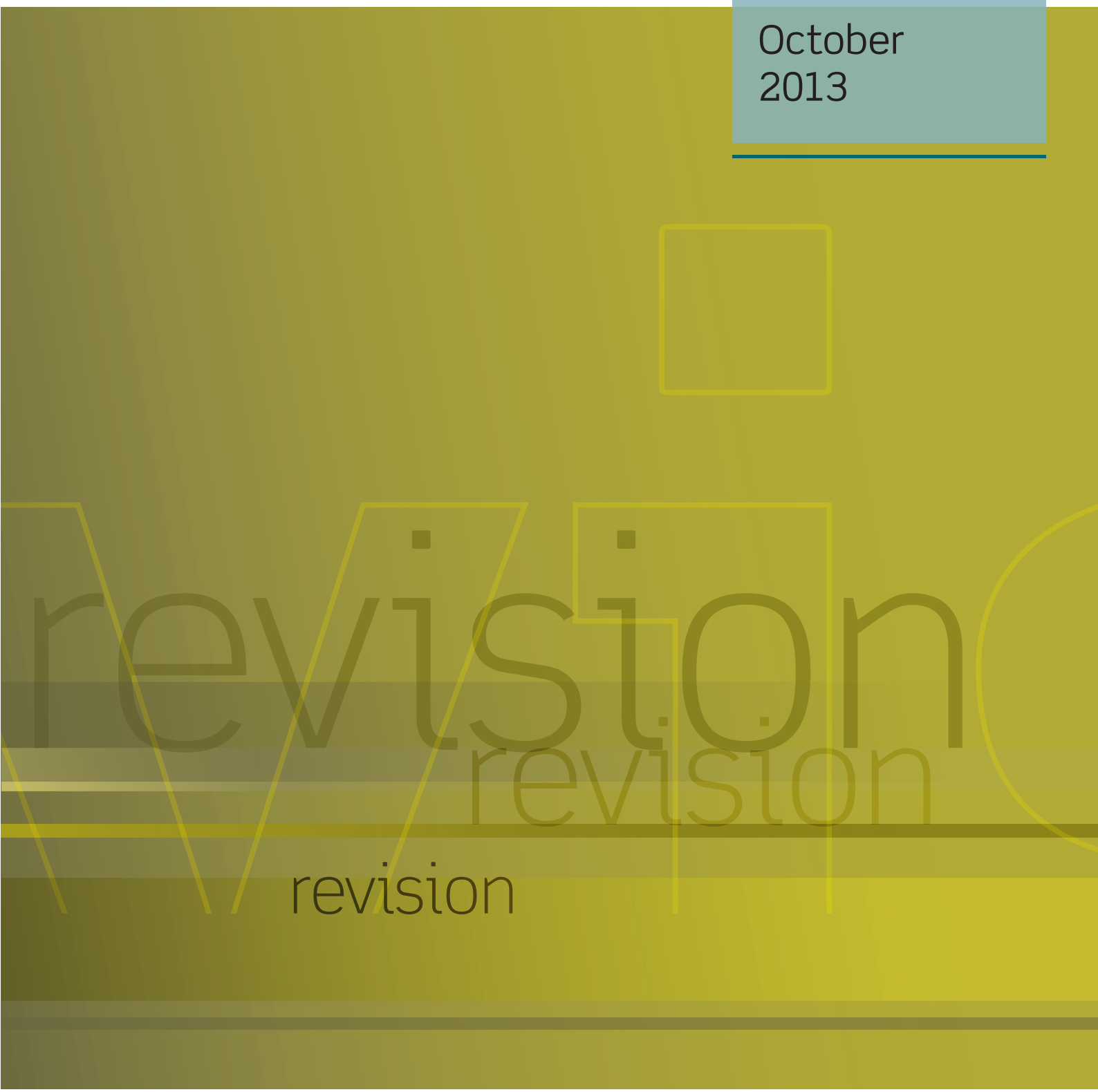
RIGSREVISIONEN

# Report to the Public Accounts Committee on mitigation of cyber attacks

October 2013



# Table of contents

Rigsrevisionen submits this report to the Public Accounts Committee under section 17(2) of the Auditor General's Act, see Consolidation Act No. 101 of 19 January 2012.

