Journal of KONBiN 2,3 (14,15) 2010
ISSN 1895-8281

USE OF THE UTILITY TREE TECHNIQUE IN PROCESS OF TREATS ANALYSIS FOR INFORMATION SECURITY IN INFORMATION AND COMMUNICATION SYSTEMS

WYKORZYSTANIE TECHNIKI DRZEWA UŻYTECZNOŚCI W PROCESIE ANALIZY ZAGROŻEŃ DLA BEZPIECZEŃSTWA INFORMACJI W SYSTEMACH TELEINFORMATYCZNYCH

Ireneusz J. Jóźwiak[1], Artur Szleszyński[2]

(1) Institute of Informatics, Faculty of Computer Science and Management,
Wrocław University of Technology,
Wybrzeże Wyspiańskiego 27 Str., 50-370 Wrocław, Poland.
(2) Chair of Systems Engineering, Department of Management,
The general Tadeusz Kościuszko Land Forces Military Academy,
Czajkowskiego 109 Str., 51-150 Wrocław, Poland.
E-mails: (1) ireneusz.jozwiak@pwr.wroc.pl (2)artur_szle@gazeta.pl

Summary: *This paper describes a technique of utility tree, which can be used in process of risk analysis for information security in information and communication systems. The technique uses connections between vulnerabilities of a system's element, a frequency of an event incidence (which exploits the vulnerability) and its the importance of such events for information security. It also describes and evaluates the influence of an event on information and communication system. The technique uses a qualitative risks assessment, which makes it simple in use.*

Key words*: risk analysis, information security, utility tree, information and communication system.*

Streszczenie: *W artykule opisano wykorzystanie techniki drzewa użyteczności w procesie analizy ryzyka dla bezpieczeństwa informacji w systemach teleinformatycznych. Technika wykorzystuje powiązanie występujące pomiędzy podatnością występującą w elemencie systemu, częstością występowania zdarzeń wykorzystującą daną podatność oraz istotnością takiego zdarzenia dla bezpieczeństwa informacji oraz funkcjonowania systemu teleinformatycznego. Technika wykorzystuje jakościową ocenę zagrożeń, dzięki czemu jest ona prosta w stosowaniu.*

Słowa kluczowe: *analiza ryzyka, bezpieczeństwo informacji, drzewo użyteczności, system teleinformatyczny*

Introduction

Threats analysis, also called as risk analysis, is a key part of developing an information security management system (ISMS) inside a company or institution (ISO/IEC-1779:2005, Białas A., 2006, Liderman K., 2006). An international standard ISO/IEC 17799:2005, asserts that information is one of crucial assets, possessed by company or institution. It has a huge influence on their continuity of work (ISO/IEC-17799:2005). The aim of to conduct risk analysis is the identification of the important asset importance and its threats plus vulnerabilities, which could be exploited by an unauthorised person. Information[1] has a value, often represented as a certain amount of money, therefore it must be protected. The main problem related to the information assets protection is a lack of their material form. It is a result of a definition of word 'information' (also called the message) which means, that information is an abstract object, which carries some context and it aim is to inform, to estimate or to take actions by its recipient. Because information is an abstract object, it is difficult to detect whether is has been stolen or damaged. A next obstacle in information security is the number of potential sources of information. According to literature of domain source of information are: speech, television, fax, personal computer, picture or written text (Hayakin S., 2004, ISO/IEC-1779:2005).

The necessity of information protection, which are gathered and processed by company's or institution's information system, has it source in law legislation. Therefore this issue should not to be ignored or omitted (Dz.U. nr 11, 1999, Dz.U. nr 133, 1997). The surveys conducted by companies, specialised in threats management, shows that the level of information protection is different for each company (Symantec 2009). The low level of information protection is compromise between law requirements and business needs of company or institution (Białas A., 2006). The information security management system can not protect all the informative resources used by company's or institution's information system. Therefore the risk analysis should point at the sensitive[2] informative assets of system (Liderman K., 2008, Białas A., 2006). Most of information, used by companies or institutions, are processed by specialized computer systems we will focus on the evaluation of threats for information security.

[1] A word information (Latin: informatio) means an idea or a clarification.

[2] The sensitiveness of the resource can be defined as predicted losses which can occur as a result of resource damage or loss.

