Defence are operational even though the requisite approvals have not been issued (Netherlands Court of Audit, 2019b).

The IT system used for the self-service passport gates

As we already wrote in section 3.3, the project for updating the software used by the system underlying the self-service passport gates involves a large number of parties with disparate responsibilities. It is important to note that the Ministry of Justice and Security is the owner of the software currently in use and is responsible for its cyber security. Early in 2017, the border guards recommended that the self-service system should undergo the approval procedure for IT systems in accordance with the Ministry of Defence's security policy. The main reason for this was that the border guards corps is, by law, the controller of the personal data processed by the system. The completion of the approval procedure provides greater assurance that this processing is safe.

The approval procedure was initiated in the spring of 2019 and a decision has now been taken on the security procedures that need to be put in place. As the future owner of the system, Schiphol N.V. is planning to implement the measures. The Ministry of Defence will be playing an advisory and supporting role in this connection. The procedure will culminate in the security authority at the Ministry of Justice and Security giving its formal permission for the system to be taken into use.

When Schiphol N.V. assessed compliance with 52 security requirements in the autumn of 2019, it found that 23 of these requirements had not been met, and that, while eight requirements had been met in part, the degree of compliance was nonetheless inadequate. Although 21 of the requirements had been met, Schiphol N.V. found that this had not yet been verified by the Ministry of Justice and Security.

On two occasions, the Ministry of Justice and Security issued temporary approvals for the self-service system. The improvement plans drawn up in response to these temporary approvals have never been implemented. The last temporary approval expired on 1 June 2018. This means that the software has been used since then without there being any guarantee that it complies with the relevant security requirements. As long as no approval, temporary or otherwise, has been granted, the magnitude of the risks remains unclear, as

also remains unclear whether these are acceptable or whether action needs to be taken to contain them. We find this situation incomprehensible in the light of the risks associated with vulnerabilities to cyber attacks.

4.2 Cyber security and the Ministry of Defence

There is a clear allocation of responsibilities for cyber security at the Ministry of Defence. The Ministry also has a well-documented cyber security policy and has created consultative mechanisms for coordinating policy among both internal and external parties. This helps the Ministry to manage the cyber security risks.

4.2.1 Cyber security policy adopted and responsibilities allocated

It is clear from the Ministry of Defence's IT and cyber security strategy that the Ministry is aware of the nascent threat of cyber attacks. The cyber security strategy refers specifically to the growing digital risks associated with border controls. The strategy has been translated into the Ministry of Defence's security policy, i.e. a systematic set of procedures and guidelines that together describe how cyber security is to be achieved and who is responsible for what.

The Operational Management Division at the Ministry of Defence accommodates a number of key roles in relation to IT and cyber security: the Defence Security Authority, the Chief Information Officer and the Chief Information Security Officer. At the time of the audit, the Division was in the process of setting up a CIO Office with a staff of around 17 officials and incorporating both the Chief Information Officer and the Chief Information Security Officer.

The commanding officer of the border guards is responsible for the operational management of border controls, within the confines of the framework laid down by the Operational Management Division. The commanding officer receives support in this respect from a Security Coordinator, who has an advisory role and helps to ensure that the procedures and guidelines formulated by the Ministry are observed on the ground. At the time of the audit, the Security Coordinator was assisted by two advisers with expert knowledge of cyber security.

HThe Joint IV Command (JIVC) is the Ministry of Defence's IT supplier. Its task is to develop and manage all the ministry's IT assets. One of the entities in the JIVC is the Defence Cyber Security Command, which performs defensive cyber security duties such as the prevention and detection of cyber attacks (see chapter 5). The Defence Cyber Security Command consists of two units, both of which play an advisory role:

- the Security Intelligence Operations Centre (SIOC), with a staff of 49;
- the Defence Computer Emergency Response Team (DefCERT), with a staff of 38.
- Systematic coordination of cyber security

4.2.2 Systematic coordination of cyber security

The interdependencies in border controls plus the rapid pace of technological development mean that consultation and knowledge-sharing in relation to cyber security are both crucial. There is both a Cyber Governance Board and an IT Governance Board at the Ministry of Defence. The members of the two boards include representatives of various branches of the armed forces (including the border guards) and a number of officials with IT responsibilities. Board meetings discuss, for example, the implementation of the Ministry of Defence's cyber strategy, the security of the IT infrastructure and the use of cryptography. We were able to inspect the minutes of meetings of both boards, as well as board documents, which showed that the boards are active and that plans for future action are indeed put into effect.

The border guards carry out border controls at Amsterdam Schiphol Airport in a setting involving a number of external parties such as freight carriers, private security firms and Customs. For this reason, where cyber security is concerned, the border guards are represented in the Airport Information Sharing and Analysis Centre and the Airport Public and Private Security Protection Platform. It is clear from documents and the minutes of meetings that the members of both consultative bodies actively share information with each other, for example on the policy on the use of telephones and laptop computers by Ministry of Defence staff on official trips abroad.

4.3 Information on IT assets

The centralised information available to the Ministry of Defence on the IT systems used for border controls is not yet up to the requisite standard. The Ministry needs to have a clear picture of IT systems, their characteristic features and the interrelationships between them. In the event of a cyber attack or the discovery of a digital vulnerability, the Ministry can use this information to quickly gain an understanding of the likely impact and make a targeted response. The current situation is that the information held by the Ministry of Defence is not centralised, complete and up to date.

The Ministry of Defence wishes to have centralised lists of all IT applications and services relating to border controls. In addition to containing information on the interlinkages between the applications and services, these lists should display the systems' technical details and describe the type of information processed by them (such as confidential

information or particular types of personal data). The information is gathered using connections between a number of underlying databases. The centralised lists of information on applications and services relating to border controls became operational in 2019 and were still under development at the time of our audit. We encountered the following problems:

- Not all the necessary connections have been established with the underlying databases, which means that not all the available information is displayed on the centralised list. As a result, certain information is missing from the overall picture.
- Certain types of information included in the list are not consistent with each other because incompatible data are listed in the same category. This may cause confusion about the accuracy of the information presented.
- Arrangements about the lists and the underlying databases are still in the course of development. For example, responsibility for certain types of information was still attributed to individuals instead of to (non-person-specific) roles. This exposes the Ministry of Defence to the risk of the list not being properly maintained.

Where there is a need to respond to an IT incident or a calamity (regardless of whether or not this was caused by a cyber attack), the lists can be used to gauge the incident's likely impact. It became clear just how important this was in 2018, when there was a major malfunction in a key generic IT asset at the Ministry of Defence, which also affected the border controls. The evaluation report on the response to the malfunction stated that it was difficult to decide which particular IT assets and services were actually affected by the malfunction. For this reason, the report recommended that the Ministry of Defence should purchase software that would allow the Ministry to maintain a centralised record of the characteristic features of and the interlinkages within the Ministry's IT infrastructure.

