Portál pre odborné publikovanie ISSN 1338-0087

Quantitative and Qualitative Assessment Tools for Information Systems Security

Pavlík Lukáš · Informačné technológie

11.05.2016

The article discusses the issue of the Security of Information Systems in organizations (further only SIS). The first part of the paper provides an analysis of several analytical tools that are most frequently used in the evaluation of Information Systems Security (further only ISS). These instruments are then analyzed and their principles are described. In conclusion a comparison is the of advantages and disadvantages of each tool, with the emphasis on their use and application possibilities.

Introduction

The issue of security is a very important branch in today's society. In most organizations, information systems represent an important area that has a direct impact on management processes within them. For this reason, the information managed by the information system organization and high value, and safety is therefore the subject of current interest of the private and the public spheres. Safety must be viewed as a whole consist of partial sub-areas, that solve various problems. An Information system consists of several levels, in which the safety and risk areas must be addressed.

The analysis and evaluation of the SIS use several major analytical tools, for instance CRAMM, Octave or Mehari. Each of these instruments is based on a different principle and its application is thus limited to a certain type. There are also other methods in addition to those well-established analytical tools, and which can also benefit from their being combine to contribute to more effective solve resolution of a particular problem. Mathematical and statistical methods can be used as possible alternatives in particular, methods of a quantitative nature are used to analyze a given system, and the results can be interpreted by a numerical expression. [12]

In this article the focus is on the analysis and comparison of analytical tools and methods of analytical tools and methods. These are analyzed in terms of their software design, construction and usage possibilities.

1. CRAMM

The CRAMM risk analysis software tool is one of the most frequently used tools. It based on gathering information about the being analysed system, performing

calculations and the quantifying the value of assets and devising subsequent countermeasures. The main advantages of such analytical instruments can be classified set countermeasures whose recommendations cover all aspects all safety aspects (ie. IT, communications, personnel etc.). Moreover, after the calculation of risk, those countermeasures which are best suited for the given area will be automatically selected. The disadvantages include the purchase price of the tool, which is used by an average of several hundred thousand trained users and costs tens of thousands of crowns. [8]

In the first phase an assessment is made using the CRAMM tools of the relative information, software and hardware components, as well as the estimated damage in the event of any disruption of assets. The second step is to assess the risks, including their identification as well as the determination of the probability of threats, vulnerabilities and risk calculations. The system is estimated using the CRAMM tool is depicted below (Fig. 1). “Clear Risk”, is regardless of the introduction of a system of checks. The final phase focuses on the design of measures against the risk of a comparison of the recommended and current measures. The algorithm expressing risks and a description of its individual parts, is expressed in Fig. 1

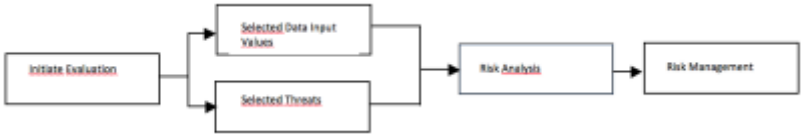

Fig. 1 algorithm in the risk analysis tool CRAMM [10]

1.1 Initiation ratings

The begin with, an assessment is made using meetings, interviews and structured questionnaires to obtain and collect the data. In the initial phase it is important to set goals, scope and boundaries of the research, and the time schedules as well as the identification of the respondents. [13,10]

1.2 Input data values

Determining the value of an asset is the main problem in identifying risks and security levels. There are three types of assets that constitute such information, data, application software, and physical assets. Valuation of the assets is consider sometimes speculative activity because it depends on who and where your own assets are. The CRAMM assessor conducts an interview with the owners of the data whose objective is to determine the true value of the data. This part of the assessment is more difficult because of the determination of the data and it owners. Evaluators can also request more detailed information for estimates that are important in the evaluation process. [13,10]