1. Problem's identification

Two kinds of methods are in use concerning the threats assessment: the quantitative and the qualitative. A first group of methods is regarded as accurate, mostly because numerical values such as: probability of a threat appears or predicted amount of losses. The main disadvantage of these group of methods are the necessity to posses the data related to the frequency of the vulnerabilities for every element and the obligation to evaluate an amount of losses in case of an incident related to vulnerability occurs. A second group methods are quantities methods, they are easy in application because they do not need the numerical values to evaluation of risks. The disadvantage of this group of methods is a subjective character in estimation such parameters as: probability of event, exploiting the vulnerability, occur and potential losses of system's element.
There are many methods of risk analysis, which need a different skill from it users, some of them involve long and complicated calculations and the use of a specific vocabulary such as HAZOP method (Białas A., 2006). The use of it is difficult and inconvenient because of the need of an expert knowledge from a person who is involved in this process. They also required a database with information concerning the vulnerabilities and it influence for proper operation of system's element. The aim of this paper is to present the easiest and effective method of risk analysis for system's elements. That method is called the utility tree technique.

2. Solution proposal

The aim of the utility tree technique is a threat analysis concerning information security related to information security attributes. The utility of method should be understood as an ability of it to: threat identification, evaluation of it importance and compensation of it. All of these activities may to keep the system's business operation continuity. To fulfil specified tasks, when is executed a risk analysis, there should be identified a relation between system's elements. Then the vulnerabilities should be found, for those elements, and at the end there ought to consider an influence each of vulnerability on proper system's operation. The basis for evaluation of message security are following information security attributes (IEC/ISO-17799:2005, ISO/IEC-15408:1):

- confidentiality,
- integrity,
- availability.

The utility tree technique uses a qualitative evaluation of probability of threats and their importance. At first this technique was used in risk assessment during the process development of software systems (Liderman K., 2006). Method uses a directed graph, which root is described information security, the branches of its represents the information security attributes. The probability of event and it importance are used by the method to assess a measure of level of threat for system. The qualitative yardsticks both of these parameters are shown in table 1 and table 2.

Table 1. Qualitative measure of probability of event exploiting the vulnerability

No	Probability of occur	Description
1.	L – low	An event occurs rarely – probability less than 0.1.
2.	M – medium	An event occurs more frequently than in the first case – probability between 0.11 and 0.6.
3.	H – high	An event occurs repeatedly – probability is higher than 0.6.

Table 2. Qualitative measure of event's importance

No	Importance	Description
1.	L - low	Low importance means that losses can be accepted. The event has not negative consequences for a system operation
2.	M – medium	The cost of losses is higher than it is in first case but it is less than 0.5 (half) value of an asset.
3.	H – high	The cost of losses is high. At the worst system could be completely damaged

The measure of level of danger to the system's operation, from the vulnerabilities, is basis on the Cartesian product. The Cartesian product, which is formed during the process of the risk analysis, is connected with information security attributes. It is presented in formula (1).

$$E \times F \times I = \{(e,f,i) : (e \in E) \wedge (f \in F) \wedge (i \in I)\} \tag{1}$$

where:

E – the set of system's elements,

F – the set of event's probability of occur, which exploit the vulnerability of system's element {L,M,H},

I – the set event's of importance values {L,M,H}

In order to assess the level of threats that should be reduced by safeguard, there ought to be chosen those of elements, where to parameter importance, for an event, was assigned the value H. That algorithm of selection, the events with big influence on information security, is a result of potential big amount of losses which could occur after exploiting of the vulnerability by an attacker. Planning a safeguard we should not to ignore the events with assigned L value to the probability of it occur. The explanation for this situation is that events such as: fires, floods, thefts , etc. rarely appear – circa 6% a total numbers of incidents in information security - but it importance for system is high. The losses generated by all mentioned earlier events can be huge (Liderman K., 2008). In the worst case the whole system could be damaged. The damages into the system could be so serious that it would be impossible to restore of its previous state. It is unacceptable situation, according to recommendations on keeping information security in ICT systems, which are described in international standards (ISO/IEC-17799:2005, ISO/IEC 13335:1). There should not to be neglected events, of which parameters of occurs probability are set on H and its importance are set on L. These kinds of events are approximately 75% a total number of security incidents into the system (Liderman K., 2008). There are consequent: misuse of an user's account name or access password to it, not follow a password policy or misuse of installed software, etc. All mentioned incidents can be a result of misunderstanding the rules of proper system use by it users. There is a possibility these events could be the probes of recognise a system's safeguards by potential intruder. They want to know what time is needed to discover these kinds of activities by system's administrator. In order to reduce the number of the incidents, company's information security management staff should to prepare a document called "company's information security policy". Next thing should be the all personnel training in proper use of the technological components of the system.

