Vadyba
Journal of Management
2016, № 1 (28)
ISSN 1648-7974

RISK MANAGEMENT IN INFORMATION SECURITY

Peter Lošonczi, Pavel Nečas, Norbert Naď
University of Security Management in Košice, Slovakia

Annotation
This papers deal with basics operational procedures of information security risk management. It briefly describes recommendations for managing the information security in order to minimize the risk occurrences in companies as well as in individuals. The individuals can also protect his/her data applying the basic principles of the standardized procedures of the information security risks management.
KEYWORDS: social engineering; risk analysis; audit; security policy.

Introduction

Identification of security risks lies in a detection of probable, unwanted, negative incidents and phenomena occurring in various forms in security environment, which can lead to sensitive information leakage (NBÚ, 2014).

It is necessary that the identification is process-oriented and divided into areas of potential threats. The aim is to have a summary of all the major areas that could be affected, to process the information about an internal and external security environment and to find the reason which motivates an intruder to acquire sensitive information. It also represents a marking of a loss and damage possibility or accomplishment of another result as was originally expected.

For example, a company A sends an email to a client with a price offer on the project, but a company B manages to get the e-mail and sends a better offer or another bargain to the very same client.

Besides assessment and perception of the risks it is important to monitor these risks for the identification, such as data leakage, hard disk crashes, filtering of outgoing sensitive information (personal identification numbers, classified information) of corporate mails etc. The risk assessment is closely related to risk management.

Risks analysis

Risk analysis in the IS is the basis for development of a more efficient method of the IS protection. The aim of the risk analysis is to properly identify and assess the threats which the information system is exposed to in order to select adequate measures. The risk analysis identifies the threats and risks that can still be accepted or corrected and analyses a status of the information security system in details (Šimák, 2006).

When identifying the risks, it is appropriate to focus on the problems and threats that can disrupt the availability, integrity and confidentiality of the data.

If there is a possibility of a risk in terms of an unauthorized manipulation with personal data, we have to observe possible weaknesses, for example changes in programs caused by so called malwares - software used to disrupt computer operations.

If we want to identify the risks of the unauthorized manipulation with the personal data, we must at least identify and monitor the present state of security and check whether:

- Virus protection is installed and updated;
- Network is properly connected and configured;
- Content is shared with only specific intended users;
- Sensitive data are stored on a computer that is connected to the Internet;
- There are data transmitted from removable media to your computer or vice versa;
- Router has activated the firewall, it is turned on and also protected against DOS attacks;
- Default passwords are not used for information equipment;
- In the case of a separate firewall it is set to the correct configuration, and rules;
- The operating system is outdated, without the support of the manufacturer, such as Windows XP;
- Operating system is regularly updated;
- Risk applications, such as Adobe Flash Player, Adobe Reader and Java are regularly updated.

The identification of the unauthorized, local access to sensitive data in the IS – we have to observe the threats by means of monitoring the assets of the system with the following programs Dude, Zabbix, Splunk, Nagios, Elastic Search and so on, so that there will not be any integrity, confidentiality, availability, performance and utilization breaches.

Potential weaknesses: an unauthorized person manages to gain an unauthorized access to the data due to using unauthorized hardware or software or moving away from the computer allowing an unauthorized person to read the data from the screen.

Minimizing risk includes:

- Checking the computer for ensuring antivirus and anti-malware protection;
- Controlling the portable media;
- Secure your computer from unauthorized persons. (Strnad, 2010)

In the context of information system security the risk analysis includes:

- Assets´ modules analysis;
- Threats analysis;
- Protection measures´ vulnerability analysis.

The risk analysis should be carried out repeatedly and after every change in the assets or at least within a year since the last risk analysis.

The risk analysis is a subjective assessment and also it does not mean that after not detecting any threat, there are no such threats at all.

The risk analysis is closely related to the process known as the risk management. This process includes the identification, selection, implementation and monitoring of protective measures in the information system.

Protective measures reduce:

- Probability of a security incident;
- Vulnerability of the information system;
- Consequences of the security incident.

Protective measures increase:

- Detecting the security incident;
- Faster recovery the whole system to its original state after the security incident. (Loveček, 2007)

Risk management

Risk management is focused on analysing and decreasing the risks using various methods and techniques of prevention, which eliminate existing problems or estimate future risks.

The risk management is a constant, repeating collection of interlinked activities, whose aim is to control the potential risks or to limit a probability of risks and decrease their influence and in the same time prevent the negative problems or incidents.

If it is possible to assess the risks based on the quantitative or various analytical methods we must control this risks and provide monitoring of these risks. The risk management gives us an opportunity to choose what measure to adopt in crisis which can be developed due to a failure of a technical or human factor.

