Imed El FRAY, Tomasz KLASA
WEST POMERANIAN UNIVERSITY OF TECHNOLOGY, DEPARTMENT OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGY,
Żołnierska 49, Szczecin

Information Security Management System proposal

Ph.D. eng. Imed El FRAY

Graduated from the Department of Marine Technology, Szczecin University of Technology in 1993. In 1997 obtained Ph.D. in the field of Marine Technology (specialty: Automatics and machine steering). Main research interests: risk analysis, trusted systems. Employed as Associate Professor at the Faculty of Computer Science and Information Technology, West Pomeranian University of Technology, Szczecin.

e-mail: ielfray@wi.zut.edu.pl

Ph.D. student Tomasz KLASA

Ph.D. student at the Faculty of Computer Science and Information Technology of the West Pomeranian University of Technology, author and co-author of a number of articles and book chapters in the area of risk management and information security.

e-mail: tklasa@wi.zut.edu.pl

Abstract

Information security in organizational and corporate information systems is currently one of the most important business problems. Losing control over vulnerable information may lead to severe losses and, as a consequence, bankruptcy. For such reason utilization of efficient information security management system becomes more and more important. Growing speed of business limits the efficiency of traditional solutions in this area, based on manual audits. Automation of assessment as well as monitoring becomes necessary, followed by a method of efficient integration of those two processes, decreasing latencies in information security management process.

Keywords: identity verification, authentication, information security.

Propozycja systemu zarządzania bezpieczeństwem informacji

Streszczenie

Bezpieczeństwo informacji w systemach informacyjnych organizacji i przedsiębiorstw jest obecnie jednym z najważniejszych problemów biznesowych. Utrata kontroli nad informacjami wrażliwymi może doprowadzić do dotkliwych strat, a w konsekwencji do bankructwa firmy. Dlatego też coraz bardziej istotne jest posiadanie sprawnie funkcjonującego systemu zarządzania bezpieczeństwem informacji. Rosnące tempo prowadzenia biznesu ogranicza efektywność tradycyjnych rozwiązań w tym obszarze, opartych na manualnych analizach ryzyka i audytach bezpieczeństwa. Konieczna staje się automatyzacja zarówno procesu oceny stanu bezpieczeństwa organizacji, jak i procesu monitorowania bezpieczeństwa informacji, oraz opracowanie metody ich efektywnej integracji. Celem automatyzacji jest zmniejszenie opóźnień w procesie zarządzania bezpieczeństwem informacji. Artykuł przedstawia propozycję integracji tych dwóch obszarów (oceny i monitorowania) w jednym, wysoce zautomatyzowanym systemie zarządzania bezpieczeństwem informacji – odpowiedź na wzrastające tempo działań biznesowych, powodujące znaczne ograniczenie dostępnego czasu na reakcję.

Słowa kluczowe: systemy informacyjne, analiza ryzyka, monitorowanie ryzyka, bezpieczeństwo informacji.

1. Introduction

Information and processes, systems and networks supporting it are import ant business assets. Identification, reaching, keeping and improving information security may be necessary to keep competitive position on the market, financial stability, profitability and accordance with law and organization image requirements [1].

Many of information systems present on the market was designed without proper attention to some aspects of security. Security, that can be achieved with the help of technical means, is limited and, according to [1], it is advised to support it with proper directives and procedures. Determining which management mechanisms are advised to apply requires detailed and accurate planning.

Risk estimation, as the most important risk management process, relies on systematic approach to estimation of scale of risk (risk analysis) and process of comparing the estimated risk with risk importance evaluation criteria (risk evaluation). It has to be done on a regular basis, especially in case of significant change in state of assets, threats, vulnerabilities, etc.

Having in mind OECD directives [2] and standards of information systems security [1, 3], risk assessment must be done in a methodic way, allowing comparative and repetitive results. The authors made an attempt to verify results of risk assessment, based on a monitoring system, which imports results of analysis and risk assessment as one of input arguments.

