KOŠICKÁ BEZPEČNOSTNÁ REVUE

KOSICE SECURITY REVUE

Vol. 9, No. 1 (2019), p. 14 – 23

ISSN 1338-4880 (print ver.), ISSN 1338-6956 (online ver.)

Model of Security Environment from the Point of View of Converged Security

Model bezpečnostního prostředí z pohledu konvergované bezpečnosti

Ludek LUKAS[1]

[1]*Tomas Bata University in Zlin, Czech Republic*

The manuscript was received on 30. 04. 2019 and was accepted after revision for publication on 15. 05. 2019

Abstract:

The safety and security is one of the key areas of interest for society and especially for organizations. Several dozen kinds of safety and security exist today. The organization must provide several kinds of security at the same time. Physical security, information security, occupational health and safety, fire protection and others are among the kinds of security provided. These kinds of safety and security usually exist independently, that causing problems. Discrepancy, greater complexity, staffing and financial costs are among those problems. Converged security is a possible solution. Converged security represents the integration of compatible kinds of safety and security. As a rule, physical security, cybersecurity and operational safety integrated into converged security within the organization. Converged security integrates separate data and events into a single unit, enabling a better understanding of the security situation. At the same time, it enables faster resolution of security breaches. Introducing converged security in an organization requires a good understanding of the security environment in which the reference object is located. Several ways of representing a security environment in the form of a model exist at present. The article describes how to create an organization's security environment model. It considers the conceptual model to be the most appropriate. This model allows a deeper analysis of the security environment. The article is a contribution to the development of theory of safety and security.

Keywords: *security environment, converged security, conceptual model, kind of safety and security.*

Model of Security Environment from Point of View of Converged Security

Ludek LUKAS

Abstrakt:

Bezpečnost patří mezi klíčové oblasti zájmu společnosti a zejména organizací. Několik desítek druhů bezpečnosti existuje v současnosti. Organizace musí zajišťovat několik druhů bezpečnosti současně. Fyzická bezpečnost, informační bezpečnost, bezpečnost a ochrana zdraví při práci, požární ochrana a další patří mezi zajišťované druhy bezpečnosti. Tyto druhy bezpečnosti existují obvykle nezávisle, což působí problémy. Nesouvztažnost, vyšší složitost, personální nároky a finanční náklady patří mezi tyto problémy. Konvergovaná bezpečnost patří k možným způsobům řešení. Konvergovaná bezpečnost je založena na integraci slučitelných druhů bezpečnosti. Fyzická bezpečnost, kybernetická bezpečnost a provozní bezpečnost se zpravidla integrují do konvergované bezpečnosti v organizaci. Konvergovaná bezpečnost integruje oddělené příznaky a události do jednoho celku a umožňuje lépe pochopit bezpečnostní situaci. Současně umožňuje rychlejší řešení narušení bezpečnosti. Zavedení konvergované bezpečnosti v organizaci vyžaduje dobře porozumět bezpečnostnímu prostředí, v němž se referenční objekt nachází. Několik způsobů reprezentace bezpečnostního prostředí ve formě modelu existuje v současnosti. Článek popisuje, jakým způsobem lze vytvořit model bezpečnostního prostředí organizace. Konceptuální model považuje za nejvhodnější. Tento model umožňuje provést hlubší analýzu bezpečnostního prostředí. Článek je příspěvkem k rozvoji teorie bezpečnosti.

Klíčová slova: *bezpečnostní prostředí, konvergovaná bezpečnost, pojmový model, druh bezpečnosti.*

Introduction

The issue of safety and security is currently an important social phenomenon. Safety and security is ensured at many levels of human society, at international and national levels, as well as at the level of organization and man. In total, over 50 kinds of safety and security have been created. The main kinds of safety and security include international security, physical security, cyber security, energy security, occupational health and safety, etc. Ensuring security in companies and organizations plays an important role. As a rule, individual kinds of safety and security are provided independently to other kinds. This way of ensuring safety and security has number of negatives. A picture of a security situation is made up of data that is scanned to identify a danger. The alarm system, which is the basis of physical security, captures the data about people movement. The data is not compared with data from cyber security, that situation blocks the early identification of security breaches. The sharp boundary between kinds of safety and security to block the creation of a comprehensive picture of security situation, which would be created by data captured in multiple kinds of safety and security.

