FOLKETINGET
STATSREVISORERNE

FOLKETINGET
RIGSREVISIONEN

January 2026
– 8/2025

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

The Danish Agency for Governmental IT Services' protection of local network equipment at central government authorities

1. Introduction

1.1. Purpose and conclusion

1. This report concerns the protection of network equipment on the local networks of central government authorities.

2. A network can only function by means of network equipment consisting of various technical devices. These may include Wi-Fi devices or devices that provide access to the network via a cable and a wall socket.

3. The local networks of central government authorities are the networks to which employees connect their work computers. The networks are necessary to enable employees to share documents and data, send emails, hold video meetings, etc. The authorities' networks communicate with the Danish Agency for Governmental IT Services' central network.

Rigsrevisionen has previously examined parts of the Danish Agency for Governmental IT Services' central network in report no. 6/2023 on the security of servers managed by the Danish Agency for Governmental IT Services. State data are stored in the Danish Agency for Governmental IT Services' central network, and it is therefore more risky if unauthorised persons gain direct access to the Danish Agency for Governmental IT Services' servers than if they gain access to the authorities' local networks.

In this report, we examine the local networks in the form of network equipment located at the ministries.

4. In two previous IT audits in 2019 and 2023, Rigsrevisionen examined and assessed, among other things, that the Danish Agency for Governmental IT Services had not implemented appropriate procedures for security update and maintenance of network equipment. This study concerns the same types of network equipment that were included in the two IT audits.

The Danish Agency for Governmental IT Services' central network
State servers and data are located on the Danish Agency for Governmental IT Services' central network. This is where the authorities' specialist systems and stored files are located. The central network is protected by more layers than the local networks of central government authorities.

According to the Danish Agency for Governmental IT Services, the network equipment at central government authorities is located where unauthorised persons do not have physical access, for example in corridors, offices and locked cabinets or rooms. This means that vulnerabilities can only be exploited through unauthorised physical access, which in most cases would also require bypassing alarms and guards. Rigsrevisionen notes, however, that the authorities also include educational institutions, where there is relatively free public access. In addition, exploitation of vulnerabilities would require bypassing the Danish Agency for Governmental IT Services' other security measures, for example firewalls. According to the Danish Agency for Governmental IT Services, there is therefore a low probability that vulnerabilities on the local networks can be exploited.

If a hacker succeeds in gaining access to an authority's local network, there is a risk that the hacker may disrupt network operations and thereby make it more difficult for the authority to carry out its tasks. In addition, there may be a risk that the hacker can intercept the communication on the network and, for example, see the documents that employees send to printers.

There may also be a risk that the hacker can use the access as a stepping stone to gain access to the Danish Agency for Governmental IT Services' central network and thereby, among other things, to confidential information about the state, businesses and citizens. This would, however, require that the hacker also bypasses a number of the Danish Agency for Governmental IT Services' other security measures. The Danish Agency for Governmental IT Services therefore assesses that this risk is low.

5. Box 1 shows an example in which a hacker group has exploited vulnerabilities in network equipment.

Box 1

Example of attacks through vulnerabilities in network equipment

A suspected Russian, state-sponsored hacker group has specialised in breaking into network equipment. They primarily target old and poorly updated equipment with known vulnerabilities. Once they have gained access, they gradually work their way further into the organisation's systems by taking over more equipment. Along the way, they can change equipment configurations and intercept data traffic. By modifying the software in the equipment itself, they can maintain hidden access and conduct espionage for years without being detected. The attacks have e.g been directed at authorities, telecommunications companies and educational institutions in North America and Europe, including critical infrastructure in Ukraine.

Source: Rigsrevisionen based on Cisco Talos.

There are only a few known examples of the type of attacks described in box 1, and Rigsrevisionen is not aware of any examples in Denmark.

In connection with this study, Rigsrevisionen has received advice from an external expert, who assesses that the probability of this type of attack is low, but that the consequences may be significant. The Danish Agency for Governmental IT Services assesses both that the probability of successful attacks on the authorities' local networks is low and that the consequences would be minor, because the attack would be detected by the Danish Agency for Governmental IT Services' other measures.