2. Information security and risk management

ISO/IEC advisory no. 73 [4] defines risk assessment as a process that consists of risk analysis and risk evaluation. The risk analysis is a process of risk identification, description and measurement. Identification requires detailed knowledge about organization, market it operates on, and deep understanding of strategic and organizational goals of the organization, including key success factors as well as threats and opportunities bound with their execution. Description and measurement of risk according to [4] relies on analysis of probability and results of execution of individual risks, for which priorities can be defined. This means that some key risks can be chosen, which should be a subject to more detailed analysis and measure their grades in (according to widely known methods) quantitative form [5-8] or qualitative form [9-12]. The final result of risk analysis process is assignment of grade describing importance of each identified risks from the perspective of significance for individual domains of the organization activity and determination of priorities of action against them. Such actions can be described by pointing out basic mechanisms of control and areas where expenditures on risk control should be increased, decreased or reorganized. Such risk evaluation requires comparison of the estimated risk level with criteria chosen by the organization. Those criteria can apply to costs and benefits, law requirements, etc.

3. Information security assessment system

As it has already been described, quantitative and qualitative methods are used for risk assessment. Most of them is based on know-how solutions and studies done by independent or governmental organizations of various countries, dedicated to utilization in government and public systems. Those methods are compliant with ISO/IEC 270xx standard family in a smaller or bigger degree [1,13]. For the purpose of further research, the authors chose the quantitative method Mehari [8]. Such choice is a result of wide accessibility of the method on GNU license. Furthermore, this method is frequently updated to be compliant with standards and directives of most international institutions

dealing with information security and risk management in information systems.

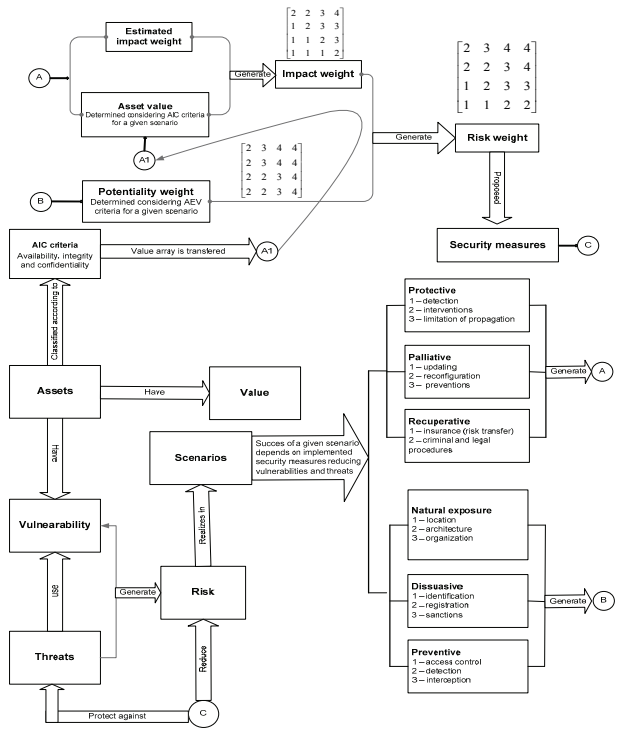

Fig. 1. Scheme of Mehari" risk analysis method [8]
Rys. 1. Schemat metody analizy ryzyka „Mehari" [8]

The MEHARI risk analysis method is based on the knowledge concerning identification and value assessment of assets, threats levels and vulnerabilities evaluation. Fig. 1 presents the scheme of the Mehari risk analysis method in which it can be seen that risk weight is determined from the risk aversion table. This table is created on the basis of two weights determined previously: potentiality and impact of threat for every risk scenario.

- potentiality weight – determined from a table with values of natural exposure and security measures (dissuasive, preventive) related to criteria AEV (accident , error, voluntary).
- impact weight – it is the function of assets values (resulting from classification) and results of actions reducing an impact of threats on assets (security measures for protection, palliative and recovery) related to each security criteria AIC (availability, integrity and confidentiality).

Tab. 1. Risk aversion table
Tab. 1. Tabela wyznaczania ryzyka

Impact				
4	2	3	4	4
3	2	3	3	4
2	1	2	2	3
1	1	1	1	2
	1	2	3	4
	Potentiality			

The risk aversion table (see Table 1) determines the way the final risk is evaluated and mutual relations between both factors: impacts and potentialities of threat. The contents of the table indicates vital risks (4 - they require the immediate implementation of countermeasures, ignoring an organization budget and security plans), very serious risks (3 - those risks have to be eliminated or minimized sooner or later, according to the established organization budget and security plans) or accepted (serious or insignificant) risks, depending on the values of impact and potentiality of threat.