4.4 Managing dependencies on external parties

Some of the IT systems used for border controls have been developed by external suppliers. The Ministry of Defence's General Security Requirements for Defence Contracts obliges firms with whom the Ministry signs contracts to meet certain cyber security requirements. The Military Intelligence and Security Service is responsible for clearing potential suppliers. Thus, the firm supplying software for the self-service passport gates has been cleared under the General Security Requirements for Defence Contracts. One of the conditions of this clearance is that the supplier, which is not based in the Netherlands, should not have remote access to the production facility in the Netherlands.

Border controls also depend on the availability of external records and services used for pre-assessments and at the manned passport-control desks and the self-service passport gates. In case of key dependencies, arrangements have been made with the data supplier about the availability of data and the provision of support in the event of malfunctions. In order to further reduce the residual risks, the border guards have access to a local digital copy of lists of wanted persons in case they cannot be consulted live. Although, obviously, this copy is not as up to date as the live lists, we believe that it provides adequate cover for the risks in question.

5 Detecting cyber attacks and vulnerabilities

This chapter examines the detection of vulnerabilities in the IT systems used for border controls, and the rapid detection of potential and actual cyber attacks. In the two sections of this chapter, we examine whether the Ministry of Defence:

- detects cyber attacks directed against the border controls by monitoring the behaviour of IT systems (section 5.1.); and
- uses security tests to identify vulnerabilities in the IT systems used for border controls (section 5.2).

We have included two case studies performed in connection with security tests. The first involves a security test performed on the self-service system (section 5.3), and the second a test performed specially for this audit on the IT system used for the pre-assessments (section 5.4).

5.1 Detecting cyber attacks by monitoring unusual behaviour

Although the Ministry of Defence has facilities for rapidly detecting cyber attacks, the IT systems used for border controls are not connected to this detection capacity. This means that there is a risk of cyber attacks directed against these systems either going unnoticed or not being noticed quickly enough by the Ministry of Defence.

5.1.1 The Ministry of Defence is capable of rapidly detecting cyber attacks

The Ministry of Defence has resources that are capable of monitoring unusual behaviour in IT systems in order to detect any (actual or potential) cyber attacks, identify their impact and take any necessary remedial action. Unusual patterns of behaviour in an IT system, such as large volumes of data traffic or a series of failed log-in attempts, may be evidence of a cyber attack. This is why IT systems need to be monitored, so as to identify any unusual patterns of behaviour.

The Ministry of Defence's Security Intelligence Operations Centre

Most organisations have a specialist department, known as a Security Operations Centre (SOC), whose task it is to detect any unusual patterns of behaviour in IT systems. At the Ministry of Defence, this department is known as the Security Intelligence Operations Centre, or SIOC. The SIOC has both the expertise and the resources that are required to detect unusual patterns of behaviour. Together, these are referred to in this report as the 'detection capacity'.

The SIOC uses security information and event management software (SIEM) to monitor the IT systems used by the Ministry of Defence and identify any unusual patterns of behaviour.

5.1.2 The IT systems used for border controls are not linked up to the SIOC

The IT systems used for border controls and for which the Ministry of Defence is responsible, are not individually linked up to the SIOC's detection capacity. The same applies to the self-service system, for which the Ministry of Justice and Security is responsible and which is also not connected to an SOC. We were unable to ascertain why the systems are not linked up to an SOC. Schiphol N.V. has its own SOC and is planning to monitor the self-service system as soon as it becomes the owner of the system.

The operating systems used by the Ministry of Defence are in fact linked up to the SIOC's detection capacity. The same applies to the interface between the IT systems used for the border controls and the outside world. As a result, it is highly likely that a cyber attack perpetrated from outside and directed against the IT systems used for the border controls would be quickly detected. But because the three IT systems are not linked up to the SIOC's detection capacity, there is less chance of the Ministry of Defence swiftly detecting a direct attack mounted from the inside. In other words, the Ministry of Defence does not have an adequate means of detecting in good time this type of attack directed against a critical process. We tested this attack scenario in a security test that was performed as part of this audit (see section 5.4).

The SIOC has drawn up a timetable showing which IT systems and components it is planning to connect to its detection capacity between the fourth quarter of 2019 and the fourth quarter of 2020. The three IT systems used for border controls do not feature in this timetable. This is despite the fact that the Ministry of Defence already referred specifically to the risks associated with automated border control processes in its Cyber Strategy for 2018.[9]

We were alarmed to see not only that the IT system used for pre-assessments is not connected to the SIOC's detection capacity, but also that the timetable clearly shows that this is not going to happen in the near future. This is despite the fact that connecting the system to the detection capacity was one of the security procedures prescribed as part of the approval procedure for the system (see section 4.1.1). Moreover, the system figures in the Ministry of Defence's list of critical IT systems, which means that it is regarded as being essential to the deployment of Ministry of Defence units.

5.1.3 No systematic approach to the improvement of detection processes

We found that, although the Ministry of Defence has made a start in terms of evaluating and improving its detection processes, it has yet to adopt a systematic approach to the refinement and improvement of these processes.

The SIOC has adopted a number of written procedures in relation to its detection capacity, thus allowing the Ministry of Defence to evaluate them and, if necessary, enhance their effectiveness and efficiency. The SIOC is currently in the early stages of evaluating its detection processes with a view to making them more effective. Whenever the SIOC receives an alert from the SIEM, it assesses whether the SIEM has worked properly. This enables the SIOC to adjust the software configuration if the SIEM is found to issue a large number of false alarms. However, as long as the three IT systems used for the border controls are not linked up to the SIOC's detection capacity, there are no alerts that can be assessed.

5.2 Using security tests to detect vulnerabilities

The Ministry of Defence has the expertise required for performing IT security tests. The Ministry of Defence's security policy stipulates that these tests should be carried out once a year. In practice, however, we found that the security of two of the three IT systems had never been tested. While the third IT system, i.e. the system used for the self-service passport gates, had been tested on one occasion, the test had had a much more limited scope than had originally been intended. As a result, there is a risk of attackers taking advantage of vulnerabilities in the three IT systems that have gone unnoticed.

5.2.1 The Ministry of Defence has the expertise and resources required for performing security tests

The Ministry of Defence has an internal entity, in the shape of the Defence Computer Emergency Response Team (DefCERT), that has the technical expertise and resources required for performing security tests. In order to safeguard their cyber security, organisations need to perform regular security tests in order to actively detect any vulnerabilities, such as weak passwords or obsolete software.

