An Example of a Methodology for Developing the Security of a Distributed Business System

Ivan Vulić
Military Technical Academy
University of Defense
Belgrade, Serbia
ivan.vulic@mod.gov.rs

Radomir Prodanović
Centre for Applied Mathematics and Electronics
Serbian Armed Forces
Belgrade, Serbia
radomir.prodanovic@vs.rs

Ivan Tot
Military Technical Academy
University of Defense
Belgrade, Serbia
ivan.tot@va.mod.gov.rs

***Abstract*—Traditional business today increasingly moves to electronic business. The new business environment creates new challenges. One such challenge is the security of business in an unsafe environment such as the Internet. Therefore, the security of electronic business should be approached in a systematic way. The authors of the paper developed a methodology for implementing security in a distributed business environment. Such methodology can be used by persons who are not from information and communication technologies.**

Keywords—electronic business, security, methodology, requirements, distributed business system

I. INTRODUCTION

In today's world of global networking, computers rarely work isolated and mostly cooperate with each another in order to communicate, process, transfer and store data. When parts of the system or system cooperate with other parts of the system or systems geographically located in multiple locations, then we discuss the distributed system.

Ease of Use Today's large business systems operate globally, and their data are distributed across multiple locations. Their business is based on the exchange of electronic data between organisational units located in multiple locations. Large business systems tend to switch to online business to earn profits from resources invested in information technology.

However, e-business apart the mentioned advantages has its own risk. The risk in e-business is data security. Business systems, commercial or non-commercial, are more or less sensitive, depending on the size of the security risk data. In order to prevent classified business data leaking, we should be a responsible and systematic approach to data protection.

Computer systems enable processing of large amounts of data in a short period for large business systems, most often in real or about real-time, so that management gets the precise data needed for making appropriate business decisions on time. The technology development has led to the replacement of large centralised computer systems where all data was stored in one place - personal computers connected to distributed computer networks. The consequences were that existing data protection techniques did not adequately follow the modernisation of hardware, system software, information systems, and computer networks.

Therefore, the development of the distributed business system security can be crucial for achieving and maintaining competitiveness, providing the flow of money, achieving profitability, ensuring the business reputation and surviving an organisation on the market.

Organisations today use standards for information security (e.g. family of ISO 27000 standards, NIST standards) that contain a large number of typical security requirements for maintaining risk at an acceptable level. The application of standards can lead to the neglect of security requirements arising from the specifics of an organisation or business process. The authors of the paper believe that the standard should be used as a framework for the disclosure of requirements that needs to be integrated through a methodological approach to security. Therefore, the authors created a methodology for developing the security of a distributed business system that can be applied to other systems.

In the second chapter, the authors present a methodology for the security development of a distributed business system, while in the third chapter they describe the process of eliciting and defining the requirements in order to avoid the generalisation of security requirements. The fourth chapter describes the application of the proposed methodology in project management. The conclusion is given in the fifth chapter.

II. METHODOLOGY FOR THE SECURITY DEVELOPMENT OF THE DISTRIBUTED BUSINESS SYSTEM

A. Identifying the Real System

Before considering security, it is necessary to determine the type of distributed system. The system can represent one type of distributed system, but it can also consist of several types of distributed systems.

This is an opportunity to determine the boundaries of the system. That is essential for determining what belongs to the system and what does not. It is necessary to determine whether there are points of interaction between the inside and outside of the system at the boundary line.

In the process of identifying the real system, the hardware component is considered through the equipment, while the software component is considered through the types of system and application programs used in the system. One of the most important elements considered insecurity is the deployment of data that can be centralised or distributed in one or more locations. Human resources should be seen in the inside and outside environment - from management to employees and to users.

Consideration of communication explains how the system entities exchange data in the system and with entities outside the system.

Data flows indicate how data is transmitted between the entity and the location of the data. Data flows can extend only in the internal environment of the system or can connect the internal and external environment. It is necessary to consider the type of data and how they are security-sensitive.

The data life cycle includes generation, processing (transformation and integration with other data), storage and destruction of data. Consideration of the life cycle provides information about subjects and entities critical for preserving data security.