The method for calculation of individual weights for each of scenarios according to Mehari and the way of dealing with critical risks (choosing proper counter measures) are described in detail in [8].

4. Information security monitoring system

Once information security is evaluated, countermeasures implemented and partial risk is known, it is time to control whether the life follows the identified scenarios, if any of the identified risks took place and how the organization dealt with them [14]. The most dangerous is situation when properly taken assessment becomes outdated unnoticed. Similarly, if the taken assumptions or chosen countermeasures turn out to be improper, a situation may easily get out of control. Manual monitoring of hundreds of scenarios and dozens of variables is possible, but extremely ineffective, making utilization of a dedicated automated monitoring system a preferred solution.

According to [15], two types of risk monitoring can be distinguished:

- active
- reactive (passive)

While in the reactive approach no additional effort is taken until a problem appears, in the active approach various data are collected to verify procedures used to minimize risk even if they seem to work fine. Although it is more expensive, it can offer much more accurate results.

This means that the active monitoring system should verify whether events are coherent with predefined risks or not and should be able to identify new risks, or at least events that are potentially dangerous and do not comply with any of current scenarios. In practice, the active risk monitoring system is a tool analyzing events to verify whether the system was properly prepared or not. Furthermore, in case of detection of incoherency between the current and expected state of the system, it should provide information about a probable scale of its influence on security. This, however, is by no means replacement of the risk analysis, but only approximate information about direction and weight of the observed incoherency, which should be then analyzed in detail during the information security assessment process.

The proposed information security monitoring system gathers data from various sources in a form of files or messages prepared according to Security Description Pattern [16]. Fig. 2 presents sources of data for the risk monitoring system.

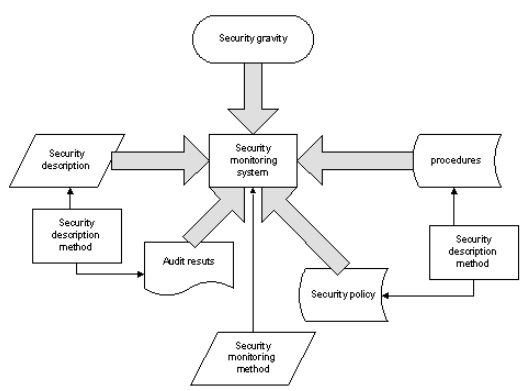

Fig. 2. Risk monitoring system
Rys. 2. System monitorowania ryzyka

All of those source systems and devices can provide data over a local, trusted network or, after optional authentication, over public networks like the Internet. This allows monitoring of remote locations and organizations of various structures – including virtual organizations. As can be seen in Fig. 2, the proposed system gathers data not only directly from system devices (security description) or its users (audit results), but also analyses security policy, procedures and results of security assessment (security gravity) for each asset or scenario.

In general, the gathered data can be shown in a form of equations:

$$\text{ExpectedState} = \text{SecurityPolicy} + \text{Procedures} + \text{SecurityDescription\_definitions} \quad (1)$$

$$\text{CurrentSecurityState} = (\text{SecurityDescription\_current} + \text{AuditResults}) \quad (2)$$

Then differential on security can be calculated as:

$$\text{SecDifference} = \text{sum}(\text{ExpectedState XOR CurrentSecurityState}) / \text{sum}(\text{FactorsTaken}) \quad (3)$$

And influence on security (including its importance) can be then calculated as:

$$\text{SecInfluence} = \text{SecDifference} * \text{SecurityGravity}(\text{asset}) \quad (4)$$

The generated suggestion of corrective actions, which may include replacement or reconfiguration of current counter measures, should be then analyzed from the perspective of the risk treatment efficiency, e.g. according to [17]. This should prevent from applying too expensive solutions or solutions that will result in minor, however positive, change of risk making cost of such migration unacceptable. It should be remembered that in most cases it is impossible to assign fixed costs of countermeasure implementation or reconfiguration. It is so because such cost depends not only on the price of the solution itself and its installation, but also on costs of decreased operability of the organization during migration.

5. Information security management system proposal

The goal of risk management is to keep proper level of company success [18] or economical minimization of unforeseen results [19]. The fulfill those conditions, the proposed information security management system is based on cooperation of two independent systems: the information security assessment system (or risk assessment system – RAS) and the information security monitoring system (or risk monitoring system – RMS). The most important in such a case is exchange and integration of data. The idea of data flow between these two systems and their main user, security manager is shown in Fig. 3.

