FOLKETINGET
STATSREVISORERNE

FOLKETINGET
RIGSREVISIONEN

January 2022
– 9/2021

Extract from Rigsrevisionen's report
submitted to the Public Accounts Committee

Five government authorities' compliance with 20 technical minimum information security requirements

1. Introduction and conclusion

1.1. Purpose and conclusion

1. This report concerns five essential government authorities' compliance with 20 national technical minimum information security requirements. The report builds on the outcome of IT audits conducted in the period from March to September 2021.

2. The 20 technical minimum information security requirements are intended to protect government workplaces against malicious cyber and information security incidents. Incidents like, for instance, attacks by malicious operators who want to gain access to confidential data or block access to data in order to extort ransoms. Seventeen of the requirements have been mandatory for government authorities since 1 January 2020 and three were made mandatory on 1 July 2020.

Malicious operators
In this report, a malicious operator is a person who intentionally or unintentionally performs a criminal offence by secretly gaining access to and/or infect victim IT systems or data. A malicious operator can be a member of staff, but it can also be a complete stranger.

3. The cyber threat against government authorities grows in pace with the digital development of the Danish society. This development is also reflected in the threat assessments published by the Danish Centre for Cyber Security. Cyberattacks are not uncommon, and several government institutions have been attacked over the years. In October 2021, it became known that cyber criminals had cheated the municipality of Hoje Taastrup by taking over a manager's email account and instructing the finance department of the municipality to pay Covid-19 related expenses. The cyber criminals had also gained access to sensitive data on an unknown number of citizens like, for instance, personal identification numbers, union affiliation and health data.

4. The task of complying with the 20 technical minimum information security requirements is particularly important for authorities that provide essential services to society or handle sensitive data on citizens, for instance. The reason is that compliance with the minimum requirements contributes to establishing a basic level of information security that helps protect the information and data for which the authorities are responsible.

5. The scope of this study includes the Danish Agency for Governmental IT Services (the Ministry of Finance), The Danish Prison and Probation Service (the Ministry of Justice), the Danish Health Data Authority (the Ministry of Health), the Danish Energy Agency (the Ministry of Climate, Energy and Utilities) and the Danish Veterinary and Food Administration (the Ministry of Food, Agriculture and Fisheries). These five authorities provide essential services to society and/or handle sensitive data on citizens and have therefore been selected for this study. The Danish Agency for Governmental IT Services was also selected for this study for another reason; it provides IT services to 19 ministerial remits, including the Danish Energy Agency and the Danish Veterinary and Food Administration, and is therefore under an obligation to meet certain of the minimum requirements on behalf of their government customers.

6. The purpose of the study is to assess whether the five essential authorities comply with the 20 technical information security requirements. We have examined:

- whether each individual authority complies with the technical minimum requirements that the authority is under an obligation to meet;
- whether the Danish Agency for Governmental IT Services and its customers – the Danish Energy Agency and the Danish Veterinary and Food Administration – comply with the technical minimum requirements in accordance with the division of responsibility that they have agreed upon.

7. Rigsrevisionen initiated this study in June 2021. It builds on the outcome of five IT audits conducted in the period from March to September 2021. After completion of the IT audits, the audited authorities have had opportunity to resolve any outstanding issues concerning compliance with the requirements.

The phrasing of four of the 20 minimum requirements is not accurate, and they have therefore been operationalized by Rigsrevisionen for the purpose of this study.

The Danish Agency for Governmental IT Services does not agree with Rigsrevisionen's interpretation of requirements nos. 13 and 18. The agency finds that Rigsrevisionen becomes norm-setting in the implementation of the requirements and is more rigorous in its interpretation than other parties. Moreover, the agency does not agree with Rigsrevisionen's assessment of the risk associated with inadequate compliance with the two requirements.

The Danish Prison and Probation Service has objected to Rigsrevisionen's interpretation of what compliance with the 20 technical minimum requirements entails. The Prison and Probation Service has informed Rigsrevisionen that the 20 technical minimum requirements were not originally developed with the purpose of providing a starting point for an IT-audit. According to the Prison and Probation Service, Rigsrevisionen has therefore, for some of the requirements, considered it necessary to specify what it takes to be compliant with the requirements. According to the Prison and Probation Service, the audit criteria can be said to have emerged from the technical requirements, but they have subsequently been subjected to Rigsrevisionen's interpretation.