Work procedures should provide an answer to how employees and external partners can influence on the security of the system itself.

B. Determining Global Security Goals

Global security goals are determined after consideration of the real system, boundaries, components, and system security, and knowing business strategy, security policies, business goals and competition.

Determination of global security goals is affected by the business system type. The goal of every employer is to be sure about the information they have in the organisation so that an unwanted person or competition does not have access to data in all

The employer must be sure about the data accuracy and reliability, so it can determine whether the data has been modified. Hence, the goal is to prevent or to have a mechanism that warns about unauthorised modification of data.

It is necessary to control the work of employees in the system and not allow them to do whatever they want. So. the goal is the necessity for providing controlled access to resources through the assigned roles, responsibilities and credentials.

The system can communicate with other systems, distant parts of its system or users. In such communication users need to be sure they are communicating with the right entity. Not only that, it is necessary to make sure that the other party received the message. In this case, it is necessary to fulfil the goal of the impossibility of false representation and repudiation for the other party that it received the message.

Depending on the degree of sensitivity and the importance of the data, as well as on the need for the user to have continuously available information for further decision-making, it is necessary to ensure continuity in system operation. It is necessary to achieve the goal of constant availability.

C. Defining Global Security Requirements

After determining the security goals, it is necessary to determine the global security requirements. These requirements are the generalisation of several smaller requirements. Security requirements are defined to achieve one or more security goals. General safety requirements are integrity, confidentiality, availability, non-compliance, authentication, access control, activity monitoring and detection of security breaches.

In addition to general safety requirements, other security requirements may also be considered, such as physical protection or recovery from unwanted events.

It is not necessary at this stage to further decompose demands because the management can create images of too much complexity, and therefore the need for large financial investments. All this could cause a rejection or creating a wrong picture of the security needs of the system.

D. Identifying the Security Domain

After the boundaries and parts of the system, resources, and processes are defined, domains are created. Depending on the complexity of the system, domains can be divided into subdomains. For example, the domain of the computer network can be divided into the following sub-domains: fixed computer network, mobile or ad hoc network. The goal of decomposing domains is to reduce complexity in further consideration of objectives, security requirements, risks, threats and controls.

At this stage of domain determination, it is necessary to look at the touchpoints (interfaces) between domains, as well as scope of overlapping domains.

E. Determination of Security Objectives by Domains

The next step after defining security domains is defining security objectives based on global goals for each domain.

The goals for each domain, when implemented, should achieve global goals. The domain goals are defined according to the area covered by this domain. The achieved goals need to be once again reviewed and verified by the design team.

Security goals can be defined based on SMART criteria [1] with the following meaning: Specific, Measurable, Achievable, Relevant, and Time-bound. After completing each process that leads to the goal realisation, it is necessary to analyse the goal towards the following two criteria [2]: Evaluation and Review.

F. Determination of Security Requirements in Domains

Well-defined security requirements are important not only to ensure an adequate level of security in the system but also to avoid the implementation of a security solution that will later turn out to be inadequate. Such security requirements give added value to functional and non-functional requests in achieving process and resource security. Security requirements should be clearly and specifically defined in order to ensure system security. Inadequately defined security requirements lead to the inability of effective assessment of the applied measures.

Therefore, the security requirements should be defined systematically to avoid the use of security requirements, generic lists and security considerations from the perspective of the attacker.

The security requirements are often developed independently of other types of requirements. As a result, security requirements are often developed for themselves, and the security aspect of functional requirements is ignored.

The development of a security requirement should be considered as a continuous activity because the operating environment and business objectives are often changed.

When determining the request it is particularly important to observe the security aspects from the attacker side. The attacker is not interested in the functional characteristics of the system unless it can be used for the attack. An attacker usually seeks flaws and weaknesses that will enable him a successful attack [3]. It is therefore important to consider the potential activities of the attackers [4], and not just the functionality of the system. A method for determining the security requirements is given in chapter III Elicitation and Defining Security Requirements.

