FRAME / METHODOLOGY FOR THE INFORMATION SECURITY MANAGEMENT IN AN E-GOVERNMENT ENVIRONMENT

Ing. Mag. Kristian Tomov,
Dr B. Balabanov
SUMMARY

• INTRODUCTION.
• INFORMATION SECURITY (IS).
• THE SECURITY OF INFORMATION SYSTEMS.
• CATEGORIZATION OF THE INFORMATION SYSTEMS.
• BASIC REQUIREMENTS FOR SECURITY MANAGEMENT AND SECURITY CONTROLS.
• SELECT THE BASIC REQUIREMENTS FOR SECURITY MANAGEMENT AND SECURITY CONTROLS.
• INFORMATION SECURITY STANDARDS AND GUIDELINES.
• FRAME / METHODOLOGY FOR THE INFORMATION SECURITY MANAGEMENT.
• ELECTRONIC SERVICES.
• THE eGOVERNANCE SERVICES.
• eGOVERNANCE INFORMATION SECURITY.
• THE MANAGEMENT OF eGOVERNANCE INFORMATION SECURITY (1,2,3).
• IMPLEMENTATION AND IMPROVEMENT OF SECURITY CONTROLS BASED ON RISK ASSESSMENT.
• PLANNING ACTIVITIES.
• CONCLUSIONS.
INTRODUCTION

The biggest threat to the government data is the human error, rather than the actions of an malicious hacker and the involved malware. This fact was discovered during a 3-year period of research performed by Rapid7 (http://www.rapid7.com/docs/Data-Breach-Report.pdf). This report is including all reported intrusions and thefts of media leading to the loss of data in the US governmental environment.

Human errors are responsible for 29% of the incidents reported by the agency in the past three years, which made the threat in the first place in terms of the number of violations. Second ranked is the loss or theft of portable devices via which the government has lost more than 80 million records, which are amazing 86% of the total officially recorded data thefts.

Based on statistics data collected in a period from the 01.2009 to the 03. 2012 the officially registered incidents were 268, via which a loss of about 94 304 173 records was registered.

In the first place were the human errors, with 78 incidents and about 11,783,776 recorded lost, the second is the loss of mobile devices (51 incident and 80706983 lost data), the loss of physical media such as CDs and/or other forms of memory in 46 incidents resulted in a loss of 296,710 records.

Only 40 incidents in a period of three years is the count on malicious hacker attack and which led to the loss of 1,082,749 records.
INFORMATION SECURITY (IS)

Information security means protecting information and information systems from unauthorized:
- access,
- use,
- disclosure,
- disruption,
- modification,
- perusal,
- inspection,
- recording or destruction.

Information security is a set combining organizational security and IT security.

INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

Systems for information security management designed to ensure the confidentiality and integrity of the organization information assets. These include policies and procedures within the organization that serve to manage, control, maintain and improve the information security.
The security of information systems is essentially a grouping of:
- security applications,
- infrastructure security
- and secure management.

The deployment, management and security at all levels is essential to achieve a secure environment, the probability of simultaneous security breaches on all layers is less likely.

This approach has been identified as the most effective in the context of the contemporary management of IT security.

This tiered approach is an approach known as "Defense in depth".

The risk analysis must consider:
- the intention and motivation,
- capability of threats,
- relevance,
- and frequency of potential attacks and/or any other kind of threat.
CATEGORIZATION THE INFORMATION SYSTEM SECURITY

Categorization in security is based on the potential impact of an threat on the organization, when certain events impact the information system and compromise it.

The system which is a part of the overall delivery system and is necessary for the service delivery of the organization and needed to perform the assigned mission, protect its assets, to fulfill its legal obligations to support their daily operations and to protect individuals, whether it is for customers and/or employees.

Categorization in security should also consider vulnerabilities and provide information about known threats to information systems and the corresponding applications.

All systems can be categorized in accordance with the impact in the following three categories:
- poor,
- medium
- high impact.
BASIC REQUIREMENTS FOR SECURITY MANAGEMENT AND SECURITY CONTROLS

- Categorization of Information Systems
- Select the basic requirements for security and controls
- Risk Assessment
- Implementation and improvement of security controls
- Monitor the effectiveness of controls and management
Basic requirements for security management and controls (also called Baseline Security Controls - BSC) are the minimum requirements for the achieving of the information security:
- security requirements for applications,
- security requirements for the infrastructure,
- security requirements for operations and for the overall security management.
- security requirements for corporate information and corporate information systems in each category.

The BSC will have five areas covering:
- general security management aspects,
- general requirements for information security,
- application security,
- infrastructure security,
- network security
- IT security systems.

(Similar to the German national approach to information security management).
The subject of information security management is handled in different standards as well as national and de-facto standards. Some standards are summarized below:

**ISO 27001 / ISO 27002**

In recent years, the complexity of information technology and the demand for certification appeared numerous manuals, standards and regulations for IT security. ISO / IEC 27001 "Information technology - Security techniques - Information systems security management, requirements specification". ISO27001] is the first international standard for information security management, which also allows a certification in accordance with the ISO 27001 requirements.