The report relates to the Danish Appropriation Act, section 7. The Ministry of Finance, and section 29. The Ministry of Climate, Energy and Building.

In the period during which the examination was carried out, the ministries were headed by the following ministers:

*The Ministry of Finance*
Bjarne Corydon: 3 October 2011 -

*Ministry of Climate, Energy and Building*
Martin Lidegaard: 3 October 2011 -

# I. Introduction and conclusion

1. This report concerns the action taken by Danish government bodies to prevent cyber attacks. Behaving sensibly in cyberspace to avoid attacks is important, but should be supplemented by technical security controls that can increase security and mitigate cyber attacks.

*In this report, **cyber attack** is referring to an intruder's attempt to gain unauthorised access to a computer system or data. The purpose of a cyber attack depends on the intruder, e.g. a foreign state, a criminal organisation or individuals who operate on their own and abuse the internet.*

2. As e-government is expanding so is the need for government bodies to protect themselves from cyber attacks and abuse of their IT systems and confidential data. Attacks on several government bodies in recent years have accentuated the need for increased security.

3. International studies have concluded that three central security controls can prevent the majority of the currently known types of attacks,

- technical restriction of download of programmes;
- limited use of local administrators;
- systematic software updates.

Rigsrevisionen has therefore assessed whether the government bodies in the study have addressed the risk of cyber attacks and whether they have implemented these three security controls. The agencies included in the study are the Agency for Governmental IT Services, the Danish Agency for Digitisation, the department of the Ministry of Climate, Energy and Building and the Danish Energy Agency.

***Security controls**; a practise or mechanism designed to improve IT security, i.e. measures that are implemented to mitigate errors and risk of loss and abuse of data, and to secure access to data and systems.*

Rigsrevisionen has also examined whether the Danish Agency for Governmental IT Services has managed the risk that an attack on one inadequately secured agency can spread to other agencies, for instance, through shared services (joint solutions). The Danish Agency for Governmental IT Services was established in 2010 and is currently providing IT operations services to around 80 government bodies, including the department and three other government bodies referred to in the above section.

4. Box 1 presents examples of successful cyber attacks that could have been prevented or mitigated, had the three security controls been implemented.

### BOX 1. EXAMPLES OF SUCCESSFUL CYBER ATTACKS

Several of the government agencies that rely on the services provided by the Danish Agency for Governmental IT Services have in recent years been affected by successful cyber attacks. An attack is considered successful by Rigsrevisionen when neither the security controls implemented by the agency nor those implemented by the Danish Agency for Governmental IT Services have managed to prevent or detect the attack, and when subsequent investigations have failed to rule out the possibility that IT systems or data have been abused. The attacks were detected because the Danish Centre for Cyber Security recorded communication with websites known for or suspected of malicious activities.

According to the Danish Centre for Cyber Security some of the attacks could have been avoided, and the consequences of the majority of the attacks considerably reduced, if the three security controls referred to in this report had been implemented in the agencies.

5. Rigsrevisionen took initiative to the examination, which is based on IT audits performed by Rigsrevisionen in the spring 2013 as part of the annual audit. Rigsrevisionen decided to submit the report to the Public Accounts Committee because the outcome of the examination was considered a matter of principle. Rigsrevisionen encourages all government bodies to consider the recommendations of the study on how to manage cyber attack risks.