G. Implementation of Appropriate Security Measures

Depending on the nature of the risk, it is necessary to decide on the measures to be taken. Each of the decisions initiates a series of risk-management activities. The ability to identify the most appropriate controls for the given risk can lead to the success or failure of the security introduction process. It is crucial to find the right combination of technical and non-technical measures for eliminating or reducing possibility of occurrences that lead to risk so that the risk is acceptable for system without causing unnecessary costs.

There are many controls that mitigate risks, and their focus is not on eliminating risk, but to reduce exposure to risk to an acceptable level. In order to mitigate the risk, it is necessary to:

- Reduce the probability of risk occurrence.
- Limit the strength of the attack.
- Reduce the sources or resources (assets) sensitivity.

Reducing the probability of risk occurrence is carried out by preventive controls, such as regular monitoring of security vulnerabilities and deficiencies, regular updating and upgrading of system and application software, users training, physical protection implementation.

In order to limit the strength of the attack, a compromise solution needs to be found. This risk mitigation approach does not have to prevent the exploitation of vulnerabilities and weakness in advance, but can limit the scope of controls or enable quick response to prevent further escalation. Most controls in this category will be oriented towards detection and recovery from attacks. Reducing resource sensitivity, without addressing any vulnerability or threat, can be done by changing the resource sensitivity. Resource sensitivity can be minimised by relocating resources under the influence of another control, e.g. moving to a better-protected location in the system, reducing the threat to the area where the vulnerable resource (application of the firewall) is located or the implementing of authentication controls.

The most commonly used controls are those that influence the limitation of risk probability or exposure to risk in some way. The controls affect the risk by removing or patching vulnerabilities. It is necessary to determine controls that eliminate the underlying problem if it is about risk repair, while risk mitigation controls need to be used to reduce exposure to risk, but not to eliminate the risk source. Most of the time is spent on planning for mitigating or limiting risks, but accepting and transferring risks are also not less important strategies.

The bases for risk acceptance are well-established and formalised processes that determine and define security exceptions. The most common request for an exception is the exclusion from a certain security standard established by the organisation. An exception may be accepted by carrying out controls from a risk mitigation plan. Management approves exceptions and risk mitigation plans, and in this way, they accept the existing level of risk.

If there is no decision to mitigate the risk, they can be made risk transfer on insurance to cover possible financial losses.

III. Elicitation and Defining Security Requirements

Security requirements are often defined as general safety requirements and as such, usually can not be implemented. In order to overcome the generality of the security requirement, it is necessary to identify the services, the operational scenario and the means that must be protected.

Determination security requirements in domains, that is, the process of eliciting and defining security requirements is carried out through the following phases:

- Phase I - Preparation for determining security requirements.
- Phase II - Security vulnerability analysis.
- Phase III - Threats modelling.
- Phase IV - Determination of security requirements.
- Phase V - Risk assessment.
- Phase VI - Categorization and prioritization.
- Phase VII - Preparation of documentation.

A. Phase I - Preparation for Determining Security Requirements

Preparation for determining security requirements by domains is carried out through three processes: assets identification, property scenarios creation and selection of techniques for requests eliciting.

The assets to be protected are identified based on global goals, global requirements, domain goals, and general requirements for the certain domain. The asset represents everything that has a value for the system. The business process and the various scenarios in which the asset appears are considered for each component of the identified property. Participants, business processes, interaction with other assets and property transformations are identified based on the scenarios. The next step is the selection of techniques to elicitation a request.

B. Phase II - Security Vulnerability Analysis

The concept of system vulnerability refers to deficiencies and weaknesses in security procedures, design, implementation or controls that can be used to impair security. According to ISO 27002: 2013 [5], vulnerability is defined as: "the weakness of assets or group assets that one or more threats can use."

The vulnerability analysis can be carried out in the following ways:

- An active approach, such as analysis by scanning or configuration analysis.
- An analysis of the system based on a checklist and experience.
- Analysis of existing security measures.

The methodology for determining the vulnerability of a system depends on the nature and status of the system. If the system is not yet designed, then the existing security policies, planned procedures, existing requirements and already developed and applied safety rules are explored. If the system is developed, then the vulnerabilities are identified by studying the planned safety rules that are described in the documentation and by results of the final testing. If the system is operational, vulnerabilities are identified through an analysis of the security features of the system, technical and procedural controls.

