FOLKETINGET
STATSREVISORERNE

FOLKETINGET
RIGSREVISIONEN

December 2024
– 7/2024

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

IT security in Banedanmark's signalling system

1. Introduction

1.1. Purpose and conclusion

1. This report concerns the IT security in Banedanmark's signalling system. The signalling system transmits signals between trains and traffic control centres, thereby managing railway traffic.

2. The railway is a crucial part of public infrastructure. The railway consists of more than 3,000 km of tracks including various critical components that support train operations, such as radio masts, fibre cables, power systems, and the signalling system. The railway is therefore vulnerable to incidents of various kinds, and Banedanmark faces a wide range of potential incidents that could affect both physical and digital infrastructure and thereby disrupt train operations. As the responsible authority, Banedanmark must prioritise efforts in relation to the various risks the railway faces.

The Centre for Cyber Security assesses that the risk of cybercrime against the railway sector is very high and that the sector's IT suppliers are prime targets for hacker attacks. An example of this risk was demonstrated in November 2022, when DSB was subjected to a cyberattack via an app from a supplier, causing S-train services to be halted for several hours.

3. Banedanmark has initiated a modernisation of the railway's signalling system with a total budget of approximately DKK 22 billion (2024 prices). Towards 2033, Banedanmark will replace all analogue signals along the railway with a digital signalling system. The system informs train drivers whether to proceed or stop and helps prevent collisions. However, as the system is digital, it introduces various IT security risks. Banedanmark defines the signalling system as a critical societal IT system, meaning that major operational disruptions can cause significant challenges for society. System failures will have consequences for both passenger and freight transport, and prolonged failures can have socio-economic consequences.

4. The purpose of the study is to assess whether Banedanmark has ensured satisfactory IT security in the signalling system to withstand incidents that can cause system failures.

Rigsrevisionen initiated the study in November 2023.

The signalling system
The signalling system covers both the mainline railway and the S-train network. This study focuses solely on the mainline railway.

The mainline railway refers to the nationwide rail network primarily serving intercity and regional trains. It connects major cities across the country. Banedanmark is responsible for maintaining the infrastructure, while DSB and Arriva operate train services.

5. The study is based on the international information security standard ISO 27001, which has been mandatory for government agencies since 2016.

ISO 27001 requires each authority to assess IT risks and prioritise necessary security measures accordingly. Based on this risk assessment, the authority must develop an action plan that prioritises the most appropriate security measures. The authority may choose to accept certain risks and instead focus on other areas.

We have based our assessment on 19 evaluation criteria derived from ISO 27001, adapted to Banedanmark's specific conditions. During the study, we adjusted these criteria to ensure we examined the most critical aspects of IT security in the signalling system. We assess that these 19 criteria allow us to make a comprehensive assessment of IT security in the signalling system.

Previous Rigsrevisionen reports on IT security in the public sector

- Report on Energinet's Outsourcing of Critical Infrastructure Operations (No. 14/2021)
- Report on the Government's IT Preparedness (No. 3/2022)
- Report on the Government's IT Preparedness II (No. 5/2023)
- Report on IT Security on Statens IT's Servers (No. 6/2023)
- Report on the Financial Supervisory Authority's IT Supervision (No. 14/2023)

We have used the same methodology in several similar studies, including examinations of IT security in government agencies, as seen in the reports on Energinet's outsourcing of critical infrastructure operations (No. 14/2021) and the reports on the government's IT preparedness (No. 3/2022 and No. 5/2023).

6. Banedanmark has assessed that the IT security issues identified in Rigsrevisionen's study contain confidential information, as they can expose vulnerabilities in the signalling system and thereby increase the threat level against Banedanmark. Banedanmark has stated that these issues only affect the duration and extent of service disruptions and do not impact passenger safety or general operational safety.

Rigsrevisionen has accommodated Banedanmark's request for confidentiality. Therefore, this report only includes general and summary descriptions of the IT security issues in the signalling system.

Conclusion

Banedanmark has significant vulnerabilities in the IT security of the signalling system. Rigsrevisionen finds this highly unsatisfactory. Consequently, there is a risk that IT security incidents can disrupt or halt train operations, which will be a major inconvenience for passengers and businesses. Prolonged system failures can also impact the national economy.