Information system audit

An information system audit can be seen as a professional and independent assessment of this conception, a solution and a routine operation of the information system or one of its parts (for example, audit of an user's connection to the Internet and its use), in terms of its ability to meet security requirements.

The information security has not developed together with development of the first computers. Initially, there were very few computers and they required special knowledge to work with and were therefore limited to a small group of specialists.

The information security, if it ever existed, was rather seen as the physical protection of the entire computer systems. This perception of safety did not vanished with the development of computers and gradual processing of huge amounts of data, for example the first computers were normally operated in designated areas with controlled access.

For the actual protection of date we must ensure that:

- Only authorized persons have access to them;
- The data to be processed is not falsified;
- We can find out who has created, changed or deleted the data;
- The data has not been released in an uncontrolled manner;
- The data is available when needed.

Security policy

A content of security policy is defined by some organizations such as the International Organization SANS (SysAdmin Audit Networking and Security), which proposes specific security policy on its website http://www.sans.org/resources/policies/ for each individual issue separately in the following categories:

- General security policy;
- Network security;
- Security server;
- Application security. (SANS, 2014)

A summary of security rules and regulations define the way how to secure organizations in terms of physical protection through privacy protection to human rights protection. In general it defines a secure usage of the information systems in the organizations (Hudec, 2014).

The security policy and the security management can be applied after the risks are analyzed, that means that the threats and likelihood of their occurrence are defined. According to STN ISO 27000 risk can be seen as a function of factors, assets, threats, vulnerability and protective measures (safeguard). Implementation and managing according to STN ISO 27000 is based on the PDCA cycle - Deming Cycle, which says: plan, act, scan and update.

The risk analysis and risk management belong to the competencies of strategic management which chooses what kind of approach to use. Information security is strategically controled because a different method of the risk management varies in expanses. This level of management includes BCM, financial management, project management and organizational standards.

The following table shows the possible implementation of individual security tactics, according to a security policy with regard to the job position.

Table 1. Implementation of individual security tactics, according to the security policy

Job Position	Tasks
Management	Provide training for the heads of departments. Track the number of working hours on the basis of employee ID card. Monitoring time of entry / exit of the employees from / to the building. Divide workers by the corporate hierarchy. ...
Security division	Change passwords at least once a month. Secure access to all corporate systems. Monitor the entrance to the building. Secure protected area against fire. ...
IT	Monitor unauthorized access. Record unauthorized access. Prevent the data loss. ...
Security guards	Secure entrance to the building. Patroling the premises. ...

Security project

Security project is a process of planning and controlling large-scale operations. It is not only about the result - project documentation, but also about a creative process. There are number of definitions of "project", which can in some way be summarized in the following definition: The project is a plan for certain changes within a specific period of time in a specific object. This definition implies the intention, which has the following attributes:

- To monitor a predetermined target;
- To define the strategy, which makes possible to achieve the predetermined goal;
- To determine the necessary resources and costs, including expected revenue;
- To set the beginning and the end.

It should be noted that each project is unique, and this uniqueness lies in the monitoring of the objectives in the specific conditions and environment in which the project is conducted. Security guidelines should include:

- General and binding conclusions of the document;
- Technical - operational defense (scale of responsibilities and jurisdiction);
- Based on the circumstances, the links should be created between another security documents, not only in the field of information security (such as work and organizational rules);
- Individual security policies or methodologies such as:
  - The policy of data backup and archiving;
  - The policy of making and allocation of passwords;
  - The policy of protection against unauthorized access to the IS;
  - The policy of access to the IS as an individual;
  - The policy of protection against malware;
  - The methodology for disposal of redundant data;
  - The methodology for reporting of suspicious events and security incidents (Doseděl, 2004).

Conclusion

Finally, it should be noted that victims of social engineering do not have to necessarily be big companies, but also an ordinary man. The development of information technologies is very dynamic and constantly evolving field and therefore we should adopt efficient measures to minimize our chances of becoming the victim.

References

DOSEDĚL, T. 2004. *Počítačová bezpečnost a ochrana dat*, Brno: Computer Press, 2004,190s. ISBN 80-251-0106-1

HUDEC, L. 2014, *Základy počítačovej bezpečnosti, aktíva, hrozby, zraniteľnosti a riziká* [online]. 2015. [cit. 2015-01-14]. Dostupné na internete: <http://www2.fiit.stuba.sk/~lhudec/CS/1_prednaska.ppt

GREGA, M., BUČKA, P.: Blended simulation - not only as an effective military training commanders and staffs in ICM operations. In: *Výstavba, rozvoj a použití AČR* 2012. - Brno: Univerzita obrany, 2012. - ISBN 978-80-7231-909-1. S. 1-11.