Another negative is the increasing security costs resulting from the independent provision of individual kinds of safety and security. This has impact for both, for technology and especially for personnel. Each kind of safety and security is usually provided by a separate group of experts, using its own security technologies and its own protection processes. The links between the kinds of safety and security are cumbersome and there is often a duplication of activities. A possible solution to this problem is to integrate selected kinds of safety and security into one unit. This creates converged security.

1. Concept of Converged Security

Convergence generally means merging, converging. Convergence occurs when the functions of several different technologies begin to overlap. It is a process of creating increasingly dense links and links between technologies and networks. Convergence is becoming apparent when users gain the advantage of having a variety of features available through a single device or single application. Their response to the security situation may be faster and more complex.

Converged security is a specific kind of safety and security that is created by combining multiple compatible kinds of safety and security into one. This kind of security, due to analyzing the correlation of security breaches, allows to detect emerging security breaches faster and more effectively. Economic benefits are also positive. Converged security in an organization typically involves physical security, cyber security, and operational security. The structure of the merged kinds of safety and security may be different. Structure of converged security depends on the needs of the reference object as well as on the necessity of compatibility of individual kinds of safety and security. Compatibility is based on the need to protect the same reference object assets. Another condition for compatibility is the time characteristics of security breaches, which should be in roughly the same terms. Within the converged security of the organization, the changeover will be within seconds - minutes - hours. If there is a merger of safety and security, where one changes in minutes and the next in years, then merging into converged security would be meaningless, because the kind of security with short changes would play a dominant role. Basic principles of converged security:

- *converged security is provided for a specific reference object,*
- *only compatible kinds of safety and security can be included in converged security,*
- *it is desirable that the kinds of safety and security involved protect the same or at least partially identical assets.*

Converged security combines selected kinds of safety and security into one. This makes it possible to evaluate the security situation as a single picture, which reflects all additions to the security situation of each kind of safety and security. The added value of merging previously independent kinds of safety and security is the ability to perceive the correlation of individual security breaches into a single. Next improvement includes faster detection of security breaches, its manner, scope, and prediction of a possible future scenario. Other significant benefits of converged security include a comprehensive and timely assessment of the security situation. This assessment allows the security situation to be adequately addressed, thereby minimizing the negative impact of security breaches.

The introduction of converged security depends on a perfect knowledge of the reference object, its assets, possible threats and impacts on assets. Comprehensive knowledge of the security situation is obtained by describing and analyzing the security environment of which the reference object is part. There are currently no stable ways how to describe the security environment. The problem lies mainly in the variety of reference object types and possible paradigms that the security community uses in its analytical work. Concept of converged security is depicted at Fig. 1.

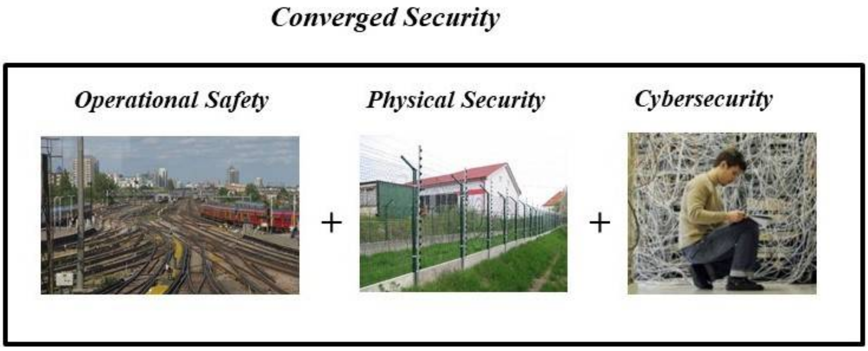


Fig. 1 Concept of Converged Security [1].