The Ministry of Defence has endorsed the importance of security tests. The Ministry of Defence's security policy includes the following passage:
"Data systems are checked annually to guarantee their technical compliance with security standards and to assess the risks associated with the actual level of security. These checks may take the form, for example, of manual or automated vulnerability scans or pen tests."

Security tests: identifying and exploiting vulnerabilities

Security is one of the aspects of an IT system that need to be tested in order to ensure that it meets the requisite quality standard. A security test involves examining how vulnerable the IT system is to misuse and/or how effective the security procedures are. Broadly speaking, security tests fall into two categories:[10]

- vulnerability scans, the idea of which is to identify vulnerabilities that are inherent to the system and which might attacker might be able to exploit; and
- pen tests (i.e. penetration tests), in which testers try and exploit vulnerabilities in order to undermine the availability, integrity (i.e. reliability) or confidentiality of the IT system.

Any vulnerabilities identified in security tests are assigned a risk category, depending on the risk of the vulnerability being misused and the potential impact of such misuse. The categories used by the Ministry of Defence are 'low', 'average', 'high' and 'critical'. A vulnerability is classified as 'critical' if it is open to easy misuse that could have a massive impact.

Security tests performed by DefCERT

The Defence Computer Emergency Response Team (DefCERT) is the department at the Ministry of Defence that is ideally suited to performing security tests. DefCERT can be requested to perform a variety of security tests, including documentation reviews, advice on new projects and vulnerability and pen tests. These tests may also involve scrutinising physical security. DefCERT puts together a special team of advisers and analysts for every job it is asked to perform. For the purpose of our audit, we interviewed a number of officials from DefCERT and were able to inspect reports on, and action plans for, security tests. Having also seen DefCERT in action in a security test performed for this audit, we were able to conclude that DefCERT is a professional operator that has the skills required for performing security tests.

Vulnerability scans performed by the SIOC

The SIOC also performs vulnerability scans on the IT systems connected to its detection capacity (see section 5.1). These involve checking, for example, whether automatic or key updates have been performed and whether virus scanners are active. The three IT systems used for border controls are not linked up to the SIOC, however, which means that the SIOC does not perform any vulnerability scans on them.

5.2.2 Security testing of IT systems for border controls is limited in scope and not all recommendations are acted on

Although the Ministry of Defence stipulates in its security policy that security tests should be carried out annually, we found that very few of these tests are actually performed in practice. Also, there is scope for improvement in the implementation of the recommendations made.

We looked at whether the three IT systems used for border controls are subjected to security tests in practice, and found that only the system used for the self-service passport gates had undergone a security test. In 2018, a contractor was instructed by the Ministry of Justice and Security to carry out a security analysis of the new software used for the self-service system. This took the form of a document review, involving an assessment of the security aspects of all the technical documents pertaining to the IT system. After reading the report on the review, we concluded that it had not uncovered any critical risks.[11] DefCERT also performed a security test on the software used for the self-service system in 2018, and this test is the subject of our case study in section 5.3.

Despite being prescribed by the Ministry of Defence's security policy, no security tests have ever been performed on the IT systems used for the pre-assessments and the manned passport-control desks. For the purpose of this audit, we set a security test in motion on the IT system used for the pre-assessments. This test was carried out by DefCERT and the method of testing and the test results are described in the case study in section 5.4.

5.3 Case study: security test performed on the self-service passport gates

Method of testing used by DefCERT and partners

In 2018, DefCERT was instructed by the Ministry of Defence to carry out a security test on the IT system used for the self-service passport gates. The immediate reason for performing the test was the installation of a software update. The security test proved difficult to plan and carry out, because of the need to consult all the various parties involved in the self-service project, the lack of prior information and the limited capacity of the parties involved. The parties together decided on the scope of the test and a plan of action. During the implementation stage of the test, DefCERT was unable to test:

- a particular IT component as planned, because Schiphol N.V. felt that doing so would pose a risk to the continuity of airport operations;
- a particular link because the Ministry of Justice and Security decided, shortly before the start of the test, not to allow the link to be included in the test;
- the latest version of the software because the software developers were still working on it at the time of the test. In other words, the latest version of the software was never tested, despite the fact that this was precisely the reason for performing the test in the first place.

Vulnerabilities identified, and DefCERT's conclusions and recommendations

DefCERT concluded that the test, with its adjusted and highly limited scope, had not revealed any critical vulnerabilities in the software. A total of 12 vulnerabilities were identified, including one that was classified as 'high-risk', seven as 'average-risk' and three as 'low-risk'. Examples of these vulnerabilities (which have now been remedied) included the use of simple passwords and failures to update software. DefCERT took the view that further testing would be needed in order to make recommendations about the overall status of the self-service project and the definitive implementation of the new version of the software. The approval of the Ministry of Defence is required for the transfer of ownership of the self-service system to Schiphol N.V. (see section 3.3) and the recommendations made by DefCERT play an important role in this respect.

Action taken in response to findings and recommendations

The head of DefCERT presented the final report on the test, listing the vulnerabilities identified and the recommendations made, to its internal client. Various parties were responsible for acting on the recommendations. DefCERT subjected the findings of the 2018 test to a further test in 2019 in order to ascertain whether the risks had been eliminated. When DefCERT tested 10 of the 12 vulnerabilities identified in 2018, it found that:

- the recommendations made about three of the vulnerabilities had been carried out;
- the recommendations made about seven of the vulnerabilities had not been carried out, and the Ministry of Justice and Security had decided to temporarily accept the risks involved.

Of the seven recommendations that had not been acted on, one was categorised as 'high-risk' and three as 'average-risk'. All of them were connected with access security and user rights in relation to the self-service system. DefCERT said that the time limits it had recommended for the implementation of its recommendations had not been met. The seven recommendations that have yet to be acted on all require action on the part of Schiphol N.V. and the software supplier. As the owner of the system, the Ministry of Justice and Security is responsible for ensuring that such action is taken.

5.4 Case study: security test performed by the Netherlands Court of Audit on the IT system used for pre-assessments

Method of testing used by the Netherlands Court of Audit and DefCERT

For the purpose of this audit, we instigated a security test on the IT system used for carrying out pre-assessments. The test was performed by DefCERT. Although the Ministry of Defence's security policy requires such tests to be performed annually, the Ministry of Defence had never actually tested the IT system used for pre-assessments. The starting point for the test was an insider threat, i.e. a cyber attack perpetrated by a Ministry of Defence employee who has access to the Ministry's network but is not authorised to access the pre-assessment system. Our reason for using this scenario was that it meant that the attacker had already crossed the main barriers, such as gaining access to the Ministry's network or to a physical Ministry of Defence site. Moreover, a cyber attack perpetrated by a member of the Ministry's staff is not unimaginable: not only does the Ministry employ a staff of around 60,000, but the Ministry of Defence's security policy also refers specifically to an 'internal attacker' as a potential threat. We wanted to find out whether it would be possible for a Ministry of Defence employee to gain unauthorised access to the IT system used for pre-assessments, and then to manipulate the system and/or to access or modify certain data, including personal data.