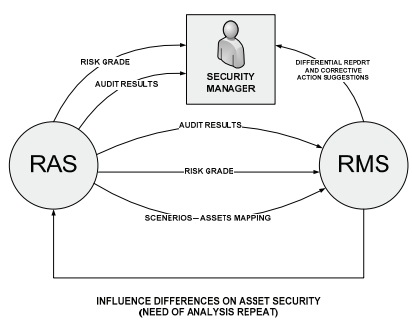

Fig. 1. Idea of Information Security Management System
Rys. 1. Idea systemu zarządzania bezpieczeństwem informacji

The information security monitoring system receives from the assessment system:
- analysis results (remaining risk values for individual scenarios),
- mapping of scenarios on assets.

The information security monitoring system generates and provides:
- differential report,
- influence of differences on assets security,
- corrective actions suggestions (changes in counter measures).

On the basis of information about influence of the identified differences on security, the assessment system determines automatically whether it is necessary to repeat the whole risk assessment process or not. Similar information sent to a security manager is provided together with new countermeasures proposals. In case of significant inconsistency between the current and expected state of security, for instance if half of user passwords was deleted overnight, the security manager is responsible for raising alert and taking manual counter measures on the system.

6. Results and conclusions

The proposed solution in fact consists of two cooperating systems, which can also be used separately. When combined, they create the automated information security management system, capable not only of audit and risk evaluation support, but also able to detect problems and suggest list of possible solutions to choose from.

Such approach to information security management, thanks to high level of automation of the process, reduces costs significantly and helps shorten the time of reaction in case of an unforeseen event. Furthermore, automation of risk assessment allows more detailed analysis without increase in costs. This is possible mostly due to shortening the time of data gathering and replacement of some manual questionnaires with automatic data gathering.

7. References

[1] Information technology – Security techniques – Code of practice for information security management, ISO/IEC 27002:2007.
[2] OECD Guidelines for the Security of Information Systems and Networks: 'Towards a Culture of Security', Paris: OECD, July 2002.
[3] Risk management – Vocabulary – Guidelines for use in standards, ISO/IEC Guide 73:2002.
[4] Expression des Besoins et Identification des Objectifs de Securite « EBIOS », DCSSI, France 2004.
[5] Baskerville R.: Information Systems Security Design Methods: Implications for Information Systems Development, Computing Surveys 25 (4), 1994.
[6] Parkert D. B.: Computer Security Management, Reston Publishing Company Inc., Reston VA, 1981.
[7] Méthodologie d'Analyse des Risques Informatique et d'Optimation par Niveau « MARION », CLUSIF, France 1998.
[8] Méthode Harmonisée d'Analyse de Risques « MEHARI » CLUSIF, France 2007.
[9] Microsoft Security Assessment Tool « MSAT », http://technet. Microsoft.com/en-us/security/cc18512.aspx.
[10] CCTA Risk Analysis and Management Metod « CRAMM », Central Computing and Telecommunications Agency, United Kingdom Government, UK 1987.
[11] Operationally Critical Threat, Asset, and Vulnerability Evaluation « OCTAVE » Carnegie Mellon University, Canada 2006.
[12] Control Objectives for Information and related Technology « COBIT » ISACA, IT Governance Institute, US 2007.
[13] ISO/IEC 27005:2008 Information technology -- Security techniques -- Information security risk management.
[14] Pawlak M.: Project management, Wydawnictwo Naukowe PWN, Warszawa 2006.
[15] Szyjewski Z.: Metodyki zarządzania projektami informatycznymi, Placet, Warszawa, 2004.
[16] Klasa T.: Information Systems Security Description Proposal, SMI 2010 – in print.
[17] Nowakowski A., Klasa T.: Evaluation of information systems' risk treatment efficiency proposal, Metody Informatyki Stosowanej, Nr 3/2009 (20), Polska Akademia Nauk Oddział w Gdańsku, Komisja Informatyki, Szczecin 2009.
[18] Frączkowski K.: IT Projects management. Projects in virtual environment. Projects success and failure factors. (in polish), Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław 2003.
[19] Lent B.: Project leading processes management (in polish), Informatyka i Telekomunikacja, Difin, Warszawa 2005.

otrzymano / received: 10.09.2010
przyjęto do druku / accepted: 01.11.2010 *artykuł recenzowany*