2.1. An example of use the utility tree technique to identification of threats for information security, in model of information and telecommunication system for electronic trade support

Into a model of ICT system, which supports an electronic trade, there could be specified elements such as:

Computer equipment:

- company's web site server,
- accounting and financial server,

- delivery, customer relationship management and stock management server,
- company's employees workstations

Network infrastructure devices:

- routers (gateways),
- switches,
- access points,
- removable storage devices,
- printers,
- scanners, digital cameras.

Software:

- content management system responsible for present an electronic shop offer,
- web site server,
- customers orders and relationship management software,
- accounting and financial software,
- stock and distribution management software,
- operating systems of company's servers computers and employees workstations.

Users:

- company ICT system administrators,
- company's accountants,
- company's marketing department employees,
- company's order and delivery service department employees.

In presented model can be specified following business processes:

- server computers, which store data, are exchanging them between one another, to fulfil business tasks,
- data exchange is fulfilled after positive verification of subject[3] identity and checked on its permission to an object,
- when clients benefits from an electronic shop offer there is required to full in a form with data necessary to deliver ordered by client goods,

[3] The term subject is understood as person or software process, which has granted permission to an asset such as catalogue, file or device. The asset, which has a value for its owner, is called as an object.

- subsystem which process client's order picks up data from Customer Relationship Management system; afterwards it grants the client a discount,
- transaction realized with internet viewer software, is executed with SSL (Secure Socket Layer) service. It required accepting, an e-shop certificate, by client's internet viewing program,
- the clients can get a login and a password to the company's electronic shop, what enables them a personalisation of company's according to their needs.

Only the components located inside the company, will be subjected at the risk analysis. The constraint is a result of an assumption that only these components of ICT system can be checked and set up by company's IT (information technology) staff. All these actions should to provide for accepted level of risk called also a residual risk. The problem is with security of information in e-shop clients' devices. The company's IT staff has no influence on clients' side computers security. The only thing which they can do are the recommendations how the customers can make their computers more secure.

During the risk analysis process discovered, in the model of company's web site server, the vulnerabilities which are shown at the figure below (fig. 1). The approximate values of probability the event occurrence and its importance, are shown in the brackets.

It is recommended to start the reduction, of identified threats, form these which affect the attribute of availability of service. The example data, presented on the figure 1, show that incidents such as deny of service were occurred. Similar situation occurred in case of intentional change of company position in searching web sites. The incidents were a source of serious financial losses for company. The reason for this was not serviced customers orders, what was result of deny of service the company's web site server. The main goal of existence the model system is supporting of electronic commerce, to fulfil that task is used a medium such as the wide area computer network. A lack of access to company's web service could not be accepted (Michalski A., 2008). The safeguard should to reduce or eliminate a total number of occurrences of described incidents to acceptable level.

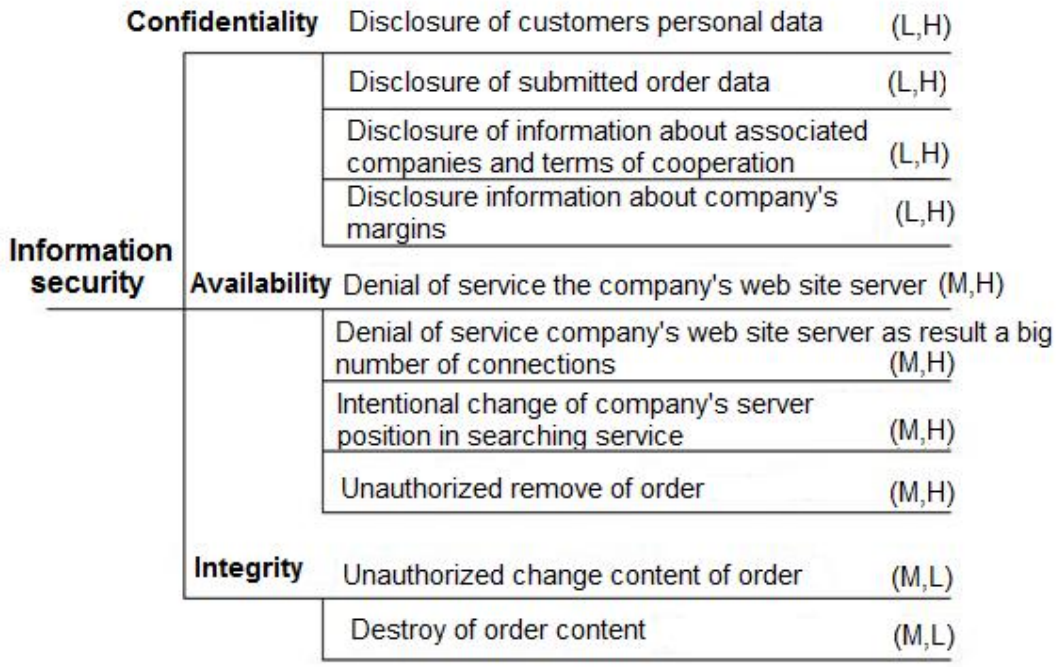

Fig. 1 The example of an utility tree for an element of the system, which supports electronic trade (source: authors own)