At our request, DefCERT prepared a plan of action for this security test in consultation with various other parties at the Ministry of Defence. The test included both a vulnerability scan (i.e. designed to identify vulnerabilities) and a pen test (i.e. designed to take advantage of vulnerabilities). DefCERT carried out the test in November 2019 at one of the Ministry of Defence's sites. The unfiltered results of the test were shared simultaneously with us and the Ministry of Defence.

DefCERT's findings, conclusions and recommendations

The test was performed according to plan. DefCERT identified 11 vulnerabilities in the IT system used for pre-assessments. None of these were categorised as 'critical'. Five were categorised as 'high-risk', three as 'average-risk' and three as 'low-risk'. Examples of these vulnerabilities (which have now been remedied) include the following:

- the use of a standard password that could be traced with the aid of the (Googled) user manual for the system;
- the possibility of assigning management rights and hence acquiring control over a server in the Ministry of Defence's central management platform. Hundreds of Ministry of Defence applications are connected to this platform, including critical ones;
- the possibility of sending emails on behalf of random Ministry of Defence officials, such as the Chief of the Defence Staff. Because the sender looks familiar to the recipient, these emails look authentic and can induce the recipient to click on fraudulent hyperlinks;
- the use of outdated software (including one software package that had no longer been supported since 2016), which means that security updates are no longer issued for them.

One of the main conclusions drawn by DefCERT was that, by combining a number of vulnerabilities, it would be able to gain access to the pre-assessment system and hence manipulate it. In this scenario, an intruder would be able to access passenger data and, in the event of a complex attack, would even be able to generate a false negative, i.e. the system would

report that a passenger was not on a list of wanted persons, even though he or she was. The risk associated with a false negative in a pre-assessment is limited as the border guards carry out a second check against the list of wanted persons at the border crossing point. However, the only point at which the border guards perform an automated check of whether certain passenger characteristics (such as the itinerary, nationality and travel companions) match a given risk profile is during the pre-assessment. A false negative could mean, for example, that a passenger whose profile matches that of a people smuggler would not easily be detected. The attack scenario was not played out, however, as it would have involved deceiving Ministry of Defence staff (i.e. using 'social engineering'), which the plan of action had ruled out. However, there can be no doubt that the scenario was both realistic and practicable.

Ministry of Defence's response to the test findings and recommendations

The report issued by DefCERT prompted the security authority at the Ministry of Defence order the problems identified in the report to be resolved. A number of high-priority issues were immediately remedied, thus eliminating the risk of the attack scenario described by DefCERT materialising in practice. The Ministry of Defence drew up a timetable for dealing with the remaining issues. All activities designed to address high-priority issues were scheduled for the first quarter of 2020. By mid-February 2020, about half of these activities had been completed, which meant that the Ministry of Defence had remedied four of the five high-priority issues..

6 Response to cyber incidents and crises

This chapter examines the way in which the Ministry of Defence responds to incidents and crises caused by a cyber attack. It assesses whether:

- procedures have been adopted for responding to incidents and crisis situations caused by a cyber attack, whether these procedures are complete and how they operate in practice (section 6.1);
- exercises are held in practice involving incidents and crisis situations caused by a cyber attack (section 6.2).

A cyber incident is a relatively minor, isolated disruption of routine processes caused by an individual with malicious intent. A cyber crisis, on the other hand, is defined as a long-term and/or complex disruption of IT systems caused by a cyber attack. It is possible for a cyber incident to evolve into a cyber crisis, as in the case of ransomware that first infects a single computer before penetrating an entire computer network.

Cyber incidents and crises in practice

Our audit team was not able to assess how the Ministry of Defence and the border guards responded to an actual cyber incident or crisis, as the border controls at Amsterdam Schiphol Airport had not been affected by any such incident or crisis at the time when we performed our audit. Nonetheless, there was a major IT malfunction in 2019 that illustrated the impact that a digital malfunction could have on airport processes.

In June 2019, an IT problem prevented checks from being carried out to see whether the names of incoming passengers appeared on lists of wanted persons. This resulted in long queues forming at the border crossing point, with the risk that large numbers of passengers would miss their flights and that other airport processes would be disrupted. In these types of situations, the Schengen Agreement permits the border guards to make an exception and allow large numbers of passengers to pass the border with only minimal checks. This is what happened for over one hour in June 2019. It is an undesirable situation that the border guards are always keen to prevent, but which they are sometimes compelled to accept during a crisis because of all the other interests that are at play.

6.1 Procedures for cyber incidents and crises

The Ministry of Defence has drawn up procedures describing the nature of the response to IT malfunctions. These include a separate procedure for breakdowns and problems caused by a cyber attack. As no scenarios have been prepared for specific cyber attacks such as with ransomware, there is a risk of a response having to be highly improvised.

6.1.1 The Ministry of Defence has general procedures for IT malfunctions

The Ministry of Defence has adopted detailed procedures for dealing with IT malfunctions, which means that staff can rely on predefined procedures and action plans in uncertain and unpredictable situations. These enable staff to maintain a firm grip on the situation and the Ministry to work gradually towards a solution.

The Ministry's procedures for incidents and crises set certain targets for the speed with which problems should be resolved. If a system is out of action for too long or if data are lost, procedures have been put in place for an incident to be scaled-up to a calamity and, if necessary, even to a crisis. The relevant roles, tasks and responsibilities are all described in detail. The procedures also clearly describe how staff should be informed about the situation and contain methods for analysing the cause of the problem. The response is evaluated once a major malfunction has been resolved or has ended, and these evaluations result in the adoption of measures to prevent a recurrence of the same problem in the future.

6.1.2 Procedures designed specifically for cyber incidents

The Ministry of Defence's Joint IV Command (JIVC) has adopted a procedure designed specifically for responding to a cyber incident. This procedure must be triggered if it becomes clear, when dealing with an incident in accordance with the general procedures, that it has been caused by a cyber attack. We should point out that we did not find out about the existence of this specific procedure until a late stage of the audit. The members of JIVC staff whom we initially interviewed did not tell us about the procedure when we asked them about it. It would seem that its existence is not common knowledge among Ministry of Defence staff. Moreover, the general procedure does not contain any explicit references to the specific procedure. The Ministry of Defence has made clear that the calamity manager who is responsible for dealing with the malfunction is also responsible for initiating the specific procedure for responding to a cyber incident.