### MAIN CONCLUSION

**The data for which the government bodies were responsible was not, at the time of the examination, adequately protected and the level of security exposed the IT systems and confidential data to undue risk of cyber attacks. The examination showed that none of the agencies had addressed their own exposure to risk in their risk assessment reports. Rigsrevisionen is of the opinion that the division of cyber security responsibilities between the Danish Agency for Government IT Services and the government bodies is unclear.**

**The examination showed that the agencies in the study had not systematically reduced the risk of cyber attacks through technical limitation of downloads from the Internet and controlled use of local administration privileges. Moreover, only two out of the four government bodies had established routines that ensured systematic updates of their programmes. Lastly, the government bodies' risk assessment reports did not provide any evidence that management had addressed how a decision not to implement the three security controls would affect the security of the agency.**

**The Danish Agency for Governmental IT Services has not to the extent required addressed the risk that a cyber attack on one government body with inadequate security controls could spread to other bodies, for instance, through the shared services. Rigsrevisionen finds that the Danish Agency for Governmental IT Services' extensive use of domain administrators has increased the risk of attacks spreading.**

**Rigsrevisionen is of the opinion that the findings of the examination are relevant to a wider circle of government bodies than those included in the study.**

**Rigsrevisionen therefore recommends that**

- **all government bodies should address the risk of cyber attacks in their risk assessments and consider whether the implemented technical restrictions on downloads of programmes from the Internet and the number of local administrator accounts have been adequately limited, and whether applied software programmes, etc. are being updated regularly.**

**Based on the outcome of the study, Rigsrevisionen also recommends that**

- **the Ministry of Finance should clarify how responsibilities for cyber security should be divided between the Danish Agency for Governmental IT Services and its clients;**

- **the Ministry of Finance and the Danish Agency for Digitisation, or the Ministry of Defence, should, through the Centre for Cyber Security, develop guidance for all government bodies on the implementation of security controls to mitigate cyber attacks.**

# II. How government bodies mitigate the risk of cyber attacks

## A. Introduction

6. The technological development drives the increased digitization of society, which has also led to improved efficiency in the public sector through the launch of new electronic solutions and services. Government bodies are now storing large amounts of electronic data, some of which are confidential, like for instance, commercial data reported to the government by private sector companies in compliance with the requirements of the Danish Competition Act. Most government bodies are also accountable for protecting information that falls within the Danish Act on Processing of Personal Data, i.e. information on citizens' health, political or religious persuasion, ethnical background, criminal record, social problems and other strictly personal matters like, for instance, tax affairs, employment terms and income situation.

The increased use of information technology has compounded the risk of suffering an attack from the internet, also referred to as a cyber attack. A recent example dates back to the early summer 2013 when intruders gained access to the personal identification numbers of several citizens' through attacks on – among other systems – the Danish Driving License Registry. Rigsrevisionen has established that also government bodies under, for instance, the Danish Ministry of Business and Growth and the Danish Ministry of Finance have suffered cyber attacks.

***The Danish Centre for Cyber Security*** *is part of the Danish Defence Intelligence Service under the Ministry of Defence. The mission of the Centre is to protect Denmark from cyber attacks, espionage and Internet theft.*

According to the Danish Centre for Cyber Security, which has assisted several private companies and public bodies in handling cyber attacks, this threat to cyber security is constantly evolving. Breaches of the confidentiality of data stored by the government may have significant adverse consequences not only for the citizens and private companies, but also for the government bodies affected.

## B. Objective, delimitation and methodology

7. The objective of the audit was to assess whether selected government bodies had sufficient focus on mitigating cyber attacks. The government bodies included in the audit were the Danish Agency for Governmental IT Services – under the Ministry of Finance – and three of its clients, i.e. the Danish Agency for Digitisation – also under the Ministry of Finance – the Ministry of Climate, Energy and Building, and the Danish Energy Agency.

8. Based on experience from previously performed IT audits, Rigsrevisionen is of the opinion that the results of the examination may apply to a wider audience of government bodies than those included in the audit.

