11/2017

STATSREVISORERNE
RIGSREVISIONEN

Extract from Rigsrevisionen's report on

protection against ransomware attacks

submitted to the Public Accounts Committee

1849

147.281 237

1976

114.6

22.480

908

February 2018

1. Introduction and conclusion

1.1. PURPOSE AND CONCLUSION

1. This report concerns whether selected essential government institutions have satisfactory protection against ransomware.

2. Government institutions are frequent targets of cyber attacks and ransomware is currently one of the biggest threats to cyber security. Ransomware is malicious software that blocks access to data. Generally, the ransomware will encrypt data and prevent the attacked institutions from using the data. Hackers will demand a ransom to decrypt the data, before the institutions can access the data again. It follows that Ransomware represents a particular threat to the accessibility of data.

Inability to access data can suddenly make it difficult for or prevent the institutions from delivering important services. Besides, institutions that have been hit by a ransomware attack are generally forced to shut down parts of or their entire IT network to investigate the extent of the attack. Last, a ransomware attack can have a significant economic impact, because the institutions risk suffering a loss of production, if, for instance, they are prevented from accessing their IT network or if data collected and processed over an extended period is lost. In 2017, a ransomware attack on the British national health services led to the cancellation of 19,000 operations and appointments. The management of the institutions should therefore have focus on the risk of ransomware attacks and implement the necessary security controls to protect against ransomware and reduce the impact of a potential attack.

RANSOMWARE
Ransomware is a type of *malware*, which is short for malicious software.

RANSOMWARE ATTACK
The word *ransomware* is a contraction of "ransom" and "software". A ransomware attack will typically block access to data and demand a ransom.

HACKER
In this report, a hacker is a person who attempts to infect computers with ransomware.

3. The study includes the Danish Health Data Authority, the Ministry of Foreign Affairs, Banedanmark and the Danish Emergency Management Agency. These four institutions were selected, because they are responsible for delivering essential services within health, foreign affairs, transport and emergency preparedness, where the access to data can be of critical importance. Furthermore, the Health Data Authority is delivering centralised IT services to the majority of government bodies under the Ministry of Health.

BANEDANMARK
Banedanmark is a government-owned enterprise that is responsible for maintaining, developing and expanding the Danish railway network.

4. The purpose of the study is to assess whether the four institutions have satisfactory protection against email-based ransomware attacks. We therefore examined 20 common security controls that provide basic protection against ransomware. In addition, we reviewed five security controls that the institutions should consider in connection with future risk assessments. Forward-looking controls include, for example, new technology that can reduce the number of fake emails entering an institution or detect and send alerts of unusual activity on computers.

The study was initiated by Rigsrevisionen and it is based on the findings of four IT audits carried out in the months April to September 2017. The study provides a snapshot of how well protected the institutions are against ransomware. The institutions have had opportunity to implement the 20 common security controls since the completion of the IT audits. Therefore, the results of the study concern only the institutions' protection against ransomware at the time of the four IT audits. The study provides a presentation of the performance of the four institutions, but it does not include a comparative analysis and ranking of their performance.

CONCLUSION

It is Rigsrevisionen's assessment that the four institutions do not have satisfactory protection against ransomware. The study shows that several common security controls to mitigate attacks have not been implemented by the four institutions. In particular, the Health Data Authority and Banedanmark had considerable gaps in security. This means that all four institutions are exposed to an increased risk of email-based ransomware attacks that would leave them unable to deliver their services for a shorter or longer period. All four institutions have informed Rigsrevisionen that they have worked on implementing several of the security controls to increase the level of protection against ransomware, since the study was completed.

The institutions' prevention of ransomware attacks, including both internal and external threats, is inadequate. It is of particular concern that none of the institutions has ensured that security software patches are up-to-date, and that three of the institutions have not implemented whitelisting to prevent staff from running malware. This increases the risk that ransomware infects parts of or the entire IT network and spreads.

WHITELISTING
Whitelisting or application whitelisting is the security practice of restricting systems from running software unless it has been cleared for safe execution.

In three of the institutions, the management is not sufficiently focused on the ransomware threat, and the risk assessments made by management in the Health Data Authority and Banedanmark do not cover all relevant aspects. This means that the institutions do not have an up-to-date assessment of the ransomware threat and are therefore in a weak position to prevent new attacks and reduce the impact of future attacks. Management in the Health Data Authority and Banedanmark have not had adequate focus on risk assessment, and IT security in these two institutions is therefore not based on priorities defined by the management.

Three of the institutions do not have adequate incident response plans in place to help them re-establish their operations after a ransomware attack. It is particularly significant that three of the institutions do not regularly test whether they will be able to restore data and systems affected by a ransomware attack. It increases the risk that the data held by these institutions is lost in connection with a ransomware attack and that the institutions will be unable to deliver their services for an extended period of time.

As the risk scenarios are constantly changing, it is important that the institutions consider implementing forward-looking security controls to increase their resilience to ransomware attacks, i.e. controls that facilitate verification of the identity of email senders and can detect and filter out potentially harmful emails. All four institutions are currently working with some of the forward-looking security controls that can help increase their protection against ransomware attacks.