The specific procedure does not contain any cyber-attack scenarios. This is despite the fact that a cyber incident is capable of throwing up highly specific dilemmas, for example where systems are infected with ransomware and the attackers demand the payment of ransom.[12] It became clear, during an interview with staff from Schiphol N.V., that a crisis exercise at the airport had sparked a debate on this very point due to the absence of guidelines about such situations.

Other situation-specific challenges may stem from unauthorised access being obtained to passenger data, for example as a result of cyber espionage. Procedures need to be formulated in advance for dealing with this type of cyber crisis situation, for example for notifying the Dutch Data Protection Authority as well as the victims of a data breach.

Various public-sector and private-sector parties are involved in border controls. The process of drawing up a procedure in advance may reveal certain areas where there is a lack of clarity or a conflict of interests, such as between commercial and security interests. These need to be discussed and clarified in advance, so that the parties know exactly how they should act and what to expect from each other in an actual crisis situation.

6.2 Practical exercises with cyber security incidents and crises

The Ministry of Defence organises exercises as a means of preparing for a cyber crisis. The Ministry also takes part in exercises organised by other parties, such as NATO or the National Cyber Security Centre (NCSC). The border guards are aware of the important role they play and the potential impact that an IT malfunction could have on border controls. The Border Controls Brigade takes part in quarterly crisis simulations at Amsterdam Schiphol Airport. There has not to date been an exercise scenario involving a cyber crisis and no such exercise is planned for the future.

The border controls operated by the border guards at Amsterdam Schiphol Airport form part of a chain of public-sector and private-sector parties in which decisions constantly need to be made based on an assessment of the relative interests of security and mobility. Any disruption of border controls can affect the entire airport. A cyber attack is a realistic risk that will most probably pose new challenges to both the border guards and Schiphol N.V. For this reason, we believe that the failure to hold any practical exercises with this scenario to date constitutes a risk. Moreover, procedures cannot be evaluated and improved without being tested.

7 Conclusions and recommendations

IT plays a crucial role in the border controls at Amsterdam Schiphol Airport and is set to become even more important in the near future. Our audit of the cyber security of the border controls showed that, despite the availability of the requisite expertise and procedures, the cyber security procedures adopted are not as effective in practice as they could be.

As more and more use is made of IT in operating border controls, so the cyber security risks will rise. In the light of all the technological advances that are set to take place in the coming years, we believe that the current level of cyber security in relation to the border controls operated by the border guards at Amsterdam Schiphol Airport is not adequate and hence is not future-proof.

Multiple public-sector and private-sector parties are involved, and they do not all share the same interests. In the case of the self-service passport gates, we found that Schiphol N.V. has an interest in the rapid refinement of the system, whereas the border guards – as the users of the system – are interested primarily in its stability and security. Moreover, a high level of coordination among the various parties is needed. As a result, there were problems with a joint security test of the self-service system, which led to the test being more limited in scope than had originally been planned. The same applies to the security requirements that the self-service system needs to satisfy: here too, the parties are dependent on each other. There is a risk that the interests of cyber security may become subordinated to those of airport operations, including the commercial interests.

Border controls are set to undergo further automation in the coming years. Their complexity and dependency on IT is also set to grow, in line with a rise in the number of systems, interlinkages and data sets. To a certain extent, the process of ongoing automation is the result of EU-wide agreements. Schiphol N.V. is one of the driving forces behind the Seamless Flow project. In the future, Schiphol N.V. will also be taking over the ownership of the self-service system from the Ministry of Justice and Security. With these future developments in mind, there is a need to guarantee now that the level of cyber security is already adequate. We found that the Ministry of Defence already possesses the necessary expertise. For this reason, our recommendations centre mainly on ensuring that everything possible is indeed done. We find it incomprehensible that this has not been the case to date.

Hardly any action has been taken to protect IT system used for border controls

Measures taken to protect the security of IT systems:

- Not implemented
- Partially implemented
- Implemented

Owner	Ministry of Defence	Ministry of Justice and Security	Ministry of Defence
Approved for use	●	●	●
Security tests carried out	●	●	● *
Connected to detection capacity	●	●	●

* At our request, this security test was performed as part of the audit.

Figuur 6 *Cyber security procedures adopted in relation to IT system*

7.1 Two of the IT systems used for border controls have not been approved

The Ministry of Defence's security policy states that security procedures should be adopted for IT systems on the basis of risk assessments. Key IT systems may not be taken into use until these measures have been implemented. However, the Ministry of Defence's IT system as used by the border guards at the manned passport-control desks is operational despite the fact that it has not received the requisite approval. This does not mean that the system is insecure, but rather that there are no guarantees that it is secure.

The Ministry of Justice and Security is responsible for organising the self-service system at the border crossing point. Although it has been decided that the system should be subject to the same approval procedure in accordance with Ministry of Defence policy, it too is operational even though the agreed cyber security procedures have not been implemented. Again, there are no guarantees that the system is capable of withstanding a cyber attack.

We urge the Minister of Defence to:

1. ensure that the requisite security procedures are adopted as swiftly as possible in relation to the IT system used for the manned passport-control desks, so that the approval procedure can be completed in accordance with the Ministry's security policy.

We urge the Minister of Justice and Security to:

2. ensure that the self-service system is subjected as swiftly as possible to the approval procedure prescribed by the Ministry of Defence's security policy, that Schiphol N.V. adopts, both now and in the future, all the requisite security procedures, and that the system is approved by the security authority at the Ministry of Justice and Security;
3. reconsider whether the planned transfer of ownership of the self-service system to Schiphol N.V. is accompanied by sufficient cyber security safeguards.

7.2 The systems used for border controls are not connected to the Security Operations Centres

There is a risk of cyber attacks directed at the three IT systems used for border controls either not being detected or not being detected in time. As the three IT systems used for the border controls are not linked directly to the detection capacity of a Security Operations Centre (SOC), only a certain proportion of any cyber attacks mounted against the border controls are open to immediate detection. This applies both to the two systems for which the Ministry of Defence is responsible, and to the self-service system owned by the Ministry of Justice and Security.

An SOC can use its detection capacity to see whether a digital attack is being mounted against IT systems. The Ministry of Defence has established an SOC known as the SIOC. Schiphol N.V. also has its own SOC. The presence of an SOC is an important prerequisite for an adequate cyber security policy. However, the systems used for border controls are not connected to this detection capacity, despite the fact that adjacent IT components such as interfaces and operating systems are linked up. This represents a risk, as an SOC cannot swiftly detect a direct attack against the IT systems. Even though the Ministry of Defence has classified one of the IT systems, i.e. the system used for pre-assessments, as a 'critical system', there are nonetheless no plans for connecting it to the SIOC.

