FOLKETINGET
STATSREVISORERNE

FOLKETINGET
RIGSREVISIONEN

December 2023
– 6/2023

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

The security of servers managed by the Danish Agency for Governmental IT Services

1. Introduction and conclusion

1.1. Purpose and conclusion

1. This report concerns the security of servers managed by the Danish Agency for Governmental IT Services.

2. Servers are essential to government IT infrastructure. The services provided by servers are diverse and include services to systems that manage sensitive personal data and critical business data.

The useful life of servers is limited. The useful life is the period during which the developer is obliged to develop security updates that fix vulnerabilities as they are detected. During a server's useful life, the manufacturer regularly issues security updates to improve the IT security of the server by patching security vulnerabilities and providing protection against new threats. At the end of a server's life (EOL), the developer will no longer provide security updates, and the server will pose a security risk. Therefore, servers must be upgraded to newer versions that can be supported by the developer. Sometimes, extended lifecycle support for EOL software can be bought for a limited period.

3. The Danish Centre for Cyber Security under the Danish Defence Intelligence Service assesses that the threat of cyber crime and cyber espionage against Denmark is very high, and the threat of cyber activism is high. Data security breaches may ultimately lead to the destruction or inaccessibility of government IT systems and data and the abuse or destruction of confidential and sensitive data on Danish citizens and companies.

Therefore, the Danish Centre for Cyber Security recommends updating all software, including server software, when new security updates are released. All public-sector authorities are required to comply with the international standard for information security, ISO 27001, which states that the exploitation of technical vulnerabilities must be prevented.

4. The Danish Agency for Governmental IT Services is an agency under the Ministry of Finance. The agency took over operations and IT support of several government authorities when it was set up in 2010. The objective was to provide the Danish public sector with better, cheaper and more secure data operations and services. More authorities have been added to the agency's client list since it was set up, and it is currently responsible for the IT operations and IT security of 151 authorities across 21 ministerial remits. IT staff from the individual authorities were transferred to the Danish Agency for Governmental IT Services when it set up.

Servers
Servers are computers and part of the IT infrastructure, and they provide services to other computers. Servers store and manage files, databases and programmes. Servers can be physical or virtual machines or software performing server services. In this report, the concept *server* refers to the server's operating system, which is the basic software in a server.

Cyber activism
Cyber activism is generally ideologically or politically motivated. Cyber activists focus on individual cases, persons or organisations that they perceive as adversaries.

The Danish Agency for Governmental IT Services
This agency is fully funded by its public-sector clients. The price of the services provided is fixed based on the principle of full cost recovery, which means that all expenses for operation, maintenance, development, support and consultancy are charged to the clients. In the Fiscal Act for 2023, the income and expenses of the agency were balanced at DKK 774 million. In 2022, the agency employed 506 full-time equivalents.

5. The purpose of the study is to assess whether the Danish Agency for Governmental IT Services under the Ministry of Finance has ensured that the servers it manages are supported by the developer and that personal data and critical business data are thus not exposed to unnecessary risk of being compromised. The report answers the following questions:

- Has the Danish Agency for Governmental IT Services upgraded or decommissioned servers on behalf of the 46 authorities in the study, before the developer ceased to provide security updates?
- Has the Danish Agency for Governmental IT Services implemented compensatory measures to manage vulnerabilities and security issues for the servers that are no longer supported by the developer?
- Has the Danish Agency for Governmental IT Services established procedures to ensure the timely upgrading and decommissioning of servers that are no longer supported by the developer?

The clients of the Danish Agency for Governmental IT Services
The clients are public authorities such as departments, agencies and independent institutions.

Rigsrevisionen took the initiative to the study in March 2023 based on an IT audit conducted by Rigsrevisionen in November 2022. The IT audit showed that security updates were no longer released for several servers managed by the Danish Agency for Governmental IT Services on behalf of the two authorities included in the study. The 46 public authorities in this study, including the Danish Agency for Governmental IT Services, represent approximately one third of the agency's clients.

6. The report is for publication, and some of the results of the study are described in general terms. However, Rigsrevisionen's analysis also includes details on IT security vulnerabilities in the Danish Agency for Governmental IT Services, which, according to the Ministry of Finance, potentially represent a risk to national security. Details of these vulnerabilities are, therefore, not reflected in the report.

Main conclusion

The Danish Agency for Governmental IT Services under the Ministry of Finance has not ensured that all servers managed by the agency are supported by the developer. The agency has failed to upgrade or decommission servers for which security updates are no longer released, and the agency's overview of the authorities' servers is incomplete. This fact is considered unsatisfactory by Rigsrevisionen and entails a risk that hackers gain access to and abuse or destroy sensitive personal data and critical business data.

The Danish Agency for Governmental IT Services has not upgraded or decommissioned servers, before the developer ceased to release security updates

537 servers managed by the Danish Agency for Governmental IT Services are no longer supported by the developer because they have reached their EOL. The 537 servers include the Danish Agency for Governmental IT Services' own servers and represent 10 % of the 5,353 servers that the agency manages on behalf of 46 authorities. The agency has not ensured upgrading or decommissioning of the servers. Moreover, the agency's overview of the servers is incomplete, which reduces the ability to respond quickly to cyberattacks and emerging cyberthreats. Since the start of the study, the agency has worked on improving its overview of servers and upgrading and decommissioning servers for which security updates are no longer released.

The Danish Agency for Governmental IT Services has not implemented sufficient compensatory measures to manage servers that are no longer supported by the developer

The Danish Agency for Governmental IT Services have a series of measures in place to reduce the risk of cyberattacks spreading. However, there is still a risk of cyberattacks spreading between servers and between authorities. The vulnerabilities of one authority may, therefore, expose other authorities to IT security risks. As an extension of the study, the agency has launched an initiative to reduce the risk of cyberattacks spreading between authorities.

The Danish Agency for Governmental IT Services has not established procedures to ensure the timely upgrading or decommissioning of servers that are no longer supported by the developer

The Danish Agency for Governmental IT Services is, by royal decree, responsible for the servers and the security of the servers. However, in most cases, the authorities are responsible for managing the systems that rely on the servers. The Danish Agency for Governmental IT Services has informed Rigsrevisionen that it is impossible for the agency to upgrade or decommission the servers because the authorities have not, as required, ensured that their administrative systems will be compatible with new servers. If upgrading or decommissioning servers has consequences for the authorities' use of the administrative systems, the Danish Agency for Governmental IT Services, which is responsible for managing the servers and is aware of the security risks, should keep contacting the authorities until they address the problems. In 2018 and 2020, the agency and some of the authorities agreed on the steps the authorities should take to allow the agency to upgrade or decommission the servers. However, the agency has not established the necessary collaboration with the authorities to facilitate timely upgrading or decommissioning. The agency has informed Rigsrevisionen that it will start using a new paradigm for agreements with the authorities in 2023 that allows follow-up on the agreements. The agency intends to establish a routine to ensure follow-up on the agreements at regular intervals.

The Danish Agency for Governmental IT Services has not ensured timely updating or decommissioning of its own servers, which does not require agreements with any other authorities. The agency has informed Rigsrevisionen that during the 1st quarter of 2024 it expects to complete the upgrading or decommissioning of those of its servers that are no longer supported by the developer.

Rigsrevisionen notes that the present set-up is not capable of solving the problem and recommends that the Ministry of Finance considers the distribution of responsibility between the Danish Agency for Governmental IT Services and the authorities in relation to the servers and ensures that the agency can shoulder its responsibility for the cyber security of the government's IT infrastructure.