2. Security environment

Safety or security is always specific. It is provided for specific reference objects. To ensure this, it is important to know the security environment that the reference object is part of. The term "security environment" is one of the key terms of security terminology. Exploring the security environment is one of the major security activities. At present, there are exploring ways to define the security environment, how to describe it and how to explore it. The research includes formalization of the description of the security environment. Knowing the security environment, security issues and security breaches is a prerequisite for addressing them and thus ensuring security. The basic reasons for exploring a security environment include:

- *identification of key elements of the security environment, understanding its role in creating security breaches,*
- *identification of the features of the security environment, its impact on the security situation,*
- *identification of major threats and risks,*
- *specification of factors determining resilience and vulnerability,*
- *identification of variants of security situation,*
- *proposing new protection measures,*
- *prediction of security environment development.*

The term "security environment" is important to define properly. Hofreiter defines a security environment as a "variable complex of external and internal conditions, relationships, activities that determine changes in the state of security". At the same time, he states that the security environment is "part of the natural, social and technogenic environment in which security situations arise at a given time and space due to actors and interactions." The definition emphasizes the spatial dimension of the security environment. [2]

The author defines "security environment as domain, that include a reference object, its assets, and all relationships and factors that have a significant impact on its security". This is a narrow definition. Security environment can be defined by broader manner as "a spatially clustered system of important elements, factors and linkages associated with the emergence and resolution of selected security problems."

The security environment is part of the environment in which security problems arise and go on. These problems depend on number of factors. As a factor is usually understood the force or impact applied in some process. It is a fact that acts and therefore has an influence. Exploring the security environment means revealing the status of the various factors involved in the security situation. According to nature and functions we divide the factors into:

- *harmful,*
- *protective,*
- *configurational,*
- *assets.*

Harmful factors are those that cause harm. Harmful factors generally refer to a medium with a detrimental or harm effect. Examples include burning, flooding, unwanted data erasure, unwanted cutting.

Protective factors prevent the occurrence of harm and in case of its occurrence ensure its solution eg by renewal. Examples include intrusion detection, offender retention, deterrence, access denial, IRS response, and so on.

Configurational factors create conditions for the action of harmful factors but are not directly involved in the harming itself. Examples are unlit spaces, scattered combustible material, there are no rules for creating passwords.

Assets designate all elements that are key to a reference object and must therefore be protected. Assets are also referred to as interests. An example is life, health, property, environment, territorial integrity.

To describe the security environment is to identify and describe the reference objects that make up it. Further identify all of factors that have influence into a security breach. It also includes sources of threats, technologies, trends of development.

3. Possibilities of security environment description

The aim of the description of the security environment is to create its general representation by suitable means. Such a description represents a model of security environment. The model is an abstraction of reality in which its essential aspects are depicted. There are only key entities and links between them in the model. An example of a description of a security environment may be:

- *conceptual model,*
- *system view,*

- *sectoral view.*

Conceptual model

The conceptual model represents a verbal description of the security environment. It usually includes an overall description of the entire security environment. There are listed reference objects, threats, sources of threats and key factors that condition the development of the security situation. There can also be described the way of providing security, its advantages and disadvantages.

A variant can be a description of a reference object or reference objects in a given entity, its characteristics and its assets. Subsequently, the main threats that threaten the reference object and its assets are described. The conclusion is a description of how to ensure security. From a conceptual model, it should be clear what policy and doctrine was chosen to ensure security. A conceptual model is a document that allows to understand and to analyze. The conceptual model is suitable for describing a security environment from the point of view of a reference object and its immediate surroundings. It is suitable for converged security.