We urge the Minister of Defence to:

4. connect the two IT systems used for border controls for which the Ministry of Defence is responsible as swiftly as possible to the detection capacity of the Ministry's SOC, and to give the highest priority to the pre-assessment system (classified as 'critical').

We urge the Minister of Justice and Security to:

5. ensure that the self-service system is connected as swiftly as possible to the detection capacity of Schiphol N.V.'s SOC.

7.3 Inadequate security testing of IT systems used for border controls

In practice, the Ministry of Defence and the Ministry of Justice and Security have performed little or no security testing on the three IT systems used for border controls. This is despite the fact that the Ministry of Defence's security policy states that annual security tests are compulsory. The one security test that was performed was limited in scope and only some of the recommendations based on its results have been implemented.

The Defence Computer Emergency Response Team (DefCERT) is the department at the Ministry of Defence that is equipped to perform security tests. In practice, however, hardly any security tests have been performed, if at all, on the three IT systems used for border controls. For example, no security tests have been performed on the IT systems used for pre-assessments and the manned passport-control desks. Although the self-service system has been tested, the test took a long time to complete, and was more limited in scope than had originally been intended. Also, only a limited number of DefCERT's recommendations have been put into effect, and the implementation process took a long time: a review performed one year after the software test found that action had been taken in respect of just three of the ten original findings. This means that there is a risk of unidentified vulnerabilities in the system remaining undetected and of their being open to misuse by cyber attackers.

A security test performed on the pre-assessment system in November 2019 at the request of our audit team revealed 11 vulnerabilities. By taking advantage of a combination of these vulnerabilities, a cyber attacker would be able to gain access to passenger data and manipulate the system. The Ministry of Defence responded by taking immediate action to prevent such an attack. The results of the test underline the importance of security testing.

We urge the Minister of Defence and the Minister of Justice and Security to act jointly in:

6. subjecting the three IT systems used for border controls as swiftly as possible to annual security testing in accordance with the Ministry of Defence's security policy, and in ensuring that recommendations are implemented.

7.4 Response to cyber incidents

The Ministry of Defence has adopted detailed procedures for dealing with IT failures. These include a specific procedure for responding to a cyber incident. The idea is for all the various parties to form a chain in such an event. No exercises have yet been held in order to demonstrate whether the procedures work well in practice should the border controls fall prey to a cyber attack. As a result, there is a risk of the parties, when acting together in a crisis situation, not responding adequately to a cyber attack.
A cyber attack mounted against the border controls may have certain specific characteristic features and consequences for which no preparations have yet been made. In the case of ransomware, for example, it is important to consider in advance the eventuality of having to pay a ransom. This type of scenario is not explicitly mentioned in the procedures. Exercises can help the parties to form a good team and can uncover any conflicts of interest, thus ensuring that no time is wasted and reducing the need for improvisation in a crisis situation.

We urge the Minister of Defence and the Minister of Justice and Security to act jointly in:

7. ensuring that the Ministry of Defence and the Ministry of Justice and Security work together with all partners in the chain in conducting exercises in managing crises caused by a cyber attack directed against the three IT systems used for the border controls at Amsterdam Schiphol Airport.

8 Ministers' response and Court of Audit afterword

The Minister of Defence and the Minister of Justice and Security responded to our report on 27 March 2020. Their responses are reproduced below. The chapter concludes with our afterword.

8.1 Responses of the Minister of Defence and the Minister of Justice and Security

We have read your audit report, entitled *Cyber security of border controls operated by Dutch border guards at Amsterdam Schiphol Airport*, with great interest. Against the background of the increasingly prominent role played by IT, cyber security has become an important issue in society today. We need to prepare ourselves for sophisticated digital threats and their potential effects. This is why the issue is of such concern to us. Day in, day out, a large number of experts at both the Ministry of Defence and the Ministry of Justice and Security actively seek to ensure that our border controls are secure, now and in the future.

A range of measures have been put in place to contain the risks and potential impact of a cyber attack directed against the IT systems at Amsterdam Schiphol Airport. Should these systems be put out of action for whatever reason, border controls will continue to be performed, but on a manual basis.

In line with your report, we recognise that the growing role played by IT systems in the border controls at Amsterdam Schiphol Airport means that further improvements need to be made and we endorse your recommendations in this respect. At the same time, we also recognise that we face immense challenges in relation to cyber security and that the IT landscape in relation to border controls is a dynamic one. We are already acting on many of the recommendations. Against this background, we are unable to guarantee at this moment whether we will be able to implement all your recommendations within the time limits or with the frequency you suggest.

We respond to your recommendations in greater detail in the following sections, in which we also describe the nature of the measures we have adopted and the reasons for adopting them.

Recommendations

Completion of the approval procedure (recommendations 1 and 3)

You recommend that the requisite security procedures be adopted as swiftly as possible, so that the approval procedures for the manned passport-control desks and the self-service system can be completed.

The IT system used for the manned passport-control desks last underwent an approval procedure in 2016. As no any major alterations have been made to the design of the system since then, the results of the 2016 procedure allow us to make an effective analysis of its security. Based on this analysis, the Ministry of Defence believes the level of risk to be both low and acceptable. The system is currently undergoing adjustments and additional security procedures are being put in place so as to provide better guarantees of the system's operational availability in the future. In order not to delay this process, it has been decided to complete the approval procedure, which was initiated in 2019, as soon as the necessary adjustments have been made.

As concerns the self-service system, we have identified the security measures that need to be taken and are planning to implement them as soon as possible. The approval procedure can then be completed once this has been done.

Connection to the detection capacity (recommendations 2 and 5)
You recommend that the IT systems included in your audit should be connected as swiftly as possible to the detection capacity of both the Ministry of Defence and Schiphol N.V. The Ministry of Defence set up its own Security Operations Centre (SOC) in 2017 so as to be able to carry out detection checks on its IT systems, whether as requested by the Ministry or at the SOC's own initiative. As it is not possible for all the systems to be connected to the SOC at the same time, we have decided that this should be done in stages. Precedence will be given to those IT systems that the Ministry regards as having the highest priority. The situation at present is that priority is being given to other critical systems, which are regarded as being more urgent.

The systems used for the manned passport-control desks and the pre-assessments are part of a network that is already connected to the SOC. This means that a number of the relevant risks are already covered. The individual systems will be connected to the SOC in due course in order to ensure that the remaining risks are also covered.

The self-service system is currently being connected to the detection capacity of Schiphol N.V.'s SOC. This is one of the security measures adopted as part of the approval procedure.