**IT-GRUNDSCHUTZ**

IT-GRUNDSCHUTZ is a national standard for information security management in Germany. It has spread to Switzerland and Austria. The standard is based on ISO 27001:2005, in terms of structure, but it is much more technically oriented. The standard consists of 4 catalogs (in a volume of 4000 pages), including information on the development of ISMS, methodology for implementation of ISMS, risk assessment and management continuity. Additional standard registers are required for all 4000 controls (unlike ISO 27001:2005 with 133 controls) and threats. The development of detailed risk assessments are conducted in specially designed application.
The security of information systems is essentially a grouping of:
- security applications,
- infrastructure security
- and secure management.
The deployment, management and security at all levels is essential to achieve a secure environment, the probability of simultaneous security breaches on all layers is less likely. This approach has been identified as the most effective in the context of the contemporary management of IT security.
The electronic service must have the following characteristics:
- Users should be informed about the available electronic services;
- Users should be aware of the benefits of these services;
- The user should be able to easily find electronic services which they need.

E-services must be accessible to all members of the intended target groups.

The information from electronic services need to be:
- comprehensive,
- accurate,
- accessible
- and easy to understand in terms of language and structure.

The provision of electronic services should be confidential service and does not violate the privacy.
THE eGOVERNANCE SERVICES

The design of eGovernance applications must be consistent, including existing legal requirements for management of data and relevant legal and regulatory requirements. From the above considerations for possible attributes, it becomes clear that the "value" of information stored and processed by eGovernance services must be protected at all levels:
- applications,
- infrastructure,
- the operation
- and active management of the service.

Information security is designed to protect information assets and is determined in terms of:
- confidentiality,
- integrity
- and availability.

A possible approach is to create security layers.

These security measures provide levels of protection including:
- applications,
- infrastructure,
- operation
- and management of the eGovernance environment.
The Governments around the world are using eGovernance and thereby information technology as an opportunity and initiative to improve:
- the interaction between government and citizens.
- the interaction between government and business,
- as well as the international governmental operations.

The eGovernance methodology should focus on providing technically secure services, but also have to provide:
- efficiency,
- effectiveness,
- flexibility
- and transparency.

The goal is that a citizen or partner should always have the opportunity to maximize the benefits of the electronic services provided by the public e-GOVERNMENT (??).
THE MANAGEMENT OF eGOVERNANCE INFORMATION SECURITY (1)

It was found that information security can be ensured only through the selection and implementation of appropriate security controls through proper risk management. The main activities in ensuring security of the information are as follows:

a) Classification of information systems,
b) Selection of controls and development of basic national requirements for information security management in the e-GOVERNMENT, including:
   - requirements for internal staff,
   - requirements for infrastructure & applications management,
   - as well as software development requirements,
   - requirements for the management and delivery of services by government.

c) Risk assessment;
d) Improve and / or enhance the security controls based on risk assessment;
e) Implementation of security controls;
f) Monitoring and analyzing the effectiveness of security controls;
g) Continuous improvement of internal controls and improvement of the internal control system managing information security.

Management as one of the determining factors for the success of the strategy and how to manage information security should be based on the methods which requires constant improvement of internal controls and management approaches.
THE MANAGEMENT OF eGOVERNANCE INFORMATION SECURITY (2)

Planning (creating ISMS) -
Creating a policy, objectives and ISMS procedures

Enforcement -
implementation and operation of the ISMS;

Check - monitor and review the ISMS;

Action - maintain and improve the ISMS.
THE MANAGEMENT OF eGOVERNANCE INFORMATION SECURITY (3)

Implementation of Information Security is **not an event but a process.** Continuous improvement is the basis on which the construction and implementation of an information security management system, with many compliance requirements, is build.

**Also known as the demings-cycle-it is designed to optimize business operations and processes in the body of the company management.**

**Planning (creating ISMS)** - Creating a policy, objectives and ISMS procedures relating to risk management and improving information security to deliver results in line with the overall policy objectives of the organization.

**Enforcement (implementation and operation of the ISMS)** - Implementation and operation of the policy, controls, processes and procedures of the ISMS.

**Check (monitor and review the ISMS)** - Evaluation of the applicable performance measurement processes dependencies of security policies, objectives and practical experience and report results for a management review.

**Action (maintain and improve the ISMS)** - Take corrective and preventive actions based on internal ISMS audit results and management review results or other relevant information, to achieve continual improvement of the ISMS.
Deploying / implementing an information security management system and its controls, based on the results of the risk assessment should be optimized. The first priority for the organization is the optimization and strategic development of the organizational structure. Thus security functions need to be clearly visible as separate units interconnected with the senior management.

Clearly defined hierarchy and the main objectives are allocated to sub-tasks and teams. This teams are responsible for the the management of information security and the information security integration through established information security organizational policies.

Each policy regulates the obligations and responsibilities of officials. Despite the established control over compliance with policies work exclusively on the consciousness of each employee.
Planning activities associated with the provision of business continuity, minimize business damage and maximize return on investment. These include short and long term plans to improve the information security management system.

Of course an additional important part is the planning of responsibilities. For this purpose, the organization creates an information security forum reporting to the senior management team. The forum is responsible for the management and improvement of the information security management system. Each unit has its own information security officer who is specially trained in compliance with all information security requirements in accordance with the specific activity of the structural unit.
CONCLUSIONS

Officials are responsible for the compliance to the information security requirements of the organization in the organization.

Security requirements and responsibilities are embedded into the employee job descriptions.

Every employee is directly responsible for security compliance, during a registered noncompliance administrative actions should be taken.

The organization must have written procedures that are part of the documentary Information Security Management System and regulate the management of documents and records, ensuring traceability and customer data security.

Processes and resources - key processes related to the customer environments.