The goal of security vulnerability analysis is to obtain a list of vulnerabilities in the system that potential sources of threat can use.

C. Phase III - Threats Modeling

By definition, the threat represents potentially security breaches of the system or an event that can hurt the system [6]. According to ISO 27002, the threat is "possible cause of an unwanted incident that could cause harm to the system or organisation".

Threats modelling is the process of identifying threats and sources of threats, determining their mutual relationship and strength, and documenting. It allows understanding the threat to the system from the perspective of a potential attacker and identifying the threats that cause the greatest consequences for the system [7]. This process results in a model that describes potential threats and sources of threats to the system and is used to make critical decisions about system security [8]. The process of threat modelling can include risk assessment and the development of a risk mitigation strategy.

There are more approaches to threats modelling such as attacker-oriented threat modelling, asset-oriented threat modelling and software-oriented threat modelling. The asset-oriented threat modelling starts from confidential system resources, while attacker-oriented threat modelling starts from the way an attacker can achieve his goals. The software-oriented threat modelling starts from the software system design and goes through the model in search of threats.

D. Phase IV - Determination of Security Requirements

Determination of requirements is a process of defining security requirements. That process determines the implementation of appropriate controls. Well-defined security requirements are the key to successful system security. The definition of the request is carried out through the following steps, Fig. 1: elicitation, analysis, definition, redefinition, validation and verification of the request.

Requirements elicitation. The requirements elicitation is a procedure of finding security requirements on the basis of goals, general requirements, assets, earlier requests, established lines of attack, standards and using appropriate techniques. During requirements elicitation, while considering a scenario, property, or attack line, can be uncovered multiple requests. When eliciting a request, it is necessary at first to elicit requirements from business processes, earlier requests, documentation, and at the end, eliciting requirements arising from the impact of vulnerability and threats.

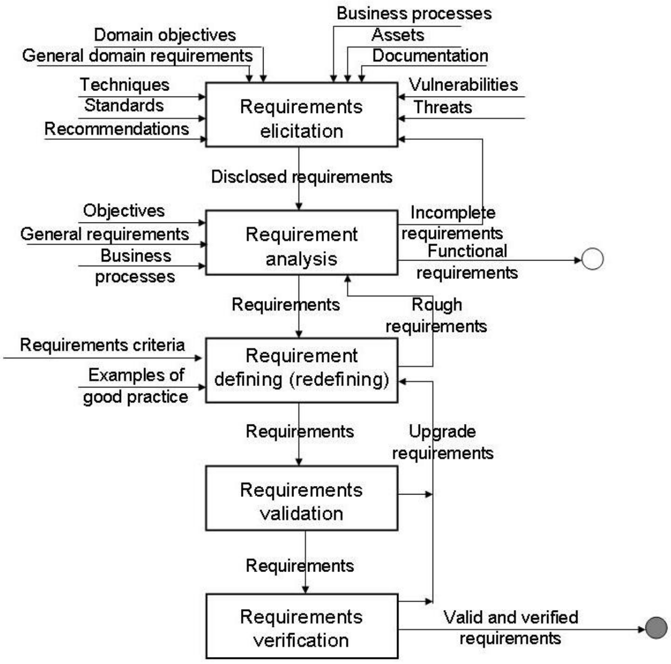

Fig.1. Procedure for determining security requirements

Requirement analysis. In this step, each disclosed request is analysed to determine the type of request (functional or security requirement), whether the request meets the security goals, its complexity, and the multiplicity of the direct or indirect appearance of the request. Complex requests return to the previous step of disclosure, in order to simplify the request, either by decomposition to multiple requests or by rejecting everything that does not part of the request.

Requirement defining (redefining). After the analysis, the requirements are shaped in a form that is concise and understandable for implementation, and for checking the implemented security controls. If the defined request is not clear enough or does not meet the criteria for good requests, it is returned to the analysis and redefining. All defined requirements go through the control of meeting the criteria for good requirements, as well as the requirements of the work team. The requirements should be defined so that security controls can be applied.