Security tests (recommendation 6)
You recommend that the three IT systems included in your audit should be subjected to annual security testing. It has been decided that the Ministry of Defence's 14 critical systems, one of which is the IT system used for pre-assessments, should be required to pass the approval procedure every three years. This three-year cycle includes a security test, as well as measures for implementing the recommendations made on the basis of the test results. It is not feasible to increase the frequency of testing in the near future, due to the large number of systems involved, the limited number of staff who are capable of performing the tests, and the amount of time required to put all the recommendations into practice.

The above cycle does not apply to the self-service system. This will be subjected to a new security test at the earliest possible date. The results will be used for further improving security. We are hoping to start testing the self-service system on an annual basis is 2021.

Conducting exercises with cyber attacks (recommendation 7)
You recommend conducting exercises in managing crises caused by a cyber attack at Amsterdam Schiphol Airport. We will get together with the relevant partners in the supply chain to discuss when such an exercise can be organised.

Transfer of ownership of the self-service system to Schiphol N.V. (recommendation 4)
You recommend reconsidering the planned transfer of ownership of the self-service system from the Ministry of Justice and Security to Schiphol N.V. Before a decision is taken on the transfer of the system's ownership to Schiphol N.V., we will first assess the most effective way of safeguarding the security of the system. This ties in with the approval procedure under the Ministry of Defence's security policy, which the self-service system is currently undergoing. The completion of the approval procedure and the system's ability to meet the security requirements on a permanent basis are two preconditions for transferring the ownership of the system to Schiphol N.V.

In conclusion
We would like to thank the Court of Audit for performing the audit and making the recommendations. Your audit report is an important contribution to the debate on the opportunities and risks created by automation.

8.2 Court of Audit afterword

The Minister of Defence and the Minister of Justice and Security recognise that the increasingly important role played by IT has created a need for improving the cyber security of border controls. They point to the range of cyber security measures that have already been put in place. The ministers claim moreover that, in the event of the IT systems being disabled, the border controls will continue to be performed, but on a manual basis. We would like to point out that the fall-back option of manual border controls will cause delays and comes with a risk of error.
The ministers state that not all recommendations can be implemented immediately and in full. By drawing up an implementation timetable, the ministers could make clear how priorities are set and what the accepted level of risk is. We urge the ministers in any event to inform the Dutch House of Representatives about the approval procedures and the process of connecting the Ministry of Defence's 14 critical IT systems to its SOC.

As regards the security tests, we are extremely concerned by the assertion that even the Ministry of Defence's 14 critical IT systems cannot be tested more frequently than once every three years. This is also contrary to the Ministry of Defence's security policy, which prescribes annual security tests. New vulnerabilities, threats and attack scenarios can easily come into being within the course of a year. IT systems must be tested on an ongoing basis to ensure that they are capable of resisting an attack. The vulnerabilities revealed by the test performed for this audit, such as the use of out-of-date software, underline the importance of annual testing. In this respect, we welcome the ministers' plans for testing the self-service system on an annual basis.

We intend to closely the monitor the progress made in implementing our recommendations and will report on our findings as and when we feel this is necessary.

Appendices

Appendix 1 Audit methods

Audit questions

This report seeks to answer the following audit questions:

1. What is the context of the border controls operated by the border guards at Amsterdam Schiphol Airport? What processes are involved? What IT systems are used to support the border controls?
2. What preventive cyber security procedures have been taken in relation to the IT systems used for the border controls?
3. What measures have been taken for detecting cyber attacks and are these adequate?
4. How do these detection measures operate in practice? Do they offer sufficient protection?
5. What response scenarios have been developed for cyber incidents? Are they adequate?
6. How do the response scenarios operate in practice? Are they adequate?

Criteria

We used the cyber security framework adopted by the National Institute of Standards and Technology (NIST) as our guide in answering audit questions 2-6. The NIST is part of the US Department of Commerce. Its cyber security framework is widely used all over the world and has links with security standards and models such as ISO 27001 and COBIT. The framework consists of five main functions two of which, i.e. Detect and Respond, are particularly relevant to our audit. We used the categories into which these two main functions are divided as tools for analysing the wide range of activities performed in relation to the cyber security of border controls. Our final opinion on the cyber security of the border controls is not based exclusively on whether or not it meets the specific criteria listed in the NIST framework. Our opinion is qualitative, and is based on our findings in a broad sense in relation to each category. See Appendix 2 for a list of the NIST categories we used and their place in the report.

Audit activities

Based on the categories listed in the NIST framework, we contacted the Ministry of Defence and the Ministry of Justice and Security in order to select interviewees and topics. We then asked to be given relevant documents and conducted a series of interviews. Following the interviews, we checked the information we had been given against the information in a number of supplementary documents. For the purpose of the audit, we made working visits to the border guards both at Amsterdam Schiphol Airport and at the location where the pre-assessments are made. We also initiated a security test of one of the IT systems used for border controls. A team of experts from the Ministry of Defence

(viz. DefCERT) performed a security test to assess the practical resilience of the system we had selected in the test situation we had proposed. The unfiltered results of the test were shared simultaneously with us and the Ministry of Defence. Following the completion of the audit, we presented our findings to the Ministry of Defence and the Ministry of Justice and Security. We took account of the comments we received from officials at both ministries in drawing up this final draft of the report.

Case studies

As no cyber attacks against the border controls have been detected to date, we were unable to evaluate the workings of cyber security in practice. We were, however, able to make use of the evaluation of a major IT failure in the past (which was not caused by a cyber attack), as well as of the results of a security test previously performed by DefCERT on the software used by the self-service system. The scenario used for the security test of the pre-assessment system performed as part of this audit was based on our own risk assessment.

Appendix 2 Audit criteria

The following table lists the categories from the NIST's Cyber Security Framework that we used for this audit. Shown alongside each category is a description of our main expectations during the audit and the section of the report in which our findings are outlined.