The Value Data is derived from the effects of a breach of confidentiality, integrity, availability and the generally accepted principles of Information Security. Interviewees describe scenarios worst-case impacts of the possible consequences in case of the unavailability of the data. This statement is available in several time-frames (eg. less than 15 minutes and more than 2 months). Furthermore, attention is focused on the destruction or modification of data. This approach, however, is deemed

insufficient, because the worst case scenario may not be very likely in the real world. [13,10]

1.3. Selected threats

In addition to determining the value of assets another key element the assessment is to determine the level of threats and vulnerabilities. Threats and vulnerabilities are analyzed in selected groups of assets that are inserted into timeframes. The CRAMM analysis tool has predefined panels, threat / group assets and combination of threat / impact. The assessment of any threat in each group would be too exhausting and so the assessor selects the appropriate threats and assets according to customer needs.[1]

There are two ways to assess vulnerabilities and threats either. It is a “full” or “fast” method of risk assessment. For a “full” way of risk assess, it usually recommended that threats and vulnerabilities are identified by means of questions and structured questionnaires. The data is then entered into the CRAMM tool, which performs a calculation of the risk. The expression levels of risk takes place on a five point scale (where1 is a negligible risk, and 5 indicates the highest degree of risk). [13,1]

A well prepared and experienced assessor may also use the “fast” risk assessment method. In this case, this means the level of threats and vulnerabilities embedded directly into the system with a rating guide. The results have a higher priority than when using the results from questionnaires. The quantitative approach, which is preferred in this process, may be the only option, because on the basis of accurate data from the statistics, one can predict the exact estimates. [13]

1.4 Risk analysis

The CRAMM analysis tool allows one to calculate the risk for each class of assets. The expression of the risk is expressed on a scale of 1 to 7 using a risk matrix. On this scale, 1 is defined as basic security and 7 represents high safety requirements. The system allows one to generate a report of the results that can then be passed on to the management of the organization. The findings of the report should be reviewed in light of its assets and their vulnerability. [13,9]

1.5 Risk management

Based on the results of the risk analysis process, countermeasures, which are necessary to reduce or eliminate risks are created. The recommended security measures should then be compared with existing countermeasures. The CRAMM analytical tool offers almost 4,000 countermeasures, which are sorted into groups and subgroups that have the same security aspect, e. g. like hardware, software, communications and the personnel environment. Any countermeasure is identified security levels, ranging from 1 (very poor) to 7 (very high). The security level is selected according to the degree of risk. [13,3]

2. Octave

Octave is an analytical tool whose goal is a comprehensive evaluation of information

risks. Octave allows the connection of key risk management departments and the support of an enterprise's business interests. This organizations needs to get the most relevant information regarding its business, operation, information technology department and the security department. Information Security Risks can only be controlled if there is a Strategic Risk Management plan in accordance with the business plans of the organization. The main benefit of the Octave methodology is its broad focus, because when the risk assessment is analyzed a large number of organizational units and their staff throughout the organization are identified, so one can get a comprehensive overview of the risks. The main drawback is the absence of a software tool that would an easier and quicker applicability. Instead Excel spreadsheets are used, but they can not replace the experience a quality presentation of results; and working with them is much slower. [8,2]

Octave is designed so that it can be adapted to the environment of the organization. This option can be seen as a major advantage of this method in most organizations that use this method, since it can therefore be adapted to their own environment. The individual phases of a system security assessment are shown in the diagram below.