Requirements validation. Requirements validation involves checking if the defined requirements reflect the set goals and future measures for mitigating or eliminating risks caused by vulnerabilities and threats. Requirements validation can be done by one of the following techniques: analysis and report on detected errors, formal inspection (auditors are placed in certain roles and follow the prescribed rules), assessment of requirements (assessment of purposes, goals, environment, risk, proposed measures, evaluation about eliminating or reducing threat or vulnerability).

Requirements verification. Requirements verification is used to verify if requests for all attack lines, vulnerabilities and threats detected in the system are defined and whether the impact of a single domain request has no negative consequences for the other domain.

E. Phase V - Risk Assessment

Risk assessment is the process of identifying, quantifying and classifying risk by priority, and according to the criteria for accepting risks and goals important to the system. The risk assessment must be an unambiguous, objective, reliable and reproducible process.

In the literature, the risk is defined as a function of the level of threat, vulnerability and value of information assets [9]. The more precisely, risk is the probability that threat has exploited some vulnerability of the property and thus jeopardise it. Mathematically, the risk can be expressed by the following formula:

Risk = threat * vulnerability * asset value (1)

This formula shows how the dependences between threat, vulnerability and asset value affect the level of risk. If we have a high level of threat and a high level of vulnerability, then the risk is high. If the threat level is high, and the asset is not as vulnerable because it has an implemented protection measure, then the level of risk will be medium. In the event when the levels of threat and vulnerability are high, but the value of the assets is low then the system will not suffer significant losses if a security incident occurs. Therefore, the risk is not high.

Risk assessment methods can be divided into qualitative [10,11,12], quantitative [13,14,15] and combined. Quantitative methods are based on mathematical methods and use exact numerical values, while qualitative methods use relative descriptive values. The combined risk assessment method is a combination of quantitative and qualitative methods.

The main difference between qualitative and quantitative risk assessment is in the value of the used parameters. The quantitative methods use numerical values, while qualitative methods describe the impact on the risk. The qualitative parameters are easier to interpret than the quantified parameters. Both types of risk assessment methods have their advantages and disadvantages.

The qualitative risk assessment largely depends on the quality of the subjective assessment. This type of method provides a complete picture of the system. The qualitative assessment results are easier to present. The result of quantitative methods is statistical data. The strength of quantitative methods is at the same time, their weakness, reflected in the fact that questions and answers must be strictly controlled. Therefore, the answers to such questions can not give a complete picture of the system. The advantage of these methods is reflected in easier creation of short reports on the performed risk assessment.

The main problem of applying risk assessment methods is that those are designed either from the point of financial analyst or from the point of view IT and security engineers. From engineers, the focus is on assessing each risk and / or group of similar risks and consequences that are causing by the risk. The approach of financial analysts is based on estimating the cost of risk on the basis of previously incurred damages, while in the engineering approach, the costs are determined based on the need for implementation of controls.

F. Phase VI - Categorization and Prioritization

The categorisation of the request is performed after the requirements validation and verification. Requirements can be categorised by domain, according to general requirements for distributed systems, by system and functional system components (system requirements, application requirements, functional requirements, requirements related to other domains). Each item in the categorisation should contain a domain.

Prioritisation of the request also should be done in addition to the categorisation. The priority of the requirements determines how much is urgent to solve the requirement. The urgency arises from a certain character and degree of risk. Prioritisation points to the need for rapid and efficient implementation of security measures in order to eliminate critical security points (processes, functions, procedures) as well as rationalising costs with maximum protection measures.

G. Phase VII - Preparation of Documentation

The preparation of security documentation is a procedure for completing the lists of requirements to be met. It arises as a result of the joint efforts of the work team and security engineer. In the documentation, except for the requirements, are described entities to which the protection and restriction measures will be implemented. The documentation should include requirements, property, threats, vulnerabilities, goals, performance, character and degree of risk. After determining control, the documentation can be updated by controls.

IV. Application of Proposed Methodology in Project Management

The project is a one-time and comprehensive process, special and unique (due to different goals, scope, deadlines, costs, necessary staff, etc.) with a clear goal and a certain beginning. It requires organisation throughout its duration until the final goal is achieved [16].

There are several definitions of the project in the literature, but it is important for all of them that the project has a goal to deliver a particular product in a planned time through organisation and resources.