9. Securing data, including mitigating the risk of cyber attacks, is an on-going process. In 2004, the government decided that all government bodies should implement *DS 484* – a national standard for data security. In recent years, the government bodies have been allowed to implement either the DS 484 or the international standard ISO 27001. Going forward, the government has decided that all public bodies must follow the new version of ISO 27001 which is expected to be available in a Danish version in October 2013. Both standards require the government bodies to carry out risk assessments that cover all relevant risk scenarios, and convert the results of the assessment into concrete security controls. The purpose of the risk assessment is to ensure effective prioritisation of resources and decide on a risk exposure level that is considered acceptable by the management.

***DS 484*** *and* ***ISO 27001*** *are information security standards. The DS 484 is a Danish standard and ISO 27001 is an internationally recognised standard. The contents differ, but they both aim to ensure information security.*

The threat to cyber security is constantly evolving and becoming more complex, whereas a risk assessment provides a snapshot of the security situation at the time of the assessment. Therefore, the security standards operate with minimum one annual risk assessment to keep management updated on current risks.

Taking into consideration the growing number of cyber attacks, in combination with the fact that most government bodies store large amounts of sensitive and confidential digital data, it is now relevant for government bodies to address the risk of cyber attacks and to consider whether appropriate security measures and controls to mitigate such attacks are in place.

10. On the basis of international studies of cyber attacks, Rigsrevisionen has concluded that the following three security controls can prevent the majority of the currently known types of attacks,

- technical restriction of download of programmes from the Internet;
- limited use of local administrators;
- systematic software updates.

*Being granted* ***local administrator*** *rights gives the employees full access and control of their work stations.*

Figuratively speaking, these three security controls can be said to possess the same qualities as the most effective anti-theft locks in the market trusted to prevent a majority of attempted burglaries.

Rigsrevisionen is of the opinion that – unless otherwise justified – implementing the three security controls is now to be considered good practice.

11. In October 2012, the Australian Department of Defence estimated that around 85 per cent of all cyber attacks can be mitigated through the implementation of a few security controls. Other international organisations like, for instance, the British Communications-Electronics Security Group (CESG) and the SANS Institute, have issued similar recommendations concerning mitigation of cyber attacks. These recommendations are updated in pace with evolving cyber threats. The SANS Institute is a private American research and education organisation that cooperates with the American National Security Agency and a long list of other players from the public and private sector.

In addition to mitigating controls, the studies referred to above also include other technical and organisational security measures. The three recommended security controls addressed in this report are among the mitigating control measures most strongly recommended by the Australian Department of Defence and by the CESG. The three controls are also found on the SANS Institute's prioritised list of 20 critical security controls – referred to as *quick wins* – which are providing substantial and immediate risk reduction without requiring major procedural or technical changes.

The description of the three security controls in the three reports mentioned above differs from the description in Rigsrevisionen's report. The three international reports all refer to *whitelisting,* which is an approach aiming to ensure that only software that has been identified as safe is allowed to run. We have examined whether the government bodies have technically restricted staff's options to download programmes, as the implementation of this security measure is less resource demanding than whitelisting, but serves the same purpose.

In the opinion of Rigsrevisionen, the conclusions of the three reports and other international studies confirm the importance of the three mitigating security controls that we address in this report. According to the Centre for Cyber Security, the conclusions from the Australian report and other similar reports can readily be transferred to a Danish setting.

12. It should be noted that the three mitigating controls cannot stand alone as good practice. Effective protection from cyber attacks requires a wide range of technical and organisational security measures that are not addressed in this report.

13. In addition to examining whether the government bodies had implemented the three security controls, we also checked whether the risk associated with a decision not to implement the controls had been recorded in the risk assessment reports in a manner that reflected that management had addressed the risk and the possibilities of mitigating cyber attacks.

