4/2017

STATSREVISORERNE
RIGSREVISIONEN

Extract from Rigsrevisionen's report on

the protection of IT systems and health data in three Danish regions

submitted to the Public Accounts Committee

November 2017

1. Introduction and conclusion

1.1. PURPOSE AND CONCLUSION

1. This report concerns the measures taken by three of the five Danish regions – Region of Southern Denmark, the Central Denmark Region and the Capital Region of Denmark – to protect access to the citizens' personal health data. Rigsrevisionen initiated the study based on IT audits conducted during the first six months of 2017.

2. The regions are responsible for running the Danish hospitals and thus also responsible for protecting sensitive health data. The regions are required to secure not only the confidentiality of health data, but also their availability and reliability so that the patients can receive timely and appropriate treatment. The regions therefore need to protect health data from falling into the wrong hands.

3. The threat against the regions' IT systems and data is growing in pace with the expansion of e-government in the regions and society in general, and so are the requirements for effective cyber-security systems. External intruders represent a threat to the regions, but so do staff in the regions if they intentionally or unintentionally abuse their access to IT systems and data.

The regions should therefore have basic security measures in place as protection against hacking and, at the same time, manage and control staff's access to IT systems and data. The latter applies, in particular, to staff with user privileges that give them full access to and control of the IT systems, because an intruder may gain the same access and control by taking over their privileges. Basic security measures in combination with management and control of user privileges can reduce the risk of compromising the regions' IT systems and data considerably.

4. The purpose of the study is to assess whether the three regions are protecting access to their IT systems and data in a manner that secures the confidentiality, availability and reliability of the citizens' personal health data.

HACKING

Hacking is an external intruder's attempt to gain unauthorised access to IT systems and data.

Hacking is also referred to as cyber attacks and security incidents.

BASIC SECURITY MEASURES

In this report the term "basic security measures" comprises the following:

- restrictions on download of programs
- running unauthorised programs is not allowed
- software and operating systems are security updated regularly
- staff are not holding local administrator privileges
- limit the risk that malware spread freely.

CONCLUSION

It is Rigsrevisionen's assessment that the three regions are not protecting the access to IT systems and health data in a satisfactory manner. As a consequence, unauthorised persons might gain access to sensitive and confidential personal data, which could affect the reliability and availability of important health data used in the treatment of hospital patients. Based on the results of the study and the current threat scenario, Rigsrevisionen finds that basic security measures against cyber attacks and protection of access to IT systems and health data should be a top priority for Denmark's five regions.

There are gaps in the regions' basic security measures against cyber attacks. Rigsrevisionen finds it particularly critical that almost all the approximately 27,000 people employed by the Region of Southern Denmark have local administrator privileges. This practice entails a significant risk that external intruders abuse the privileges of staff to gain access to and compromise IT systems and health data. The operating systems on a large number of computers in the Central Denmark Region and the Capital Region of Denmark are outdated and no longer security updated, which exposes the two regions to increased risk of cyber attacks.

To this should be added that the management of the Region of Southern Denmark has failed to provide an overall framework for IT security in the examined areas and management's prioritisation and management of IT security to protect health data therefore lack clear direction. An effective IT-security policy must be embedded in top management – particularly in large organisations like the regions.

Generally, the three regions need to improve their management and monitoring of staff with administrator privileges, for instance by reviewing the requirement to hold privileged accounts regularly. The fact that none of the three regions in the study have limited access to the internet when staff login with administrator privileges or restricted download of software to the extent necessary, increases the risk that staff, unintentionally, download malicious software that infects the IT systems and threatens health data.

During the audit, Rigsrevisionen detected passwords for system and service accounts in the Capital Region of Denmark and the Region of Southern Denmark that had not been changed for a very long time; some were six to nine years old and did not meet best-practice requirements for minimum number of characters in passwords. This increases the risk of internal and external abuse of access to IT systems and data. However, the study shows that the three regions are all focusing on limiting the number of system and service accounts with administrator privileges.

The logging systems implemented in the 3 regions are inadequate. Failure to log online activity makes it difficult or impossible for the regions to detect and track cyber attacks and abuse of user privileges. The Capital Region of Denmark is not reviewing log files systematically, and the Central Denmark Region has not implemented any of the three logging practices examined, despite the fact that the region has developed a logging policy.

The three regions have informed Rigsrevisionen that they have now taken steps to implement specific measures that will address several of the issues raised by Rigsrevisionen.