Security of server rooms and office premises

Is the physical security of premises related to the State's IT infrastructure ensured?

Report of the National Audit
Office to the Riigikogu
Tallinn, 30 October 2023

Security of server rooms and office premises

Is the physical security of premises related to the State's IT infrastructure ensured?

What did we find and conclude from the audit?

IT Centre – institution managed by the ministry, which handles the administration of the ICT of the area of government and the development and maintenance of information systems

Necessary security measures are generally implemented in the server rooms and technical rooms necessary for the operation of server rooms in ten audited state institutions and one audited legal entity in public law. Primary security measures are implemented in the office premises of IT centres to ensure physical security, and the risk of unauthorised access to the premises has been mitigated to an acceptable level.

Despite the positive overall assessment, the National Audit Office found some deficiencies in ensuring the physical security of server rooms and office premises.

During the audit, the National Audit Office found several problems in ensuring the necessary conditions in server rooms, i.e. in the operation of cooling and ventilation equipment, but also fire, smoke and water leak detectors. In some of the server rooms observed during the audit, cooling of the room was organised inefficiently. In addition, uninterruptible power supplies and cooling devices were located inside the older server rooms in two of the audited institutions, which increases the risk of equipment overheating or fire. Some server rooms did not have precision air conditioning equipment in use. Combustible materials, such as cardboard boxes, were stored in the server rooms and auxiliary room to the server room in some of the audited institutions.

The National Audit Office made observations about the security of server rooms and office premises and the protection of security systems. In one of the audited institutions, the server room was not under alarm. The video surveillance system of another audited institution was not sufficiently protected, and the central unit of video surveillance was accessible to an excessively large number of users. In several institutions, the procedures did not specify the minimum period for retention of video surveillance recordings, and one institution did not have access and security logs. In the office building of one of the audited institutions, only office premises on the entrance floor were under alarm during off-hours.

In the protection of the outer security perimeter of the buildings of server rooms, there were problems with the protection of facilities necessary for the operation of server rooms. For example, the outer perimeter of the building of one of the audited institutions was not covered with the necessary sensors. There were also shortcomings in the protection of one servicing substation.

In the organisation of access management, we found problems in the implementation of both organisational and technical measures. For

example, the server room of one of the audited institutions was accessed with one-factor authentication, i.e. using only an access control card. In another institution, it was possible to access the central unit of the access system with administrator rights from a security desk computer.

As a result of the audit, the National Audit Office made more detailed observations about the security of each audited institution and gave recommendations on how to improve the situation.

Responses of the auditees: The auditees agreed with most of the observations and recommendations of the National Audit Office and presented their plans for eliminating the deficiencies and implementing the necessary security measures. Regarding individual observations, the audited institutions decided to accept the risks and/or implement other additional security measures to mitigate the risk.