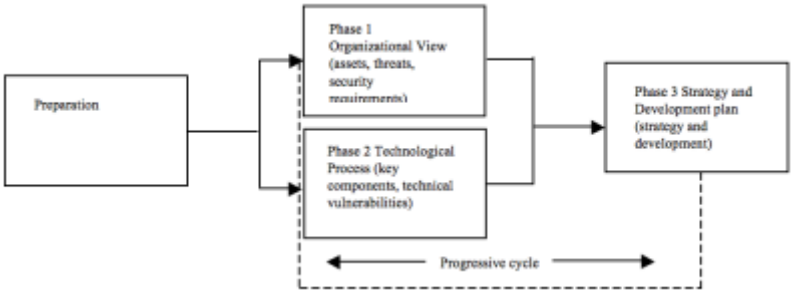

Fig. 2 The Octave Three Phase methodology

The Octave analysis tool performs an analysis and assessment of the information risks in three phases. In the first phase, the analytical team identifies important information relating to the assets and the current strategy for protecting these assets. The team then determines which of these assets is (most) important for the functioning of the organization. In the second phase the team of analysis evaluate the information structure and to supplement threat analysis, performed in the previous step. At this stage it is also necessary to notify the management concerned of potential impacts. In the third phase the team perform a risk identification analysis and prepares a plan for any reducing risks to critical assets. [14]

3. Mehari

The main aim of this tool is to provide the necessary support for staff in the organization's information security team. This support is implemented with the tools that are involved in the development of managerial activities and there by assisting in management goals. Mehari tries to offer tools that are able to support all of the assets, activities and processes that affect the security of an organization. Risk Management is realized through operational and managerial activities. One of the the advantages of this methodology may include a knowledge base that includes all of the safety procedures and their importance, and the corresponding risk. From this knowledge base, then the entire security framework of the organization. As the weaknesses climb, this indicates a certain incompleteness of information security solutions, as well

as in the Octave methodology, it thus lacks a quality software tool. [8]

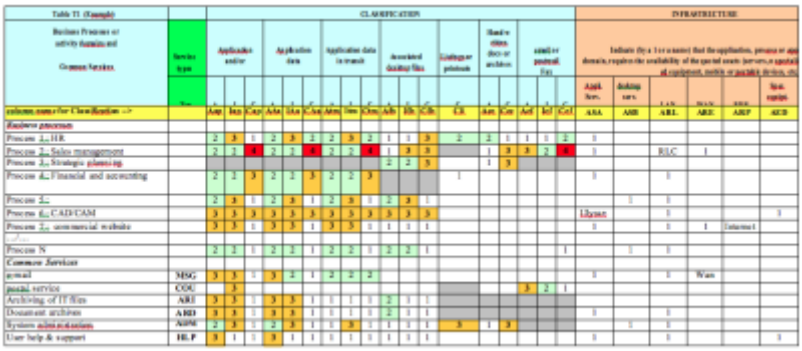

Fig. 3 Example of calculating risk in business processes using the Mehari's tool [11]

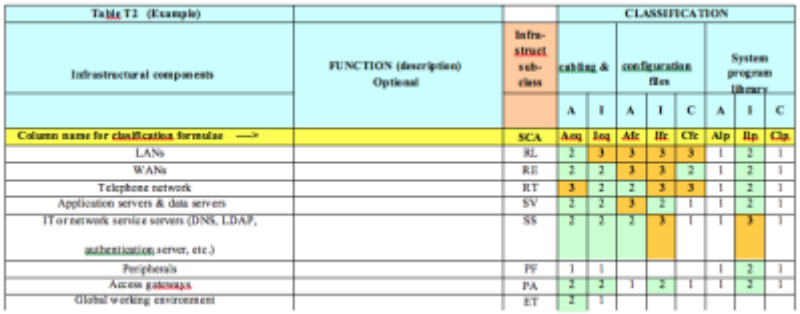

Table T2 (Example)			CLASSIFICATION								
Infrastructural components	FUNCTION (description) Optional	Infra-struct sub-class	cabling &		configuration files			System program library		
			A	I	A	I	C	A	I	C
Column name for classification formulae ---->		SCA	Acq	Icq	Afc	Ifc	Cfc	Alp	Ilp	Clp
LANs		RL	2	3	3	3	3	1	2	1
WANs		RE	2	2	3	3	2	1	2	1
Telephone network		RT	3	2	2	3	3	1	2	1
Application servers & data servers		SV	2	2	3	2	1	1	2	1
IT or network service servers (DNS, LDAP, authentication server, etc.)		SS	2	2	2	3	1	1	3	1
Peripherals		PF	1	1				1	2	1
Access gateways		PA	2	2	1	2	1	1	2	1
Global working environment		ET	2	1						

Fig. 4 Example of calculating risk for structural components in the Mehari IS tool [11]

The Mehari tool includes several modules that are used for the analysis and assessment of the security situation of the system. These modules are divided into the following areas:

- Risk Analysis,
- A safety evaluation,
- Analysis,
- Scale Disorders.