The Danish Energy Agency has noted that the report does not adequately describe the proportions of the inadequate compliance, nor does it take into consideration mitigating measures that can minimize the risk associated with the inadequate compliance with the individual requirements.

In the opinion of Rigsrevisionen, compliance with the 20 technical minimum requirements ensures a basic level of information security. As mentioned above, a few of the requirements are not accurately defined, i.e. requirements nos. 6, 13, 15 and 18, and they have therefore been operationalized by Rigsrevisionen. The requirements were operationalized from an information security and best practice perspective. Section 1.3 on audit criteria offers a description of how Rigsrevisionen operationalized the requirements. In the report, Rigsrevisionen describes the risk associated with failure to comply with the requirements. The risks described flow, among other things, from the risks described in conjunction with the requirements on the website *sikkerdigital.dk* and Rigsrevisionen's communication with the Danish Centre for Cyber Security.

Partial compliance with the minimum requirements is not an option, in the opinion of Rigsrevisionen. Still, information regarding authorities that have pointed out that they only need to deal with a few things to achieve full compliance with a minimum requirement, or authorities that have provided comments on mitigating measures, is reflected in the report.

Main conclusion

The Ministry of Finance, the Ministry of Justice, the Ministry of Health, the Ministry of Climate, Energy and Utilities, and the Ministry of Food, Agriculture and Fisheries have not ensured that the five selected authorities complied with all 20 technical minimum requirements for information security, when Rigsrevisionen conducted an audit of the area in 2021. This is considered unsatisfactory by Rigsrevisionen, since most of the requirements should have been implemented by 1 January 2020. The consequence is that the authorities' IT-systems, mobile phones and tablets have been more vulnerable to cyberattacks and abuse.

None of the authorities complied with all the technical minimum requirements at the time of the audit

The Health Data Authority met 12 requirements, the Energy Agency met 15 requirements, the Prison and Probation Service met 16 requirements and the Veterinary and Food Administration met 17 requirements. The Danish Agency for Governmental IT Services did not meet all 20 requirements either, but only 18, despite the fact that the Danish Agency for Governmental IT Services is a professional actor in the area, whose core task is to deliver IT operations and services to other government authorities. This, despite the fact that the 20 minimum requirements came into effect 12-18 months ago.

None of the authorities complied with minimum requirement no. 13 concerning the updating of mobile devices. For instance, failure to update mobile phones regularly increases the risk of malicious operators gaining access to confidential data or succeeding in monitoring the authority (for example by listening in on mobile phone calls).

Four of the authorities have drawn up action plans for implementing the minimum requirements that they did not meet at the time of the audit. The Danish Agency for Governmental IT Services has informed Rigsrevisionen that risk assessments will be undertaken, but have not yet been carried out.

The Danish Agency for Governmental IT Services has ensured that the Energy Agency and the Veterinary and Food Administration meet the majority of the technical minimum requirements, but coordination between the Agency for Governmental IT Services and the two authorities has been inadequate in respect to two requirements

In its capacity as supplier of IT services, the Danish Agency for Governmental IT Services is under an obligation to ensure that 13 of the 20 requirements are met on behalf of the Energy Agency and the Veterinary and Food Administration, who are customers with the Danish Agency for Governmental IT Services. The study shows that the Agency for Governmental IT Services has fulfilled this obligation.

The Energy Agency and the Veterinary and Food Administration can enter into an agreement with the Agency for Governmental IT Services to ensure compliance with four additional minimum requirements beyond the 13 referred to above. Such an agreement requires coordination of activities between the parties. Rigsrevisionen found examples of inadequate coordination with the Veterinary and Food Administration and the Energy Agency from the side of the Agency for Governmental IT Services in relation to requirement no. 18 concerning encryption of website communication, whereas the Energy Agency has failed to coordinate adequately with the Agency for Governmental IT Services in relation to requirement no. 20 that concerns regular updating of web servers.

Rigsrevisionen recommends that the Ministry of Finance ensures further specification and elaboration of four of the requirements in order to minimize any doubts on what it takes to meet the individual requirements

Rigsrevisionen notes that four of the requirements are open to interpretation and are indeed interpreted by the authorities in different manners due to, among other things, inaccurate wording. This observation applies to requirement no. 6 concerning restriction of local administrator privileges, requirement no. 13 concerning regular updating of mobile devices, requirement no. 15 concerning logging and requirement no. 18 concerning encryption of website communication.