*A **domain administrator** has considerably more rights than a local administrator. A domain administrator has full rights, access and control of all IT systems and data in the business or organisation. The risk of an attack spreading increases if a domain administrator's user account is compromised by a hacker.*

In relation to the Danish Agency for Governmental IT Services, we focused particularly on its assessment and test of the risk that an attack on one of its clients could spread to other clients. Rigsrevisionen finds that the security level of the agency and its clients should be considered collectively because security weaknesses identified either at the agency or one of its clients could potentially affect other clients. In continuation hereof, we examined whether the Danish Agency for Governmental IT Services had limited its use of domain administrators, who may increase the risk of an attack spreading to other clients.

Rigsrevisionen also reviewed the standard agreement entered between the agency and its clients in order to determine how the responsibility for the three security controls had been divided between them.

Finally, Rigsrevisionen examined the government bodies' security policies and other relevant documents, and conducted interviews with relevant staff. Rigsrevisionen also received a report worked out by the Danish Agency for Governmental IT Services on the current security updating policy applied on its clients' computers. We reviewed this report to assess the clients' security policies concerning security updates.

14. Rigsrevisionen's draft report was presented to the Ministry of Finance, the Ministry of Climate, Energy and Building, the Danish Agency for Governmental Services, the Danish Agency for Digitisation, the Danish Energy Agency and the Centre for Cyber Security, and their comments have to the widest extent possible been incorporated in this final version of the report.

15. Appendix 1 (glossary) explains relevant words and terms used in the report. Appendix 2 provides a list of sources of the international studies referred to in the report.

## C. Examination of the three security controls

16. Rigsrevisionen examined whether the selected government bodies had implemented the three recommended security controls.

Table 1 shows the results of Rigsrevisionen's examination of practice in the selected government bodies.

**Table 1. Security policy in selected government bodies**

| | Danish Agency for Governmental IT Service | Danish Agency for Digitisation | Ministry of Climate, Energy and Building | Danish Energy Agency |
|---|---|---|---|---|
| Restrictions on download of programmes from the Internet | No | No | No | No |
| Limited use of local administrators | No | No | No | No |
| Systematic security updates of programmes | Yes | No | No | Yes |

Note: "No" means that the government body does not consistently follow good practice.
"Yes" means that the government body consistently follows good practice, although deviations occur.

The following sections elaborate on the three security controls and the results of the examination as reflected in table 1.

**Downloading programmes from the Internet**

17. IT systems may be configured to prevent staff from downloading programmes from the Internet, yet allowing them to download pictures, documents and graphic presentations. This means that the members of staff are only allowed to use programmes that are considered relevant for their work, i.e. programmes for data processing, spread sheets and Internet access. The employer may also decide to configure the systems in a manner that allows staff to download software from the Internet. This approach increases the risk that staff members – unknowingly – download malicious software like, for instance a hacker's remote control software. Rigsrevisionen has examined whether the government bodies technically restrict their employees from downloading software from the Internet.

***Downloading** a programme means transferring data from the Internet to a local computer. To run the program, users will subsequently need to install the programme on their local computer.*

18. Rigsrevisionen's examination showed that none of the government bodies had implemented any such technical restrictions concerning downloads, and thus none of them had implemented the first of the three recommended security controls.

None of the four government bodies had in their risk assessments recorded why technical restrictions concerning downloads from the Internet had not been implemented. Rigsrevisionen is of the opinion that it should be recorded that management has addressed the risk that the government agency will be exposed to if downloading of programmes from the Internet is not technically restricted.

**Use of local administrators**

19. The employer may decide on a configuration of computers that restricts user privileges. Or the employer may decide to grant local administrator privileges to all members of staff, which give them full access and control of their computers. An attacker may take over the rights of a local administrator and, for instance, close the anti-virus programmes and other programmes designed to mitigate attacks, and then proceed to gain access to other IT systems in the organisation. The system privileges of local administrator can be used by attackers to install various malicious programmes on the computer. Rigsrevisionen has examined whether the four selected government bodies have limited the use of local administrators in their respective organisations.