Although the threat has been serious for several years, it is continuously changing character, and hackers are constantly adopting new tools and methods. The Danish Resilience Agency assesses that the threat from cyber espionage is very high.

The Danish Resilience Agency recommends that network equipment are security updated on an ongoing basis. Protection may also, for example, be achieved through a technical access control, meaning that only approved devices, such as computers supplied by the Danish Agency for Governmental IT Services, can access the networks. In addition, there are other layers that protect the information on the networks, such as data encryption.

6. The Ministry of Finance is responsible for IT operations at central government authorities across 23 ministries and more than 800 locations in Denmark and abroad. IT operations are handled by the Danish Agency for Governmental IT Services, which is an agency under the Ministry of Finance. The Danish Agency for Governmental IT Services therefore also has the responsibility for the security of network equipment on the local networks of central government authorities. The authorities themselves are responsible for physical access control at the locations.

7. The Danish Agency for Governmental IT Services purchases network equipment from private manufacturers. The manufacturers continuously identify vulnerabilities in the equipment that may make the networks uinsecure. When manufacturers identify vulnerabilities, they release updates that can eliminate them. It is the implementation of these updates that The Danish Resilience Agency recommends.

Central government authorities not included in the study

At the time of the study, the Danish Agency for Governmental IT Services did not handle IT operations for the Ministry of Taxation and the Ministry of Defence. In addition, there are individual authorities under other ministries for which the Danish Agency for Governmental IT Services is also not responsible for IT operations, including the police.

8. The purpose of the study is to assess whether the Danish Agency for Governmental IT Services has ensured satisfactory protection of network equipment at central government authorities. We answer the following questions in the report:

- Has the Danish Agency for Governmental IT Services continuously implemented the security updates released by the manufacturer?
- Has the Danish Agency for Governmental IT Services carried out an adequate risk assessment of the authorities' network equipment?

Rigsrevisionen initiated the study in June 2025.

9. The report has been prepared for publication. By agreement with the Ministry of Finance, and in consideration of state security, we have not listed or provided examples of vulnerabilities at named authorities.

Conclusion

The Danish Agency for Governmental IT Services has not ensured a fully satisfactory protection of network equipment at central government authorities. This is because The Danish Agency for Governmental IT Services has not carried out an adequate risk assessment of the vulnerabilities in the network equipment and at the same time does not have a complete overview of all the equipment it is required to protect.

The Danish Agency for Governmental IT Services has not continuously implemented the security updates released by manufacturers, but the Danish Agency for Governmental IT Services has stated that it has instead initiated a programme to modernise the local networks.

The Danish Agency for Governmental IT Services has carried out an overall risk assessment in which it assesses that the risk associated with critical vulnerabilities in the authorities' network equipment is low. However, the risk assessment does not continuously address individual critical vulnerabilities in the network equipment as they are announced by manufacturers, including the risks these vulnerabilities pose to the authorities' local networks. In addition, the Danish Agency for Governmental IT Services does not have a complete overview of the network equipment at central government authorities and thus of what the Danish Agency for Governmental IT Services is required to protect. This means that there may be network equipment with vulnerabilities that The Danish Agency for Governmental IT Services is not aware of.

Furthermore, the Danish Agency for Governmental IT Services has implemented a technical access control intended to ensure that only approved devices, such as computers supplied by the Danish Agency for Governmental IT Services, can access an authority's wired network. At the time of the study, the Danish Agency for Governmental IT Services did not have a full overview of whether the access control had been sufficiently implemented on the relevant network equipment. In early January 2026, Rigsrevisionen received material which, according to the Danish Agency for Governmental IT Services, documents that the access control has largely been implemented. Due to the late timing, Rigsrevisionen has not been able to assess the documentation.

Rigsrevisionen recommends that the Danish Agency for Governmental IT Services specifically addresses individual vulnerabilities as they are announced. In addition, the Danish Agency for Governmental IT Services should establish a complete overview of the network equipment for which it is responsible to protect.