Implementation of security standards and procedures

Tõnis Reimo
tynis@cyber.ee
Topics

In this section we will discuss about security standards and implementation of IT security system. We will give overview about practices of implementation of security systems.
Evolution of approach

- Information Security is something...
  - … which is problem of IT department?
  - … which is problem of CEO/CIO/CTO?
  - … which involves all main resources and business processes in company. Responsibilities for security processes are defined in organization.
Hard facts...

- Information is a nation's greatest asset
- Accidents, errors, negligence, cyberattacks are everyday reality
- Ensuring security is a laborious, expensive and reduces a usability
- Information security is a "crafty": all the ways must be prevented, the technology is not enough: the organization, infrastructure, procedures, technical measures
Data Security?

- Components of Information security:
  - Availability -
  - Confidentiality -
  - Integrity -

- **Requirements**
  - Legal & Business

- **Processes**
  - User management and System administration

- **Resources**
Implementation process

- Legal & business requirements
  - Security/Risk analysis – defining the assets
    - Security policy
      - Security measures:
        - Organizational measures
        - Technical measures
  - Whole process is time consuming and costly
Level of (Information)security and costs

<table>
<thead>
<tr>
<th>Costs</th>
<th>Incidents</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>100</td>
<td>0</td>
</tr>
</tbody>
</table>
Common problems

- Most of systems:
  - Use *similar* technology
  - Operated by similar processes
  - Have similar security requirements

- **Security specialists are not in every organization!**

- **IT Baseline Protection**
  - Standardized solutions to common problems
  - IT Baseline standards
    - BSI guidelines and catalogue
    - ISO/IEC 13335-3 *(discontinued)*
Cost of security

- Incidents
- Information Security
- Total

Cost vs. Security level

- Low
- Medium
- High

Security level 0 to 100
Pains

- Need for security is recognized after incidents
  - Most of incidents will pass unnoticed.
- Change of work processes → opposed by the employees and management:
  - 90% of implementation work is internal sales and PR
- Financing must be ensured for:
  - Technology
  - Audits
  - Training
  - Additional workload to IT department
Implementation process

1) Create list of informational assets
2) Define security classifications of databases
3) Define security classifications for other assets
4) Define security levels for classified assets
5) Analyze need for security zones
6) Add security modules to specification of informational assets
7) Create list of security measures
8) Create implementation plan for security measures
9) Implement it
10) Check security situation, evaluate risks, implement additional measures (when needed)
Action plan

- Create a team, train them, motivate (incl. management)
- Get understanding, to what/which you can implement baseline security
- Valuate security classifications levels, create zones in organization (when needed)
- Select modules -> measures
- Create implementation plan for management and technical measures
  - Prioritize
  - Valuate and create plan for use of resources
  - Give a tasks to responsible persons
- Implement
- Check situation of actual security situation, valuate risks, change when needed
- Audit, start from beginning - **Continuous process!**
Challenges

- To get management support – not just financial, but their real interest for results
- To get people understand that security help to increase quality and peace of everyday work.
- People respect rules and agreements when they have been involved to the process
- Tech specialists are needed – specially for documentation, recovery plans, backups etc. (1 doc.writer, 1 for tests)
Challenges

- Start is hardest part. When policy is implemented – it will be optimized during practical use.
- Get opinion-leaders behind your initiative
- Create user-groups: a place where to complain about hardship (in beginning) and exchange experiences (later)
- Routine. Security situation must be reviewed at least once in a year.
- Each process must have a person who is responsible
Challenges

- Keep management/audit roles separated from executing roles.
- People do not understand how important might be info in their local hard drives. They do not recognize risks: information leaks, errors created during synchronization, loss of data,
- People are lazy – it's hard to get them document where they keep and which kind of information.
Upcoming challenges

- Security management outsourcing?
- Security in cloud e-services?
References

- COBIT – www.isaca.org/cobit
- ISO12207, ISO27000
- https://www.isaca.org/
- GTAG (Global Technology Audit Guide)
  http://www.theiia.org/guidance/technology/gtag/
- https://www.bsi.bund.de/cln_174/ContentBSI/EN/Publications/BSI_standards/standards.html
- https://www.bsi.bund.de/cln_174/ContentBSI/grundschutz/kataloge/kataloge.html