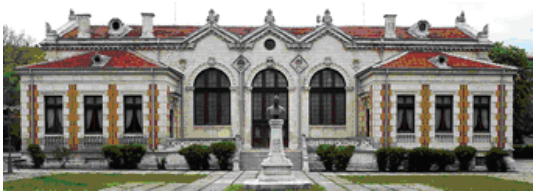

Journal scientific and applied research, vol. 5, 2014
Association Scientific and Applied Research
International Journal

Original Contribution ISSN 1314-6289

APPROACHES TO IDENTIFY VULNERABILITIES IN THE SECURITY SYSTEM OF THE SOCIAL ORGANIZATION AND COMPUTER RESOURCES

Hristo Hristov, Petar Boyanov, Tichomir Trifonov

KONSTANTIN PRESLAVSKY UNIVERSITY OF SHUMEN,
SHUMEN 9712, 115, UNIVERSITETSKA STR,
E-MAIL: hristov63@abv.bg, peshoaikido@abv.bg, trif.69@abv.bg

Abstract: *Essential component of organizing stage of the counteraction for the encroachment against the business organization is to identify vulnerabilities of the social organization. The purpose of this stage is to identify all existing and potential weaknesses and disadvantages of the security system of the organization, creating a circumstance for adversely effects on the sources of threat.*

Key words: *Company Security system, computer security, encroachments, indefensibility, management, mechanisms, security environment, protection, threats, vulnerabilities.*

1. Introduction

In the suggested counteraction organizing methodology of outrage against the security system (fig.1) the vulnerabilities of the social organization have got significant role in the overall management process of counteraction. The aim at this stage is to determine all availabilities and social weaknesses and disadvantages of the organization security system, creating circumstance for an unfavorable effect of the sources of threat.

The vulnerability identifying and assessment is a process with that is being evaluated the weaknesses of the system for physical security, personal security, the procedures or other organization functioning areas that could be exploited. The purpose of this process is to be revealed weaknesses in the security system, information systems and networks and unprotected crucial infrastructure of the organization [1].

The vulnerability could be defined as disadvantage or weakness of the security system for given social organization that could be intentionally or accidental exploited and therefore, to be obtained disturbances in the politics for organization security [2].

The disadvantages and weaknesses could be related to the entire architecture or designed and applied mechanisms and procedures for protection and system security control. Each social organization builds own system of security mechanisms and procedures in accordance with law and administrative regulations and standards in the security sphere and functioning organization environment [3].

2. Analysis of the security system

The organization security system is set of administrative, organizational, technical, operative and information procedures, mechanisms and actions, ensuring the protection of given social organization and creating circumstances for reliably mission execution of the organization [4].