IVANČÍK, R.: Kybernetická bezpečnosť – neoddeliteľná súčasť národnej a medzinárodnej bezpečnosti. In *Národná a medzinárodná bezpečnosť 2012 : zborník príspevkov z medzinárodnej vedeckej konferencie.* Liptovský Mikuláš : Akadémia ozbrojených síl generála M. R. Štefánika. 2012. s. 173-182. ISBN 978-80-8040-450-5.

IVANČÍK, R., KAZANSKÝ, R.: Kybernetická bezpečnosť. In *Bezpečnostné fórum 2015, zborník vedeckých prác z 8. medzinárodnej vedeckej konferencie.* Banská Bystrica : Vydavateľstvo Univerzity Mateja Bela – Belianum, s. 78-85. ISBN 978-80-557-0849-2.

LOVEČEK, T. 2007, *Bezpečnosť informačných systémov*, Žilina, Žilinská univerzita, 2007, 246s, ISBN 80-807-0767-5.

NBÚ, 2014 [online]. 2014. [cit. 2014-12-14]. Dostupné na internete: <http://www.nbusr.sk/ipublisher/files/nbusr.sk/oblasti-bezpecnosti/objektova-a-fyzicka/>

SANS INSTITUTE. 2014, [online]. [cit. 2014-12-16] dostupné online <http://www.securingthehuman.org/info/170182>

STRNÁD, O. 2010. *Riadenie rizík informačnej bezpečnosti*. Ostrava: AMOS 2010. ISBN: 978-80-904523-9-8

ŠIMÁK, L. 2006. *Manažement rizík* : Žilina, FŠI ŽU, 2006, [online]. [cit. 2014-12-14] dostupné online http://fsi.uniza.sk/kkm/files/publikacie/mn_rizik.pdf

TICHÝ, M. 2006. *Ovládání rizika, analýza a manažment*. Praha: C. H. Beck, 2006. ISBN 80- 7179-415-5

RISK MANAGEMENT IN INFORMATION SECURITY

Summary

Risk analysis in IS (information systems) is a key component for creating a more effective system for the information system protection. When identifying the risks it is important to focus on the impacts and threats, which can invade the availability, integrity and credibility of the information. If there is a possibility of a threat in terms of an unauthorized modification of personal data, we have to observe possible

weaknesses, for example changes in programmes caused for example by so called malwares

Risk management is a field of management focused on the analysis and decreasing the risks by means of various methods and techniques of the risk prevention, which eliminate the current or estimate the future factors increasing the risks.

The IS audit can be seen as a specialized and independent assessment of a concept, solution plan and a routine operation of the information system itself or one of its part (e.g.: audit of the users´ internet connection and its utilization), in terms of its ability to fulfil the security requirement

Summary of security policies defines the way which protects an organization starting with persons protection through privacy protection up to civil rights protection. It defines in general a secure use of the information system within the organization. The security management and security policy can be applied only after the risk analysis has been carried out, in other words an identification of threats and the probability of their occurrence has been successfully done. Safety project is a process of planning and managing the large scale operations. Creative process is as important as the final result – project documentation.

KEYWORDS: social engineering, risk analysis, audit, security policy

RECEIVED: 27 January 2016 **ACCEPTED: 20 April 2016**

Peter Lošonczi In the year 2000 he finished the master of engineering study programme at the Faculty of Mechanical Engineering in Kosice. In the year 2006 he finished Ph.D. study at the University of Žilina, the Faculty of Special Engineering in the study programme Security Management in the field of study Security of Persons and Property. He is an author and co-author of textbooks, scientific papers and participated in solving the security projects in the field of personal data protection. He is a certified manager and information security management auditor according to ISO 27000. Since 2008 he has been a Vice-Rector for Informatics and Development at the USM in Kosice.

Pavel Nečas, Colonel (GS. Ret.) was born on August 26, 1960 in Brno. Having achieved numerous assignments at the Slovak Air Force training and education establishments and in research and development branches during his fruitful career, he holds a Master Degree in Command, Control, Communication and Information Systems, a Doctorate Degree in Operational and Tactical Deployment of the Air Forces and Air Defence and a Professor Degree in National and International Defence and Security Policy. He is an author and co-author of many monographs, books, papers and articles published worldwide. At present, professor Nečas acts as the Vice Rector for Science, Research and Foreign Affairs at the University of Security Management in Kosice, Slovakia.

Norbert Naď In 2015 he finished the master of engineering study programme at the University of Security Management in Košice. He is a professional Army officer - specialist on information security technologies. He works as a lecturer at the University of Security Management in Kosice, The Institute of Civil Security, Department of cyber security.