3.1 Risk analysis

Risk analysis is provided for as a "driving force" in each safety publication. However, in most cases it is not recommended, which risk analysis methods should be used. The Mehari provides an analytical tool that has long been a structured approach based on simple principles. [5] A risk situation can be characterized by the following factors:

- Structural or organizational factors that do not depend on security measures, but on the main activities of the organization, its environment and context,
- To reduce the risk factors that are a direct function of the implemented security measures.

Through risk analysis, one can determine maximum level of the severity of the consequences of risky situations. This is typically a structural factor, while the security assessment will be used to evaluate the risk reduction factors. The Mehari tool allows both a quantitative and a qualitative assessment of these factors and helps in assessing the level of risk and in achieving the desired results. At the same time, Mehari also integrates tools (e.g. assessment criteria and formulas) and knowledge-

base (particularly for diagnosing security measures), which is a complement to the ISO / IEC 27005 [15]

3.2 Safety evaluation

The Mehari tool also allows the integration of diagnostic questionnaires relating to the security controls, which enable a high-quality evaluation of the level mechanisms and the solutions aimed at reducing the risk. [15]

3.3 Analysis

Security is also all about protecting property. Regardless of how security policy is oriented, there is always one common principle upon which all managers agree. There must be a balance between investments in security and the company's assets. The aim of the assets safety analysis is to answer the following question: What could happen and if it happens, will it be serious? The Mehari modules also provides an analysis of assets which delivers results in the form of:

- Value scale defects,
- Classification of information and IT resources. [15]

3.4 Scale disorders

Identifying faults and potential risk events start with the company's activities and is aimed at identifying potential failures in production processes. This will result in:

- A description of possible types of errors,
- A definition of the parameters that affect the severity of individual failures,
- An assessment of the critical thresholds for those parameters that determine the severity of the disorder. [6]

The use of Mehari's analytical tools

The main focus of Mehari tolls is on risk assessment and reduction. The relevant knowledge base, mechanisms and tools are developed for this purpose. Corporate managers can use this tool as:

- A permanent working method and workgroup guide,
- A working method used in parallel with other security management practices,
- A working method, used only to supplement other work methods.

Given these facts, the Mehari tool contains a large number of methods and procedures that enable a risk analysis to be performied, if so needed. These are of course, the aforementioned knowledge base, manuals and guides that, describe the various modules. These modules (i. e. assets, risks, vulnerabilities) are designed for people who issue the decisions in the security of information systems. [15]

Discussion

Given the wide scope of the security issues field, the CRAMM, Mehari and Octave tools are some the various analytical tools used for establishing certain boundaries

that determine their possible applications. One of the most common tools is the CRAMM tool, although its cost is the highest of the three. This is mainly because it has quality software design, and a fairly wide range of functions. These features allow quick and easy decisions. The Mehari is the second most-widely used tool, although it is not as good as the CRAMM software support. However it includes several modules that facilitate a better grasp of the issues.