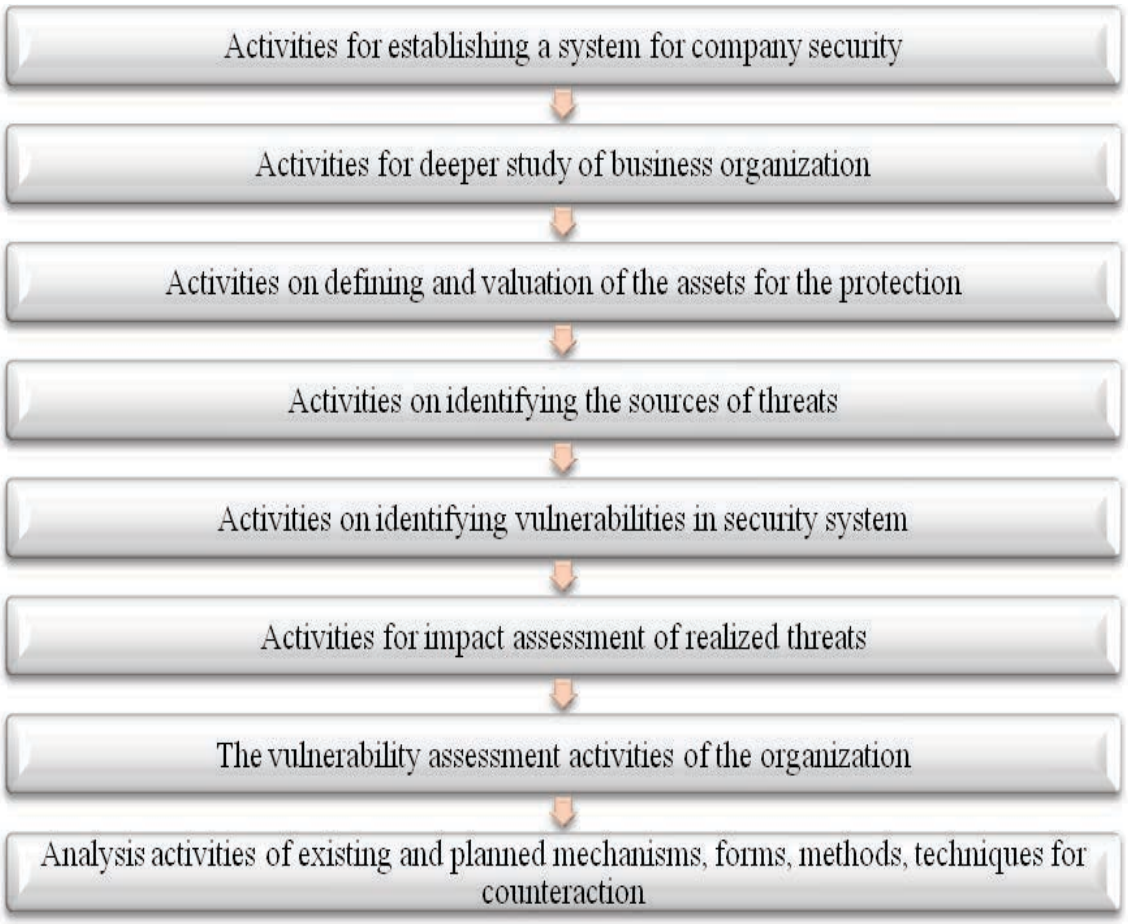

Fig.1. Counteraction methodology of outrage against the security system.

The efficient counteraction management demands in detail knowing and permanent monitoring and system control for the security of the social organization in order revealing the availability of the weaknesses and disadvantages, leading to vulnerability from the impact of determined or potential sources of threat [1].

The permanent monitoring of the security system advantages for the timely indications revealing for system vulnerability and preventively actions taking for eliminating the disadvantages and weaknesses and prevention the negative influence from the sources of threat.

The reasons for disadvantages appearance and weaknesses in the security system could be neither insufficient degree of adequacy of the complex of administrative, organizational, technical and operative acts, mechanisms and procedures of dynamic changing security environment and nor current problems in the system functioning, connected with low quality or incomplete implementation of the planned security measures.

The indentifying the system vulnerability for protection of given social organization could be accomplished by applying different methods, techniques depending on the degree of development and function stage of the particular security system.

The identifying and assessment for presence of vulnerabilities will have different purposefulness and object of study at various stages of the design of the security system simultaneously by induction the system and by its functioning [1],[2],[5],[6].

At the stage of project of the security system (by induction of new system or by vastly transformation of existing) the search vulnerabilities process would be pointed to revealing the weaknesses and disadvantages in the security politics of the social organization, the planned procedures in the sphere of the security, defining the requirements to the system and etc. In the process of security system induction, the vulnerabilities' identifying must be expanded and involve studying and assessment of the planned security actions, results of the initial tests, system assessment and etc. At full functioning security system, the vulnerabilities identifying should be expanded to the analysis of the characteristics of the security system, control mechanisms and procedures, used for protection the organization [2],[3],[7].

It is possible the applying a set of different methods for identifying the vulnerabilities: analysis and assessment of identified weaknesses and disadvantages; using proactive methods for security system testing; requirements developing for security and assessment the adequacy of existing protection mechanisms and procedures, etc.

The analysis and assessment of the identified weaknesses and disadvantages of the security system are pointed in the defining the fact, do they represent and what is the vulnerability level of the system. Applying this vulnerability identifying method could involve using various techniques of information gathering for earlier and current weaknesses and disadvantages: documents analysis, filling different questionnaires, interview for a job, using automated scanning systems and etc [4],[6].

The review and analysis of documents includes work on documents connected with law regulation of the environment in that functions a given social organization - legal and sublegal basis, instructions and directives; documents defining the social organization work; documents related to the structure and functionality of the security system; analyses, reports, inquires, doings related to marked infractions of personal, physical, information, industrial security and information and network security systems; Results of audits and inspection records.

The developing and using questionnaires of information gathering for weaknesses and disadvantages of the planned and used mechanisms and security control procedures were related to obtaining special staff assessment that is committed to the designing and exploitation of the security system. The system vulnerabilities could be best rated by the staff, working on the security problems and obtaining objective state assessment. This technique could be implemented with a visit and conducting an interview, that has increased the extent of analysis objectivity [2],[3],[4].

The visiting and interview with the staff, committed to management, designing, including, exploitation, security system maintaining were important components of the entire assessment for system reliability and vulnerabilities identifying placed the social organization under conditions of insecurity. With the visiting and interviewing there could be contributed immediate idea and information about the functioning of the mechanisms and procedures to ensure the security of social organization [2].

Applying automated scanning systems was proactive technique for revealing weaknesses and disadvantages of the security system. This was a technical method for control and finding vulnerabilities mainly in the physical security system and the information security and network systems [5].

Another major method for vulnerabilities identifying is testing the security system of the social organization. This is a proactive method and includes applying of various techniques for detecting weaknesses and disadvantages in individual branches and system nodes, which may leads to vulnerability. The method involves developing and implementing a plan to test the effectiveness of the applied mechanisms and security and control procedures, applying a test for sustainability assessment of the system against interventions in penetration or eliminating the protecting mechanisms [6],[7].