Tabble 1 *List of main expectations for each NIST category*

NIST category	Main expectations	Section
Governance	Coherent cyber security policy; clear responsibilities; roles and responsibilities coordinated and aligned with internal roles and external partners.	4.2
Information Protection Processes and Procedures	Security policies and procedures are maintained and used to build and configure systems and assets, depending on the degree of risk.	4.1
Protective Technology	Technical security solutions are used to protect systems against cyber attacks.	4.1
Risk Assessment	Threats are analysed using a variety of sources and the analyses are used in order to determine the level of measures required.	4.1
Asset Management	IT resources are inventoried and catalogued, and this information is used for performing cyber security analyses.	4.2
Supply Chain Risk Management	Cyber supply chain processes, components, contracts, checks and balances are identified in order to mitigate the degree of risk.	4.4
Anomalies and Events	An inventory is made of the normal operation of IT systems and indicators (i.e. events) that could point to a cyber attack being made.	5.1
Security Continuous Monitoring	IT systems are constantly monitored to detect potential cyber security events, with the aid of an SIEM and regular security tests.	5.1 5.2
Detection Processes	Information on the operation of detection processes, which are improved on the basis of evaluation results.	5.1
Response Planning	Procedures are maintained for responding to a cyber incident or crisis; the parties concerned and their roles, responsibilities and objectives are defined in these procedures.	6.1
Communications	Response activities are communicated to and coordinated with internal and external stakeholders in the supply chain.	6.1
Analysis	Processes are established to analyse an incident or crisis, as a basis for an adequate response.	6.1
Mitigation	Activities are established for different types of cyber attacks, in order to resolve a crisis and revert to normality.	6.1
Improvements	Exercises and evaluations of cyber incidents and crises, and proposals for improving the response.	6.1 6.2

Appendix 3 Key to abbreviations and technical terms

Cyber security	A set of mechanisms and procedures for preventing damage caused by the disruption, failure or misuse of IT systems and to repair any damage thus caused.
Dark web	A secret part of the internet that cannot be found using regular browsers and search engines. It is best known as a hotbed of criminal activity.
DefCERT	Defence Computer Emergency Response Team
EES	Entry/Exit System
ESTA	Electronic System for Travel Authorization
ETIAS	European Travel Information and Authorisation System
False negative	A test result which wrongly indicates a negative
Hack	Gain access to a computer, network, hardware or software. This is illegal if access is unauthorised or if done without a proper reason.
Insider threat	A threat to an organisation that comes from within the organisation. If an employee, a former employee or a supplier takes advantage of his or her position to perform malicious activities, this is regarded as constituting an insider threat.
JIVC	Joint IV Command
Malware	Software used by attackers to gain remote access to an IT system in order to damage it or steal information. It is a contraction of 'malicious software'.
NCSC	National Cyber Security Centre.
Pen test	Short for 'penetration test', in which an organisation tests the practical effectiveness of its digital security by hacking into its own IT systems.
Ransomware	A type of malicious software in which the attacker blocks access to an IT system or files and demands payment of ransom before the system or files are released.
Seamless Flow	A new system based on facial recognition technology that is designed to streamline the passenger process at Amsterdam Schiphol Airport, from check-in to boarding.
SIEM	Security Information and Event Management software
SIOC	Security Intelligence Operations Centre
SOC	Security Operations Centre

Appendix 4 Bibliography

Publications

Cyberveilig Nederland (2019). *Cybersecurity Woordenboek (2019) Van cybersecurity naar Nederlands*. The Hague: own publication.

Ministry of Defence (2017). *Introductiebundel Defensie*. Den Haag: own publication.

National Coordinator for Security and Counterterrorism (2018). *National Cyber Security Agenda, A cyber secure Netherlands*. The Hague: own publication.

National Coordinator for Security and Counterterrorism & National Cyber Security Centre (2019). *Cybersecuritybeeld Nederland 2019*. The Hague: own publication.

Netherlands Court of Audit (2019a). *Cyber security and critical water structures*. The Hague: own publication.

Netherlands Court of Audit (2019b). *Rapport bij het jaarverslag 2017 Ministerie van Defensie (X)*. The Hague: own publication.

Netherlands Scientific Council for Government Policy (2019). *Preparing for Digital Disruption*. The Hague: own publication.

Legislation

General Data Protection Regulation (Implementation) Act.

Government Accounts Act 2016. Act of 22 March 2017 regulating the management of, the distribution of information on, the auditing of and the reporting on central government finances, on the management of public liquid assets held outside the Kingdom, and on the supervision of the management of public liquid assets and public financial assets held outside the Kingdom.

Network and IT Systems (Security) Act. Act of 17 October 2018 regulating the implementation of Directive (EU) 2016/1148.

Network and IT Systems (Security) Decree. Decree of 30 October 2018 regulating the enforcement of the Network and IT Systems (Security) Act.

Regulation (EC) No 562/2006 of the European Parliament and of the Council of 15 March 2006 establishing a Community Code on the rules governing the movement of persons across borders (Schengen Borders Code).

Appendix 5 Endnotes

1. A commonly used list of critical processes is that adopted by the National Coordinator for Security and Counterterrorism. 'Handling flights and aircraft' is one of the processes on this list. This includes border controls at airports.
2. Netherlands Court of Audit, State of Central Government Accounts 2018, p. 39.
3. For further information, see the ACI Europe Airport Industry Connectivity Report 2019.
4. It was announced in June 2019 that passenger information had been stolen in a cyber attack mounted against the US border protection agency. This information, including photographs of passengers, subsequently surfaced on the dark web. The personal data of 9.4 million passengers, including passport and credit card details, were stolen when Cathay Pacific was hacked in October 2018. One month before that, information on 380,000 passenger transactions had been stolen from British Airways.
5. This system is known as EES (Entry/Exit System).
6. For further information, see https://magazines.defensie.nl, for example.
7. This is no more than a rough outline of the border crossing procedures. Where the self-service passport gates are concerned, for example, nationals of certain countries (such as the US and Japan) are entitled to use the gates when leaving the Netherlands provided that their passports are suited for use with them.
8. Organisations can ask the NCSC for information on the security aspects of the latest hardware and software vulnerabilities. The NCSC also publishes a weekly list of all the security information it has sent during the past week, as well as a list of media articles and posts on cyber security during the same week.
9. Page 11 of the Defence Cyber Strategy for 2018.
10. The same distinction is also made in the Government Information Security Baseline Survey.
11. lthough our audit team found that the IT systems used for border controls had been subjected to a number of other tests, there is no immediate reason for classifying these as security tests. Although concerned with the quality of the software, they do not specifically address the issue of cyber security. For example, functional tests were performed in order to ascertain whether systems were operating in accordance with the requirements set by the International Civil Aviation Organisation (ICAO). The source code used by the self-service system and the face recognition algorithm is also subject to regular testing.
12. There has been a rise in the use of ransomware in recent years. When Maastricht University suffered a ransomware attack at the end of 2019, the university ended up paying a ransom to the attackers so as to be able to decrypt data that had been encrypted.

Information

Communication Department
P.O. Box 20015
2500 EA The Hague
The Netherlands
+31 70 342 44 00
voorlichting@rekenkamer.nl
www.courtofaudit.nl

Cover

Design: Corps Ontwerpers
Photo: Ton Koene/Alamy Stock Photo

Translater

Tony Parr Business Translations

Den Haag, April 2020