20. Rigsrevisionen's examination showed that the four government bodies have all chosen to grant local administrator privileges to all members of staff. Thus the second of the three recommended security control measures had not been implemented either.

None of the four organisations had in their risk assessments provided any reasons for their use of local administrators. Rigsrevisionen is of the opinion that it should be recorded that management has addressed the risk that the government body will be exposed to, if the use of local administrators is not limited.

**Software security updates**

21. Attackers may use weaknesses in programmes like, for instance, Adobe Reader, Adobe Flash Player, Java and the browsers (e.g. Internet Explorer) that are installed on most computers. If the organisations systematically update the programmes, these weaknesses can be mitigated to the minimum. The software manufacturers release new security updates regularly and at a frequency that is closely linked to the identification of security weaknesses. It is not uncommon that new security updates for specific programmes are released a couple of times per month. Rigsrevisionen has examined whether the government bodies are systematically updating the four programmes referred to above.

22. The Agency for Governmental IT Services and the Danish Energy Agency are both updating their programmes systematically, as opposed to the two other bodies in the study. Thus two of the four audited government bodies had not implemented the third security control measure.

The examination also showed that the government bodies had not in their risk assessments provided reasons for their practice concerning security updates of programmes. Rigsrevisionen is of the opinion that it should be documented that the management has considered the risk that the organisation is exposed to when programmes are not security updated regularly.

The study did show, however, that practice is changing. At the time when the audit was carried out, the Danish Agency for Governmental IT Services was in the process of rolling out new computers to all its clients. The roll out, which had just been completed at the Danish Energy Agency, will improve security, because the clients' programmes will be updated with the frequency that is applied at the Danish Agency for Governmental Services. The roll out is expected to be completed before year-end 2013.

23. Rigsrevisionen's immediate expectation is that the roll out of new computers will solve most of the problems relating to inadequate security update policies. Rigsrevisionen has, however, been informed that some of the around 1,500 systems, that are run by the Danish Agency for Governmental IT Services on behalf of its clients, make it difficult to install the security updates on the computers. The reason is that some of the clients' professional support systems have been developed for specific software versions, for instance, for a specific version of the Internet browser. Installation of a new version of the browser on the computer may therefore obstruct execution of particular programmes and the security update will thus reduce or even eliminate the functionality of the computer.

Neither the Danish Agency for Governmental IT Services nor several of its clients have an overview of the professional support systems that are causing the problems in relation to the security updates or the total costs involved in resolving the security issue. Thus the information that is available at this point does not suffice to determine the scope of the task. It is therefore also too early to determine whether the agency's roll out of the new computers will solve this particular security challenge.

## D. Examination of specific security controls at the Danish Agency for Governmental IT Services

**Risk of cyber attacks spreading**

24. The objective of sharing the IT services provided by the Danish Agency for Governmental IT Services is to reduce costs per transaction like, for instance, execution of payments or database searches. Updating of antivirus programmes on all computers can, for example, be handled by one server. Shared hard disks can be used across government departments, agencies and bodies, and staff can work across IT systems and data.

The trend towards shared services can, however, also increase the clients' risk exposure; the weakest link in the security chain may jeopardise the IT security of the other clients. A cyber attack on one organisation with inadequate security controls may give intruders easy access to other clients' confidential data. Thus the Danish Agency for Governmental IT Services' clients are – in terms of security – mutually dependent on each other.

The Centre for Cyber Security has reported examples of cyber attacks on government bodies that have spread to other administrative units within the same ministry. Rigsrevisionen urges the Danish Agency for Governmental IT Services to take an active approach to mitigating the risk of attacks spreading within a ministry and across ministry boundaries. Such action should include risk assessment and subsequent test of the security level achieved.