Project management is the application of knowledge, skills, tools and techniques in the realisation of project activities in order to fulfil all the requirements of a project. Project management is carried out through the implementation and integration of project management processes that include initiating, planning, executing, monitoring, controlling and closing [17].

A process is a set of interrelated activities performing to create a particular product, service, or another result [17]. PMBOK (Project Management Body of Knowledge) groups processes based on their common characteristics in ten categories called project management knowledge areas, (Fig. 2). Knowledge areas group processes according to their common characteristics, and groups of processes more or less based on their order of execution in the management process.

Each project has its own specific goals. In addition to the goals that are aimed to fulfil the requirements of the project contractor, the authors believe that the goal of project safety in project management should also be considered nowadays. This goal should include project security through the following security objectives: authentication, confidentiality, integrity, non-compliance, privacy, availability, trust. In order to achieve these security objectives in project management, the authors suggest introducing a functional area of security management that would be implemented through all processes and areas of knowledge of project management. Project security management is carried out through the proposed methodology.

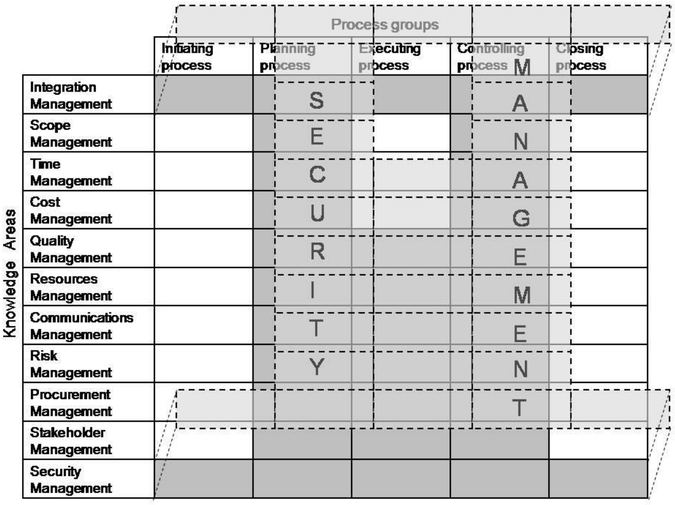

Fig. 2. Knowledge area project management security

Project security management refers to security management through project processes and knowledge areas. This means that security management includes determining security objectives, a project area considering security, the disclosure and definition of security requirements through risk assessment, the adoption and implementation of appropriate security measures. This knowledge area is applied in all process groups and areas of knowledge that are characteristic of the observed process, as in Fig. 2.

Project safety is initiated through the identification of project boundaries during the project initiation process. When the project boundaries are defined, and according to the significance of the project and the request of the project contractor, the project's security objectives (global objectives) are determined. The security requirements of the project (global safety requirements) are then determined. Their realisation should meet the security objectives.

Project security domains and their interconnection are identified during the planning process. The goal of establishing domains is to include all areas of knowledge and their mutual relationship in order not to omit all key project security points.

TABLE I. APPLICATION OF PROPOSED METHODOLOGY THROUGH PROCESS GROUPS

Process groups	**Phase of proposed methodology**	**Example**
Initiating process	Identifying the Real System	Identification of the project, project objectives, inputs and expected output from the project.
	Determining Global Security Goals	Security sensitive project data generated in strictly controlled and security terms, privacy, integrity, authenticity and non-repudiation.
	Defining Global Security Requirements	Protect against loss, damage and violation of the confidentiality of the project data.
Planning process	Identifying the Security Domain	The domain of the organisation - represents the project management organisation. Computer network domain - refers to the internal computer network used for the project.
	Determination of Security Objectives by Domains	Establish distributed responsibilities in the organisation, as well as a chain of responsibilities. Confidentiality of messages in communication in the inner environment and with the external environment is ensured.
	Determination of Security Requirements in Domains	Enable only certain individuals to have insight into parts of the project of special importance. All messages exchanged between members of the project should be protected.
Executing process	Implementation of Appropriate Security Measures	Apply strong authentication to access devices. Identify persons who can access specific parts of the project. All messages exchanged encrypt with a cryptographic algorithm.
Closing process	Implementation of Appropriate Security Measures	Destroy unnecessary documentation. Keep the project documentation in a safe with a strong authentication mechanism.