The development of security requirements and evaluating the adequacy of existing defense mechanisms is the main method aimed at assessing the compliance of planning and implementing controls and procedures with the requirements and criteria for reliably ensuring the security of the organization. The developed security requirements contain basic minimum safety standards that can be used to systematically identify and assess the vulnerabilities in the personal, physical and information security systems.

The security criteria may relate to various aspects of operation of the organization - the security process management in the technical areas [1].

At the level of security process management the security criteria may include: accurate determination of the obligations; separation of responsibilities; capabilities for responding to incidents; periodic review of the security system; security investigation and certification of personnel; personnel training on security issues; risk assessment system; designing and implementation a security plan and etc [3].

At the operational level, the criteria are related to the operational functioning of the system: control of physical security environment; control and ensuring capabilities; procedures for internal information sharing and etc.

At the technical level of security the criteria are related to providing technical reliability of communications and also of the cryptographic systems and identifying systems and access control; Intrusion detection system, etc.

Thus the proposed methods and techniques to identify vulnerabilities in the security system of social organization represent only part of the possible approaches for objective and reliable identification of the deficiencies and weaknesses of the system. Due to the fact that impossible to be realized absolute complete identification of the vulnerabilities in one system and could not provide the same level of protection for all sections available with weaknesses, it is necessary to identify and prioritize these with the highest degree of crucial importance for functioning of the organization, in order to provide maximum protection.

The possibility of systematically identification and assessment of the units of the organization, having a key role in the functioning and implementation of its mission, even allows by insufficient resources to be provided optimum protection for these critical units and minimize their vulnerability to adverse effects.

The principle of assessment units and objects with critical importance for the operation of a social organization allows to reliably their protection, based on focusing the resources and ensure achievement of objectives.

The identification of the vulnerabilities of the security system of a given social organization as an important component in the process of counteraction of violations should be carried out systematically, using a wide range of methods and approaches to ensure the objectivity of the process and favor the building of a reliable protection of the organization against modern attacks and threats. The Complex review of the process of identifying the potential sources of threat and identifying vulnerabilities creates a basis for objective analysis and assessment of harm and conditions for effective implementation of the strategy for resistance management.

In the analysis of potential sources of threat and vulnerabilities besides the standard methods of analysis can be used more methods and techniques such as decision-making in conditions of risk and uncertainty; Measurement of the main

trend and dispersion; Modeling real opportunity; Analysis of the threat; Analysis "a fault tree" and etc [6].

"The main objective of the analysis is to maximize the usefulness of the information obtained from operational and open source by extracting of new information. [7]"

The purposeful processing of information sources of threats and vulnerabilities of the security system is the basic idea of obtaining a new, qualitative term, information product, which is a prerequisite for carrying out an objective assessment of the cyber-attacks, the size, direction and intensity of the negative impact on the organization and the need to implement appropriate strategies for counteraction.

Analysis of the pair source of threat - vulnerability allows to determine or predict the way of function of the sources of threat on the social organization and on this basis to plan and implement effective counteraction and entire optimization of the security system. An important stage in the analysis is to determine the probability and at this stage must be analyzed: motivation, capacity and capabilities of the source of the threat; nature and characteristics of vulnerabilities; the existence and effectiveness protection mechanisms and procedures of the security system.

3. Conclusion

In conclusion there may be assumed that the assessment of the vulnerability of social organization includes the following: task analysis of the organization and assessment of the potential impact of the source of the threat on their implementation; assessment the elements in the organization with critical meaning for the performance of its mission; assessment of the security system of the organization; possibility assessment for recovering after realized encroachment.

Acknowledgements

This paper is supported by the Project BG051PO00l-3.3.06-0003 “Building and steady development of PhD students, post-PhD and young scientists in the areas of the natural, technical and mathematical sciences”. The Project is realized by the financial support of the Operative Program “Development of the human resources” of the European social found of the European Union.

References:

[1] Decker, R., Homeland Security: A Risk management Approach, Statement before Senate Committee on Governmental Affairs, Washington, D.C., 2001.p.10

[2] Sandev, G. Security of organizations, Konstantin Preslavsky University Press, Shumen, 2012, ISBN 978-954-577-621-2.

[3] Stanev, St, Zhelezov St, Computer and Network Security, Konstantin Preslavsky University Press, Shumen, 2002

[4] Mlechenkov, M., „Methodology for developing a system for information security", Vasil Levski" National Military University, Artillery, AAD and CIS faculty, Shumen, 2010. s.5.

[5] Dimanova D., Iliev Sv., Steganography - the art of hiding information,. Konstantin Preslavsky University Press, Shumen, 2013

[6] RiskManagementStandards, 2002.p.14.

[7] Vladimirov, P., Management of the special services, S., 2002, SB. p.164-190.