25. Rigsrevisionen examined whether the Danish Agency for Governmental IT Services had assessed the risk of an attack on one government body compromising the IT security of other government bodies. Rigsrevisionen also examined whether the agency had tested if compromised IT systems in one government body could threaten the system security of the agency's other clients.

It turned out that the Danish Agency for Governmental IT Services had not assessed the risk of an attack on one government body compromising the IT security of the agency's other clients. Nor had the agency conducted tests to establish whether an attack on one government body could compromise the system security of the agency's other clients. The agency has informed Rigsrevisionen that the security level of the operations centre is adequate, but recognises that there is a need to determine – and subsequently test – the risk of attacks spreading.

**Risk connected to extensive use of domain administrators**

26. Rigsrevisionen examined the Danish Agency for Governmental IT Services' use of domain administrators. Domain administrators have full rights, access and control of all IT systems and data in the respective organisation. The privileges of a domain administrator may be compromised and thus made available to an intruder, which will increase the risk of an attack spreading.

27. The Danish Agency for Governmental IT Services had granted rights and permissions to a large number of domain administrators – a practice that represents a significant risk in relation to potential attacks.

28. The agency has informed Rigsrevisionen that the number of domain administrators has been considerably reduced. Implementing reductions beyond the current level without affecting the stable operations of the agency will – in the opinion of the agency – be difficult. The agency agrees with Rigsrevisionen that a change of practice and increased monitoring of the administrators can improve security.

The agency has stated that the overall IT security has been improved for the government bodies that are relying on the services provided by the agency, but that the establishment of an operations centre will also lead to the emergence of new risks related, for instance, to cyber attacks.

## E. Responsibility for the security of the government bodies

*The **infrastructure** of the Danish Agency for Governmental IT Services include servers, networks, computers and general programmes like, for instance, office e-mail/calendar and user rights management systems.*

29. It appears from the standard agreement entered between the Danish Agency for Governmental IT Services and the clients that the agency is responsible for the IT infrastructure operations and security, whereas the government bodies are responsible for running and ensuring the security of their professional support systems. The agreement also refers to security updates, but not to download of programmes or the use of local administrators. Rigsrevisionen is of the opinion that the agreement does not clearly specify how responsibilities concerning the security controls referred to in this report, should be divided between the parties.

***Professional support systems** are systems that offer the facilities needed to perform specific tasks. These systems are run on top of the Danish Agency for Governmental IT Services' IT infrastructure.*

In reality the choices made by the individual government bodies concerning their professional support systems affect the agency's efforts to develop a secure IT infrastructure, which again affects the security of the government bodies. On the other hand, the agency's choices concerning the IT infrastructure security affect the government bodies' business opportunities.

30. Private businesses are obliged to submit digital information to the government and the government registers data on the citizens – sometimes contrary to their wishes. In the opinion of Rigsrevisionen, the responsibility for ensuring that data remain confidential rests with the ministry that is collecting and storing the information. It follows that the government bodies, owning the data, should be responsible for ensuring adequate protection of the data.