Security objectives arising from global security objectives are determined in security domains. Then is performed the disclosure and definition of the security requirement for domains. The security controls that are applied during the executing process are determined based on the security requirements.

During the control, the process is performed checking the implementation of safety controls, and if there are some deviations, correction is made. The effectiveness of the implemented security measures is analysed, and security measures of business secrets are being emphasised in the process of closing the project. Table 1 discusses the application of the proposed methodology through the process groups.

V. Conclusion

A distributed business system is a complex system that requires special attention to security. Business systems are characterised by the existence of sensitive information whose violation of security leads to endangering business interests. It is necessary to have an appropriate safety methodology in order to realise the security of such a system.

Security of the business system should not be based on the moment of attack and damage. It should be considered through a systematic approach to anticipate and assess the weaknesses of the system, assess the risk, and implement appropriate controls in a timely manner. Existing security methodologies are complex and require specific training to be applied. The very nature of the distributed system determines that resources can be deployed to locations where there is no professional staff, and such resources need to be protected. The paper presents the methodology that can be used by persons who are not from information and communication technologies.

References

[1] P. J. Meyer, “What would you do if you knew you couldn’t fail? Creating S.M.A.R.T. Goals, Attitude Is Everything: If You Want to Succeed Above and Beyond,” Meyer Resource Group, Incorporated, 2003, ISBN 978-0-89811-304-4.

[2] G. Yemm, “Essential Guide to Leading Your Team: How to Set Goals, Measure Performance and Reward Talent,” FT Press, 2012, ISBN-10: 0273772422

[3] R. J. Ellison, A. P. “Moore, Trustworthy Refinement Through Intrusion-Aware Design (CMU/SEI-2003-TR-002, ADA414865),” Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2003.

[4] J. H Allen, S. Barnum, R. J. Ellison, G. McGraw, and N. R. Mead, “Software Security Engineering: A Guide for Project Managers,” Addison-Wesley, Boston, 2008.

[5] ISO/IEC, “Information technology — Security techniques — Code of practice for information security controls, ISO/IEC 27002:2013,” 2013

[6] M. Bishop, “Computer Security: Art and Science,” MA: Addison-Wesley Professional, Boston, 2002, ISBN: 0201440997.

[7] M. Howard, D. LeBlanc, “Writing Secure Code,” Microsoft Press, 2nd edition, 2002, ISBN-10: 0735617228

[8] F. Swiderski, W. Snyder, “Threat Modeling,” Microsoft Press, 2004, ISBN-10: 0735619913

[9] A. Jones, D. Ashenden, “Risk Management for Computer Security, ” Elsevier, 2005, ISBN: 9780750677950

[10] J. Kouns, D. Minoli, “Information Technology Risk Management in Enterprise Environments: A Review of Industry Practices and a Practical Guide to Risk Management Teams,” John Wiley & Sons, 2011, ISBN: 978-0-471-76254-6

[11] W. Sonnenreich, “Return On Security Investment (ROSI) - A Practical Quantitative Model,” Journal of Research and Practice in Information Technology, Vol. 38, No. 1., 2006.

[12] B. Berger, “Data-Centric Quantitative Computer Security Risk Assessment,” SANS Institute, 2003

[13] T.R. Peltier, “Information Security Risk Analysis,” Third Edition, Auerbach Publications, CRC Press, 2010, ISBN 9781439839560

[14] R. A. Caralli, J. F. Stevens, L. R. Young, and W. R. Wilson, “Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process,” Technical Report CMU/SEI-2007-TR-012, Carnegie Mellon, 2007.

[15] Z. Yazar, “A qualitative risk analysis and management tool – CRAMM,” SANS Institute InfoSec Reading Room, 2002.

[16] A. Hauc, Upravljanje projektima/Project Management, Informator, Zagreb, 1991

[17] Project Management Institute, „A Guide to the Project Management Body of Knowledge“, 6th edition, Newton Square, 2017