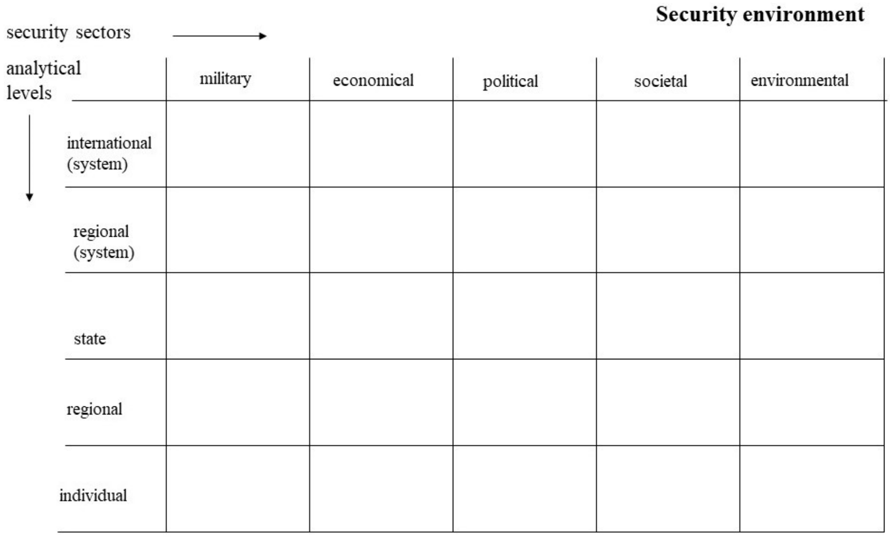
System view

The basic idea of the system view is to express the security environment in the form of a system. The system is composed of elements and relations (links). The elements of the system will be reference objects, threat sources, security system elements, and other elements that identify key security factors. Relations will indicate harmful actions, preventive and repressive protection activities, and other support activities. The view can be expressed in multiple layers. The system view is suitable for describing a security environment composed of multiple reference objects.

Sectoral view

The description is used in international security. It is based on the specification of security problems. It is based on a blind map of the security environment, including security sectors and analytical layers. Blind map of the security environment is depicted in Fig. 2. The idea for description comes from the Copenhagen Security School. Security sectors include the military, political, economic, societal and environmental sectors. At present, the information sector can be associated with them. The analytical layers determine the level of detail and include the international level up to the individual level. All relevant facts that describe the security environment are drawn into this map. These can be security problems, reference objects, threats, and factors. Relations between elements can be part of the model. [1]

The conceptual model is most appropriate for converged security. The system view can also use.



Security environment

security sectors →

analytical levels ↓	military	economical	political	societal	environmental
international (system)					
regional (system)					
state					
regional					
individual					

Fig. 2 Blind Map of the Security Environment [1].

4. Structure of conceptual model

Within the RECOS project focused on converged security, the author addressed the problem of creating a model of security environment. After a longer discussion, the conceptual model was chosen. This model was used to analyze and understand the safety and security assurance of reference models such as railway station, town hall, electrical station and university campus. In each conceptual model, the reference object was described by:

- *name and type of reference object,*
- *characteristic of the reference object, its determination,*
- *basic parameters and technical data of the reference object,*
- *assets of the reference object,*
- *process architecture,*
- *technology architecture,*
- *the system of protection,*
- *threats and risks of the reference object*
- *final evaluation.*

Name and type of reference object

The aim is to specify only the name and type of reference object. There is used the conceptual apparatus from the given field (public administration, transport, energy, soft targets). For example “Train station Přerov".

Characteristic of the reference object, its determination

The aim of the part is a short description of the reference object. Especially mention its purpose and aim function (what the reference object actually does). Then, verbally describe the object, including its topological structure. It will also describe its specifics and if it is an element of a higher whole (especially transport, energy), then its role, or priority in a higher whole.

Basic parameters and technical data of the reference object

The aim is to present the basic performance, spatial, technological parameters of the reference object. Parameters shows the aim function, to identify the impact of harm. The description of topological structure of the reference object will also be part of the description.

Reference object assets

The chapter identifies the basic assets of the reference object to be protected. That assets should be linked to the object's aim function. Examples of assets are passengers, employees, buildings, data, etc.

Process architecture

The aim of this chapter is to identify the process structure and create a process model of the reference object. In logical continuity from input to output, filling the aim function of the reference object. Processes should be divided into major and supportive processes. This scheme will be the basis for identifying technologies that fulfill the aim function. It will also be linked to operational safety.

Technological architecture

The aim of this section is to describe the technologies implementing processes (activities) to fulfill the aim function. Failure of technology can jeopardize the aim function of the reference object, and therefore it will be important to play a role in the reference object. Separate technologies (technological units) should be described by basic features, including technical and performance parameters. It is also good to indicate structure of reference object, if it is point, line, area or polygon. At the same time, it should be stated on which technologies they depend and what depends on them (description of correlation). A description of the control system and the information system will play an important role. Descriptions of these systems will form the basis for the cybersecurity of the reference object.