Rigsrevisionen, 2 October 2013

Lone Strøm

/Peder Juhl Madsen

## Appendix 1. Glossary

| | |
|---|---|
| Adobe Flash | An add-on programme that can be downloaded from the Internet. The programme allows the user to view graphics like, for instance, a movie trailer, videos and websites. |
| Adobe Reader | An add-on programme that can be downloaded from the Internet. The programme is required to view, print, sign and comment on pdf documents. |
| Annual audit | Rigsrevisionen's annual audit includes on-going audit of, for instance, business procedures and internal controls, including IT audit and closing audit of annual accounts. The results of the on-going audits are generally reported to the auditee and the ministry concerned. |
| Antivirus programme | A computer programme that detects, prevents, and takes action to disarm or remove malicious software programmes before they gain access or spread. Antivirus programmes often include a function that scans the traffic between the computer and the Internet to prevent malicious software from going in or out of the computer. |
| Browser | A software application that is installed on the computer and allows the user to locate, retrieve and display content on the Internet. One of the most widely used browsers is Microsoft's Internet Explorer, which comes with many computers. |
| Cyber attack | Is in this report referring to an attempt to get unauthorised access to IT systems or data. The purpose of such attacks and the methods used depend on the attacker, i.e. a foreign state, a criminal organisation or individuals who break into computer systems on their own. |
| Danish Centre for Cyber Security | Is part of the Danish Defence Intelligence Service under the Ministry of Defence. The mission of the Centre is to protect Denmark from cyber attacks, espionage and Internet theft. |
| Data owner | The data owners are responsible for securing data through implementation of the necessary technical and organisational measures. Although tasks concerning data processing, including collection, recording and storing, may have been outsourced, the data owner will still be responsible for ensuring that the security level is adequate. |
| Digitising | Conversion of data, sound or images to digital formal and wide use of electronic media and computer-based business procedures. |
| Domain administrator | A domain administrator has full rights, access and control of all IT systems and data in an organisation. Domain administrators have considerably more privileges than local administrators. |
| Download | Transferring, for instance, programme or audio and image files from the Internet to a computer. |
| DS 484 and ISO 27001 | Information security standards. The DS 484 is a Danish standard and ISO 27001 is an internationally recognised standard. The contents differ, but they both aim to ensure information security. |
| Government bodies | An administrative unit of government, whose management is accountable for one or several budgets and accounts relating to the Danish Appropriation Act. |
| Hard disk | This is where all data are recorded and stored in the computer, i.e. programmes, games, music, images, etc. |
| Information security | Referring to security relating to all digitally-based information, but also, for instance, to the physical framework and paper-based documents. |
| Infrastructure | The infrastructure of the Danish Agency for Governmental IT Services refers to its hardware, software and network resources, i.e. servers, computers and general programmes like, for instance, office e-mail/calendar and rights management systems. |
| Internet Explorer | One among many browsers. Internet Explorer is a Microsoft product. |

| | |
|---|---|
| Java | Is an add-on programme that can be downloaded from the Internet. It helps the browser display formats like, for instance, Adobe Flash. Many websites and functions are based on Java, for example, Google Maps and NemID (Easy ID – digital signature solution). |
| Local administrator | Local administrators have full rights, access and control of their work station. |
| Professional support systems | Professional support systems offer the facilities needed to perform specific tasks – in this context tasks relating to the clients of the Danish Agency for Governmental IT Services. These systems are run on top of the IT infrastructure of the Danish Agency for Governmental IT Services, i.e. hardware, software, network resources and other services. |
| Security controls | Is in this report referring to a practice or mechanism designed to improve IT security, i.e. measures that are implemented to mitigate errors and risk of loss and abuse of data, and to secure access to data and system. |
| Security updates | Weaknesses of known programmes are used by intruders to gain access to the computer. Security updates correct identified weaknesses in programmes. |
| Shared services | Merging administrative functions into one unit and standardizing and streamline the performance of tasks. |
| Whitelisting | A list of programmes that are considered safe to run; programmes are automatically checked and only programmes that are on the list will be accepted for use. Implementing whitelisting requires maintenance of information on the users' tasks and detailed information on which programme versions they require to perform their tasks. |

## Appendix 2. List of sources

Australian Government, Department of Defence, Intelligence and Security, the Defence Signals Directorate (2012): *Strategies to Mitigate Targeted Cyber Intrusions:* www.dsd.gov.au/publications/Top_35_Mitigations_2012.pdf

British Government Communications Headquarters, Communications-Electronics Security Group (2012): *10 steps to Cyber Security*: www.bis.gov.uk/assets/biscore/business-sectors/docs/0-9/12-1121-10-steps-to-cyber-security-advice-sheets

SANS Institute (2013): *Critical Controls for Effective Cyber Defense:* www.sans.org/critical-security-controls/cag4-1.pdf