The overall risk analysis algorithm is more systematized. In the last-mentioned tool which is Octave. Octave is the least used because it lacks quality software design. Analysis and evaluation of risks only takes place in an Excel environment and thus decision-making outputs are not very well-prepared. It has therefore been concluded that the software performance of analysis tools is an important factor in determing their usefulness. Without high-quality computer performance, one can-not obtain outcomes that could be presented such that decision-making for analytical tools users is as easy and accurate as possible. [16,7]

Conclusion

The aim of this article was to show the possibilities of using selected quantitative and qualitative tools and methods that can be used to evaluate the security of information systems in an organization. In many cases, these methods can be used as an additional alternative for existing analytical instruments. This step can broaden the scope of an investigation that may yield better results. Given the importance of information systems and their safety, this issue is under constant development. We can thus predict a certain level of development in these tools and methods due to new threats that will appear in the future. It should therefore be a combination of these tools and methods, one of the ways to identify these new threats and to propose timely measures. These steps should be implemented due to the type and degree of threat for the information system.

Reference:

1. Online textbook – Decision analysis and alternative solutions [online]. [feeling. 06/10/2015]. Available from: http://ucebnice-eia.zf.mendelu.cz/rozhodovaci-analyzy
2. JAŠEK, Roman. Information and data security. Zlín: Tomas Bata University in Zlín, 2006, 140 pp. ISBN 80-7318-456-7.
3. JAŠEK, Roman and Martin LUKÁŠ. Informatics in Public Administration. Zlín: Tomas Bata University in Zlín, 2003, 215 pp. ISBN 80-7318-147-9.
4. raisin, Eva. General principles of work with portal Czech Point [online]. Brod Egon Center, 2013 [cit. 01/10/2015]. Available from: http://www.muhb.cz/czp-obecne-zaklady-pdf/s-829834
5. FIRE, Josef. Information security. Plzen: Publishing Ales Cenek, 2005. 309 pp. ISBN 80-8689-838-5.
6. SULEK, Martin. Organizational and regime measures: Silesian University [online]. [feeling. 06/10/2015]. Available from: http://www.slu.cz/math/cz/knihovna/ucebni-texty/Ochrana-osob-a-majetku/Organizacni-a-rezimove-opatreni-a-fyzicka-ochrana.pdf
7. White, George ŠMÍD, Frank King and Vladimir HLAVÁČ. Information Technology:

Database and Knowledge Systems. Prague: Czech Technical University, 2009, 126 pp. ISBN 80-01-02790-2.
8. KING, David. Brno University of Technology, Faculty of Business. Information security company: Doctoral thesis. Brno, 2010.
9. Doucek, Peter. Information security management. 2nd expanded edition. Prague: Professional Publishing, 2011. ISBN 978-80-7431-050-8.
10. Astakhov Alexander. Art Information Risk Management [online]. 2015 [feeling. 2015 11-25]. Available from: http://www.slideshare.net/sapient/sapient-nitro
11. ARTINIĆ, Ante and Marko ŠMALCELJ. Overview of methodologies for risk assessment. Zadar, 2010, p. 10
12. Lukáš, Ludek et al. Security Technologies, Systems and Management. Zlín: VeRBuM, 2011, 316 pp. ISBN 978-80-87500-05-7.
13. Yazar, Zeki. SANS Institute InfoSec Reading Room: A Qualitative Risk Analysis and Management Tool – CRAMM [online]. United Kingdom, 2002 [cit. 02/01/2016]. 15 p. Available from: https://www.sans.org/reading-room/whitepapers/auditing/qualitative-risk-analy-is-management-tool-cramm-83
14. CARALLI, Richard A., James F. STEVENS, Lisa R. Young and William R. WILSON. Improving the Information Security Risk Assessment Process [online]. Pittsburgh, Carnegie Mellon University, 2007, 154 pp. [Cit. 02/02/2016]. Available from: ftp://ftp.sei.cmu.edu/pub/documents/07.reports/07tr012.pdf
15. Louis Roule, Jean. Mehari Overview 2010 [online]. Paris, 2010, 18 pp. [Cit. 03/01/2016]. Available from: https://www.clusif.asso.fr/fr/production/ouvrages/pdf/MEHARI-2010-Overview.pdf
16. STEENBERGEN, R.D.J.M. Safety, Reliability and Risk Analysis: Beyond the Horizon. Great Britain, 2013. ISBN 1138001236th