Technological architecture

The aim of this section is to describe the technologies implementing processes (activities) to fulfill the aim function. Failure of technology can jeopardize the aim function of the reference object, and therefore it will be important to play a role in the reference object. Separate technologies (technological units) should be described by basic features, including technical and performance parameters. There should be depicted topological structure of reference object, if it is point, line, area or polygon. At the same time, it should be stated which technologies are key. A description of the control system and the information system will play an important role. Description of these systems will form the basis for the cybersecurity of the reference object.

System of protection

The aim of the chapter is to describe the basic structure of the reference element system of protection. The aim of the converged security is to describe the basic parameters of the installed physical security system, the cyber security system, the operational security system. It should be clear from the description how this kind of safety and security is ensured, what technologies are used for it, and what data (demascating symptoms) can be obtained from sources of information, detectors, sensors.

Threats and risks of the reference object

The aim of this chapter is to list the threats that the reference object will face in area of physical security, cyber security, and operational security. Subsequently, a risk analysis will be conducted to identify key risks. Typical disruption scenarios will be described for the selected threats, showing how the security breach in the reference object will pass over time, how it will cause a reduction of functionality and harm or negative impact.

This conceptual model of reference object gives an overview of its nature, purpose, mode of operation, technologies, etc. Further on assets, threats, and security assurance. The created conceptual model allows us to understand the current state of security, resilience and vulnerability. Thanks to the depth of the description, it allows to identify correlations in the reference object. The model is the basis for long-term improvement of safety and security. Any significant change should be included in the conceptual model or updated so that the model reflects the current state.

Conclusion

Understanding of the security environment is essential to ensuring security and safety. This also applies to converged security. Converged security is a combination of multiple selected kinds of safety and security into one unit. Introducing converged security into an organization requires its well-known security environment. One of the tools for a formalized description of the security environment is the conceptual model. The conceptual model is the document in which the reference system is described. The content of the description consists of object characteristics, object architecture, technology, assets, protection system and threats. Creating a model will allow to understand how security is provided, what determines resilience and vulnerability. Such a document should be continually updated according to the development of the security environment to reflect the real situation. By changing staff, new security managers will be able to understand how security is ensured and what the advantages and disadvantages of securing are.

Acknowledgment

This work was supported by the Ministry of Interior project No. VI2017209054 „ An analytical software module for the real-time resilience evaluation from point of the converged security" solved in 2017 – 2019.

References

[1] LUKAS, Ludek. *Theory of Security I.* Zlín: Radim Bačuvčík - VeRBuM, 2017. ISBN 978-80-87500-89-7.

[2] HOFREITER, Ladislav. *The Security Environment of the Contemporary World*. Zlin: Radim Bacuvcik - VeRBuM, 2016. ISBN 978-80-87500-79-8.

[3] BUZAN, Barry, Ole WAEVER and Jaap de WILDE. *Security: a new framework for analysis.* London: Lynne Rienner Publishers, 1997. ISBN 978-1555877842.

[4] HOFREITER, Ladislav. *Object Protection Management.* Zilina: EDIS, 2016. ISBN 978-80-554-1164-4.

[5] SMITH, Clifton, BROOKS, David. *Security Science: The Theory and Practice of Security*. Walthman, MA: Butterworth-Heimann, 2013. ISBN 978-0123944368.

[6] HOFREITER, L., MARIS, L., LUKAS, L., KISTER, L., GRZYWNA, Z. New approaches to the analysis of the security environment and their importance for security management. In: *Communications - Scientific Letters of the University of Zilina*, vol. 17, no. 1, 20115, p. 99-104.

[7] HROMADA, M. Security models. In: *Kosicka Bezpecnostna Revue*, vol. 2015, no. 2, p. 118-127.

Author:

[1]**Ludek Lukas –** Tomas Bata University in Zlín, Czech Republic, e-mail: lukas@utb.cz