Database access management

Does database access management ensure that only authorised individuals can access data?

Report of the National Audit Office of
Estonia to Riigikogu
Tallinn, 1 February 2023

Database access management

Does database access management ensure that only authorised individuals can access data?

Summary of audit results

The audit of the National Audit Office showed that, although access management ensures that only authorised persons can access the data in the audited databases, in the case of two databases, the access rights that these persons have are too broad. Institutions must address analysing log data and checking the validity of data queries more than before in order to prevent incidents or reduce the impact of incidents that have already occurred.

The mandatory information security implementation audit for national databases was carried out in four of the five audited databases. These audits did not verify the security measures of the access management module as the auditors were not required to do so pursuant to the audit guidelines of the three-level baseline security system ISKE. Auditing of access rights should be made mandatory for sensitive data in the future, as it would help to mitigate risks related to data security.

In the SKAIS1 (Social Security Information System) and STAR (Social Services and Benefits Registry) databases, user access is too extensive. For example, in STAR, an official of a local authority has access to procedures related to residents of other local authorities and data contained therein. Insofar as STAR has not implemented measures necessary for verifying the analysis of logs and the justification of queries, the risk of misuse of data increases.

Log data, i.e. information about the events that occurred in the database, were collected and stored in the audited databases, but these logs were not systematically or regularly analysed and the respective obligation was not established in the documents governing the activities of institutions or databases. It is necessary to analyse the log data in order to detect errors or incidents committed in the databases on an ongoing or retrospective basis and to determine the reasons for their occurrence.

No regular or systematic monitoring or check of the justification of queries has been carried out in the audited databases. Such checks were not regulated in detail in the documents governing the activities of institutions of databases either. Checks were carried out irregularly and only after discovered incidents, queries/complaints from data subjects, or other external events.

In 2021, the Incident Response Department of the Information Systems Authority registered about 73,800 automated reports regarding security vulnerabilities and about 2,200 incidents with impact in Estonia (see Figure 1). Most of these incidents were based on access takeover or were

Audited databases:

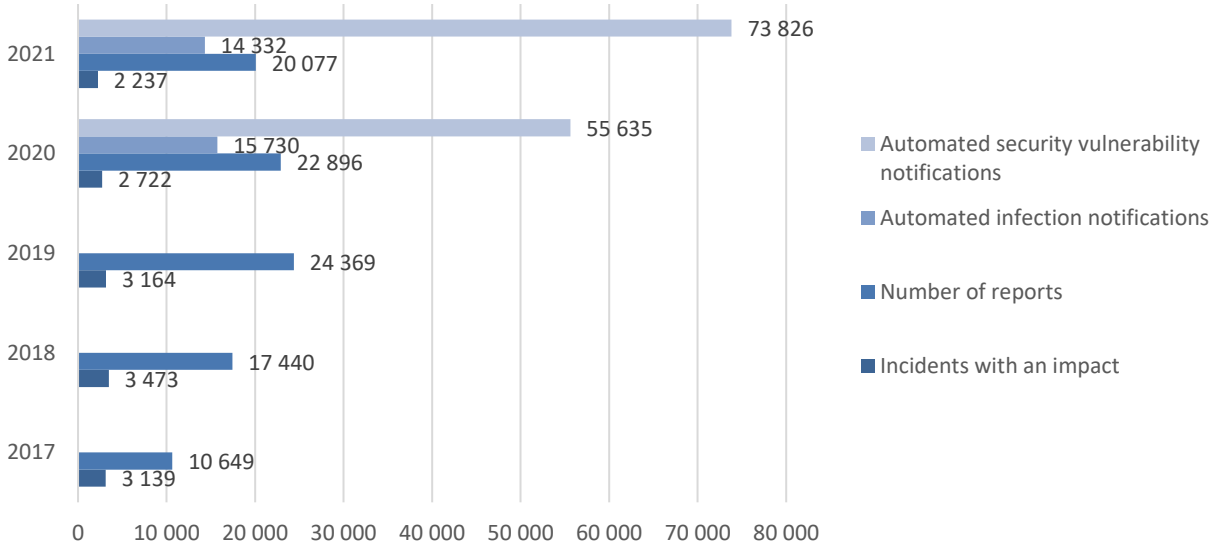
- Social Security Information System (SKAIS);
- Social Services and Benefits Registry (STAR);
- Criminal Records Database;
- e-File misdemeanour procedure interface; and
- Automatic biometric identification system database.

Main audit observations

aimed at exploiting access rights to take over user accounts of others and thereby compromise the integrity of data or leak data.

National databases that contain large amounts of personal data can also be a target for cyber attacks.

Figure 1. Incidents and reports in 2017–2021



Source: Information System Authority

Main recommendations of the audit

Recommendations of the National Audit Office to the Minister of Justice, Director General of the Police and Border Guard Board, Director General of the Social Insurance Board, Director of the Health and Welfare Information Systems Centre, Director of the Centre of Registers and Information Systems, and the Director General of the Information Technology and Development Centre of the Ministry of Social Affairs:

- Improve the information security procedures of areas of government or institutions in such a way that the verification of the justification of queries is also regulated.
- Improve the information security procedures of areas of government or institutions in such a way that obligation to carry out ongoing analysis of logs is also regulated as well as adopt the security information and event analysis tool SIEM.

The Chancellor of the Ministry of Justice, Director General of the Police and Border Guard Board, Director General of the Social Insurance Board, Director of the Health and Welfare Information Systems Centre, Director of the Centre of Registers and Information Systems, and the Director General of the Information Technology and Development Centre of the Ministry of Social Affairs agree with the recommendations of the National Audit Office and commence with implementing them this year.

Recommendation of the National Audit Office to the Minister of Entrepreneurship and Information Technology:

- Change the rules and guidelines for auditing the implementation of the information security framework (ISKE and later E-ITS) so that access rights are also audited for at least the moderate integrity and confidentiality security class.

The **Minister of Enterprise and Technology** replied that according to the guidelines for an audit based on E-ITS established on 16 December 2022, the auditor checks how the organisation has implemented the basic measures applied to it. If these measures have been implemented partially for some reason, this aspect will also be checked. In E-ITS, there are measures related to access management, such as rules for managing user accounts, granting, changing and revoking rights, and documenting user rights.

Recommendation of the National Audit Office to the Director General of the Social Insurance Board and the Director of the Health and Welfare Information Systems Centre:

- Ensure that users of the STAR database in local authorities can only access the data and related procedures of people who have registered the address of their place of residence in the same local authority. However, if access to procedures related to residents of other local authorities is needed, determine the control procedure for additional access validation.

The Director General of the Social Insurance Board replied that from the point of view of the Board, this is not a redundancy as the need for a broader approach is related to the specifics of the work of local authorities.

Comment of the National Audit Office: If, in the opinion of the Social Insurance Board, it is not possible to organise the access request procedure quickly enough and in the way that the process of assessing the need for assistance requires, other measures must be implemented to prevent and detect misuse of data (see points 64 and 86).