Riigi Infosüsteemi Amet

Estonian Security System Overview

Topics

- History and the reasons for choosing IT Grundschutz;
- ISKE;
- Auditing/Certification
- Future challenges;
- Problems;
- Conclusions

Why we needed IT Security Standard?

- In which level should be citizen's data protected?
- How much should ministries and agencies invest into IT Security?
- How to estimate availability, integrity, confidentiality needs in the same scale?

Selection of base system

- We needed standard which:

  Has appropriate security goals and security level;

  Has big granularity;

  Is updated regularly- at least after every1-2 years;

  Is available free of charge or with very low costs;

  Preferably European Standard.

IT security standards in 2003

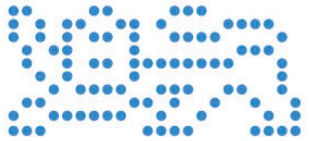
- ISO 13335;
- ISO 17799;
- **BSI- IT Baseline Protection Manual;**
- Canadian Handbook on Information Technology Security;
- US Department of Energy Security Manuals;
- Information Security Baseline Controls, Australia;
- NIST 800 series

Why IT Grundschutz?

- Regularly updated;
- **No need for time consuming risk-assessment;**
- Comprehensive set of safeguards;
- Suitable granularity;
- Enables to justify investments into IT security in a needed level;
- Enables to develop a common understanding about the security level needed in public sector information systems.

Information Security

Information security is an on-going process, which is aimed at ensuring the confidentiality, integrity and availability of data and assets. The goal is to find a balance between these three components.



The aim of Cyber security

- Protect against IT risks and mitigate them;
- To ensure service continuity;
- Maximizing the return of investments;
- The compliance function (laws, standards, etc);
- Creating a strong and safety image to partners

ISKE

- An information security standard that is developed for the Estonian public sector.
- The goal of ISKE implementation is to ensure the security level sufficient for the data processed in IT systems;
- The necessary security level is achieved by implementing the standard organizational, infrastructural/ physical and technical security measures;
- The preparation and development of ISKE is based on a German information security standard - IT Baseline Protection Manual (IT-Grundschutz in German), which has been adapted to match the Estonian situation.

ISKE

- Chronology:

1998 first attempt to adopt the IT baseline Protection Manual;

2003 first version in Estonian- called ISKE, based on 2003 English version of the ITBPM;

Government decree on the system of security measures for information Systems;

2008 ISKE must be implemented in Estonian public sector (organizations processing important registers);

2012 Dec, latest version in Estonian- based on IT Grundschutz ver 12.1

ISKE as baseline security system

- **Baseline security system** – one set of developed security measures, which will be applicable to all information assets, regardless of their real security requirements. Contains more than 1,000 security measures. The main disadvantage of the system is the implementation of an average set of measures to systems with different security requirements.

ISKE as three-level baseline system

- **Three-level baseline security system** – three different sets of security measures for three different security requirements have been developed (different databases and information systems may have different security levels). Compared to the one-level baseline security system this version is more accurate (economic), while being more inaccurate, compared to detailed risk analysis.

ISKE as three-level baseline system

- The levelled baseline security system is more economical, as there is no need to exercise expensive security measures on data with limited security requirements.
- Additional expenses on data and information system analysis and for outsourcing the required set of security measures will be applicable to the implementation of a security system of different levels.

How IT BPM was adopted?

Simplified process for the implementation of ISKE

1. Mapping of databases
2. Mapping of information systems and other information assets
3. Identification of links between databases, information systems and other information assets
4. Identification of required security class and level for databases;
5. Identification of required security class and level for information systems and other information assets
6. Identification of typical modules, which comply with information systems and other information assets
7. Identification of required security measures for information systems and other information assets

ISKE- Government Regulation

- According to the Government of the Republic Regulation no. 273 of 12 August 2004- ISKE is compulsory in organizations of state and local administration who handle databases/ registers.

Auditing

- Regulated by the same government act;
- Ministries, agencies + registers connected to the state IS-> obligated to perform IT audit:
  - H level-> every 2 years;
  - M level-> every 3 years;
  - L level-> every 4 years
- Local county gov.-s Ministry of Economic Affairs orders “randomly”

Problems

- Taken as an obligation, not as an helpful handbook;
- Is designed for large corporations;
- auditing process is a little bit expensive because it is carried out by CISA certified auditors;
- Handbook is over 3000 pages long, and that is scaring some people out.

Conclusions
IT Grundschutz to ISKE

- We made a right choice several years ago;
- Customization is possible with low costs;
- Good quality level translation also;
- Big challenge is to increase the effectiveness of standard implementation and auditing.

Sample security measures

- From ISKE Implementing instructions
  - Background vetting upon hiring staff
  - 24/7opportunity for the notification of incidents
  - Logging of remote access
  - Remote indication, notifying of mail server space being over quota
  - Server room temperature monitoring with automated notification of excessive deviations
  - Reserve generator
  - Automated notification of several failed log-in attempts
  - Requirement to accompany visitors

Sample security measures 2

- Video surveillance
- Object based or combined authentication
- Automated notification of several failed log-in attempts
- Remote maintenance, performed via modem, is prohibited
- Installation of water pipes prohibited in server and archive premises
- Periodical replacement of cell phone batteries
- Two spare communication channels
- Use of virus control and attack identification software of two different providers
- Requirement for documenting and marking of cabling works within 2 hours

Questions?

Thank you for your attention!

For more information:

Aare.Reintam@ria.ee