RIGSREVISIONEN

Extract from the report to the Public Accounts Committee on the access to IT systems that support the provision of essential services to the Danish society

October 2015

1. Introduction and conclusion

1.1. Purpose and conclusion

1. This report concerns the measures taken by a number of government institutions to protect IT systems and data that support the infrastructure of the Danish society from unauthorised access, obtained on the basis of domain administrator privileges.

2. Like all other IT systems, also IT systems that support the provision of essential services to society, can be accessed by users with domain administrator privileges. These privileges represent the highest level of access and control over the institutions' IT systems and data and they are managed in the so-called *Active Directory (AD).* Privileges of this nature may also allow circumvention of security measures implemented by the institutions. Depending on the system design of the institution, domain administrator privileges may also give access to essential IT systems and data that are not managed in the AD.

Active Directory (AD) *is a management system, which allows the institutions to manage and control access rights to systems and data.*

Security measures *are designed to contribute to preventing or detecting that IT systems and data are abused and compromised. Measures can include, for instance, technical restrictions to prevent undesired actions.*

3. The report concerns the following six institutions: Energinet.dk (government enterprise under the Ministry of Energy, Utilities and Climate that owns the Danish electricity and gas transmission system), Banedanmark (government enterprise responsible for maintaining and running the Danish railway network) under the Ministry of Transport and Building, National Sundheds-it under the Ministry of Health with responsibility for the development and running of the department's IT systems, the Agency for Governmental IT Services under the Ministry of Finance with responsibility for IT running on behalf of a number of departmental portfolio areas, the Danish Prison and Probation Service, and the central IT department for the Danish police under the Ministry of Justice. These six institutions deliver a broad range of essential services to the Danish society.

4. The institutions rely on well-functioning and secure IT systems to perform their tasks effectively. It is therefore crucial that the institutions manage and control domain administrator privileges to mitigate both internal abuse, where trusted employees abuse their domain administrator privileges or handle their privileges negligently, and external abuse where a hacker, for instance, has managed to obtain unauthorised access to the IT systems of the institution and is taking over and abusing the domain administrator privileges. For instance, a hacker may obtain access to IT systems and data that are managed in the AD. It is also important for the institutions to ensure adequate monitoring of privileged user activity in order to detect and resolve incidents where IT systems and data are abused and compromised.

IT systems and data are abused and compromised *if a person obtains unauthorised access to any number of the institution's IT systems and data. A person may, for instance, interrupt or change the execution of programs or change, delete or read/steal data.*

5. It appears from the *Intelligence Risk Assessment 2014* report issued by the Danish Defence Intelligence Service that the technological development has increased the risk of cyber attacks and that the risk pattern is constantly changing, which has again increased the need for security measures. To this should be added that it appears from the risk assessment report from 2013 that the threat posed by employees who negligently or deliberately compromise security in their workplace is also growing.

6. The institutions' execution of their tasks may be affected and disrupted if their data are abused and compromised. Moreover, at certain institutions, abused and compromised data may also jeopardize the security of confidential personal data and other confidential data. The nature of the consequences of abused and compromised IT systems and data vary and depend on the task portfolio of the individual institutions.

The institutions have informed Rigsrevisionen that they have implemented various compensating measures to limit both the risk and consequences of unauthorised access obtained via domain administrator privileges and the risk that data are abused and compromised. According to the institutions, this means that abuse of domain administrator privileges in the ADs examined, will not affect the supply security for electricity and gas and the safety of railway operations, for instance. According to the institutions, it is not possible to obtain access via the domain administrator privileges in the ADs to IT systems and data that are used in connection with the direct treatment of patients. Nor is it possible to access to critical IT systems and data that support the police in their work be obtained through the ADs.

7. The report is focused on the significant risk that is associated with inadequate management and control of domain administrator privileges, which makes it possible for unauthorized persons to obtain access to the IT systems and data of the institutions. Rigsrevisionen has not examined for what specific purposes unauthorised access to the institutions' systems and data can be used.

8. The study is based on IT audits performed by Rigsrevisionen during the first half of 2015.

9. The study disclosed a number of critical security gaps that will represent a security risk until the institutions have rectified the situation. For IT security reasons, Rigsrevisionen has therefore made the exceptional decision to anonymise the audit findings.

Rigsrevisionen finds it important to publish the results of the study, which may apply to a circle of government institutions beyond the six examined in the report and therefore may contribute to improving IT security in the government, in general.

10. The purpose of the study is to assess whether government institutions follow the recommendations on good IT security practices to protect access to IT systems and data that support the infrastructure of the Danish society. We have therefore examined how the institutions manage and control domain administrator privileges, including how the institutions monitor and log privileged user activity.

CONCLUSION

It is Rigsrevisionen's overall assessment that the six institutions, at the time of the examination, did not comply with a number of generally accepted recommendations on good IT security practices to protect access to IT systems and data that support the infrastructure of the Danish society. Especially two of the institutions did not comply the recommendations.

That the six institutions have not complied with the recommendations may increase the risk of unauthorised access to IT systems and data that are managed in the AD. Consequently, the delivery of essential services to society may be affected and disrupted, and the security of confidential data, for which the institutions are responsible, may be at risk.

The study revealed a number of weaknesses in the management and control of domain administrator privileges in all six institutions. Rigsrevisionen would like to highlight the fact that the institutions have not adequately limited the number of domain administrator privileges. The institutions have not changed non-personal passwords annually, and the majority of these passwords are up to seven years old. A few of the passwords have not been changed since the late 1990s.

The study also showed that the use of domain administrator privileges was inadequately logged; for instance, four of the institutions have not separated the duties for administrators with access to the logging system, which makes it possible for persons who have obtained unauthorised access to the system to cover their tracks. Moreover, five of the institutions are not reviewing their log files regularly, which reduces their chances of detecting and resolving abuse of domain administrator privileges and IT security breaches.

In light of the IT security risk to which the government is exposed, Rigsrevisionen finds that the institutions should improve their management, control and logging of domain administrator privileges in order to reduce the risk that IT systems and data, managed in the AD, are abused and compromised. Since the risk exposure constantly changes, the institutions should also, regularly and actively, consider the effectiveness of their management, control and logging of domain administrator privileges.

It is Rigsrevisionen’s assessment that several of the weaknesses detected in the management, control and logging of domain administrator privileges can be rectified relatively easy, whereas other will be costly and require more work to correct. Rigsrevisionen therefore concludes that management needs to focus and prioritize the area to correct the problems identified during Rigsrevisionen’s examination.

The institutions have informed Rigsrevisionen that they have implemented various compensating measures and that they, since the study was made, have planned, launched and implemented steps that will correct a number of the established weaknesses.