It is recommended to monitor the system operation for check effects of earlier works. It is recommended to measure of security level by conduction of penetrative tests. They should to uncover wholes into implemented safeguards. The measure is crucial for evaluation a level of information confidentiality, what is important in case of protection of client's personal data. The keeping client's personal data in secrecy is a law regulation which may have an influence on company's good reputation (Dz.U. nr 133, 1997). Another area of responsibility are the incidents related to the attribute of information integrity. Data sent via telecommunication network can be intentionally or unintentionally change. This situation may to suggest that we can observe a beginning of an attack, which aim is to check how the system deal with that kind of incident is handled by the system.

Low frequency of appearance such events is probably caused by misjudgement of the system's safeguard, by potential attacker. a safeguards implemented inside the system. The aim of a potential attacker is to recognise the data exchanged protocol between electronic shop and customer. Understanding of flow chart of exchanged data and its protection

mechanism, by an intruder, can be a reason of system discredit. That thing can be a cause of big financial and nonfinancial losses.
Activities mentioned above may contribute to the process of specifying the security requirements in data processing systems. The requirements contain a detailed description what should to do for rise or keep the information security. They also be useful to verify the reached results of implemented changes. The aim of such activities is maintain and improve the level of information security for company ICT system.

3. Conclusions

The method presented in this paper allows on easy evaluation the threats importance for company's or institution's ICT system's components. The aim of method is a simplicity of it use for the risk analysis. This factor is important for those who are not very experienced in risk analysis, the using a qualitative measure is easier for them. The main disadvantage of this method is the tendency to skirt round of some important threats for information security. The only one way to reduce described threat is carry on risk analysis as a repeated activity non as one time thing. This solution is recommended by international standards (ISO/IEC-17799:2005 ,ISO/IEC-13335:1).
Presented at table 1 and table 2, quantification criteria for probability of hazard occur and its importance can be modified on the basis of data from system's events logs.
The method, despite its imperfections, enables the recognitions of the risks, which may occur in the system. This knowledge can be use to prepare the safeguards, which can to reduce losses and can keep business continuity. The advantage of method is its simplicity. The method does not need any heavy calculation or complicated tables with description of the threats probability and its importance.

References

1. Białas A.: *Bezpieczeństwo informacji i usług we współczesnej firmie i instytucji*, WNT, Warszawa 2006.
2. Hayakin S.: *Systemy telekomunikacyjne t.1*, Wydawnictwa Komunikacji i Łączności, Warszawa 2004.
3. *International Standard ISO/IEC TR 13335-1 Information technology – guidelines for management of IT security – Part 1: Concept and models for IT security* - International Standard Organization, Geneva 1996.

4. *International Standard ISO/IEC 15408-1- Information Technology. Security techniques – Evaluation criteria for IT security. Part I. Introduction and general model*, Second edition , International Standard Organization, Geneva 2005.
5. *Polska Norma PN-ISO/IEC 17799:2007 Technika Informatyczna. Techniki bezpieczeństwa. Praktyczne zasady zarządzania bezpieczeństwem informacji*, PKN, Warszawa 2007.
6. Liderman K.: *Analiza ryzyka i ochrona informacji w systemach komputerowych*, PWN, Warszawa 2008.
7. Liderman K.: *Wykorzystanie drzewa zagrożeń w analizie ryzyka*, [w:] Bezpieczeństwo teleinformatyczne. Aspekty techniczne i prawne, red. K. Liderman, Wojskowa Akademia Techniczna, Warszawa 2006.
8. *Small and Midsized Businesses Aware of Security Risks, But Not Doing All They Can to Protect Information. While SMBs understand security risks, a high percentage have failed to enact basic safeguards* [on-line access] http://www.symantec.com/about/news/release/article.jsp?prid=20090409_01
9. *Ustawa o ochronie informacji niejawnych*, Dz.U.1999 nr 11 poz. 95 nr z dn. 22 stycznia 1999 r. z póź. Zmianami
10. *Ustawa o ochronie danych osobowych*, Dz. U. 1997 nr 133 poz. 833 z dn. 29 sierpnia 1997 r. Z póź. zmianami