INFORMATION SECURITY RISK ESTIMATION FOR CLOUD INFRASTRUCTURE

A.V. Tsaregorodtsev[1], O.Ja. Kravets[2], O.N. Choporov[2], A.N. Zelenina[3]

[1] Moscow State Linguistic University, [2]*Voronezh State Technical University,* [3] Voronezh Institute of High Technologies
e-mail: csit@bk.ru
Russian Federation

Abstract: Due to the fact that cloud computing bring with them new challenges in the field of information security, it is imperative for organizations to control the process of information risk management in the cloud. This paper proposes a risk assessment approach for assessing the potential damage from the attack on the implementation of components of confidential data and justify the need for the inclusion of private clouds with a high degree of protection in a hybrid cloud computing environment. Suggested approach to information security risk estimation allows conduction of cloud environment security functioning in conditions of considered vulnerability class influence and also an effectiveness of measure and facility complex to withstand these vulnerabilities. On the basis of received estimation an opportunity to choose between different variants of cloud computing environment configuration and choose more appropriate way according to security requirements arises.

Keywords: cloud computing, information security threats, information risk analysis, information security requirements.

1. INTRODUCTION

The analysis of possible threats and risk analysis are the basis for the choice of measures to provide information security of cloud computing systems, which must be executed to decrease risk to accessible level [1, 5, 6].

While a quantitative risk assessment is widespread in some spheres such as finances and credit, a quantitative risk assessment in information security is usually accompanied by a row of restrictions where the absence of data for verification of these methods takes a special part [2, 3, 4].

Suggested approach for risk analysis and management will allow to make reasonable decisions when choosing information security systems, software for components of information systems (IS), functioning on a basis of cloud computing technologies [20, 21].

2. FUNDAMENTALS OF QUANTITATIVE RISK ASSESSMENT METHOD

Let us define key concepts which will be used in the suggested approach. The vulnerability is a software defect or a weakness in the security system, which can be exploited by third parties to cause damage or harm to an organization [2, 3, 4, 13]. Known vulnerabilities are vulnerabilities, which either have no bug fixes or have bug fixes applied with a time delay. The security threat is a potential objectionable event in the object of assessment, which can lead to a successful use of exploit with unwanted influence on confidentiality, integrity and availability of assessment object assets. The result of vulnerability exploitation by any threat can be appearance of an unwanted event, which is called the malicious use [2, 3, 13]. It is worth to be noticed that malicious uses can appear only with the existence of threat as well as of vulnerability and concerned vulnerability can be exploited by a certain threat. It means that a multiplicity of all potential malicious uses is the subset of both vulnerability list and potential threats list. Consequently, where M – malicious events list, ST – threats multiplicity, SV – vulnerability multiplicity.

Let us present the qualitative risk assessment method in the form of the following steps (table 1).

Table 1. Qualitative information security risk assessment method

№	Step description	
1	**Risk identification**	
	1.1	Identification of information security risks and influence on assets
	1.2	Identification of assessment object vulnerabilities, provision principles, processes, procedures and security environment
2	**Risk analysis**	
	2.1	Influence level estimation of malicious use
	2.2	Frequency estimation of malicious use
3	**Risk assessment**	
	3.1	Risk level definition for each list of frequency and influence
	3.2	Risk assessment and comparison with criterions of risk acceptance
	3.3	Risk categorization for processing into lists of risks
	3.4	Internal relations definition between risk lists
	3.5	Identification of conflicts between risk lists
	3.6	Appointment of priority list and risks
	3.7	Solution of found conflicts
4	**Risk processing**	
	4.1	Identification of alternative decisions for security provision and their grouping into lists
	4.2	Effect identification and targets of alternative systems of information security (ISS)
	4.3	Estimation and search of optimal ISS or decision list for security ensuring

On the top level suggested approach to risk estimation includes two general steps. First step describes an analysis managed by risk which includes malicious use list and connected with it risk levels estimation, which are the result of steps 2, 3 of suggested method with the following comparison of received data with criteria of risk acceptance which are defined at the first step. The result of this phase is a list of risks requiring processing [9].

Processing risk list, alternative decision list and other compromise parameters appropriate to the development, project or financial condition are the input data for the second step of the method, in frames of which information security risks are problems and challenges requiring decision in the form of available alternative security mechanisms [9].

Described under the first step actions include key analysis elements: threat list, vulnerabilities, malicious use, its frequency and influence, information security risk, risk acceptance criterion [7, 8, 13]. Figure 1 describes key essences and their relations of the first step of risk assessment approach. All these constituents are necessary for evaluation of estimation object risk level and its assessment focusing on comprehension of what risk requires processing [18].

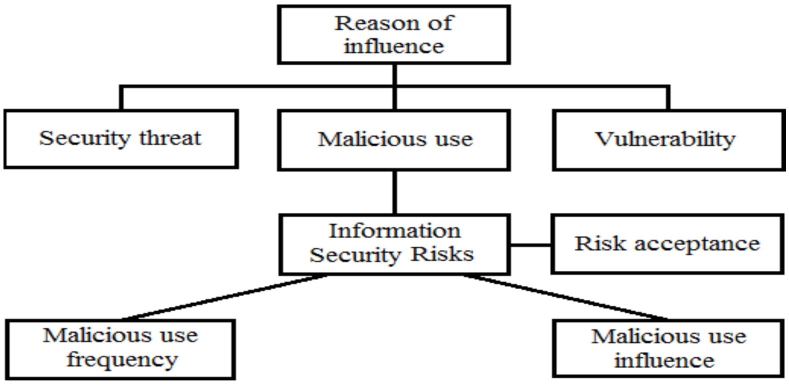

Figure 1. Indexes for risk level calculation in frames of the first step

Herewith a risk is calculated for every malicious use by means of combination of its frequency with one of influences. It means that malicious use leads to appearance of one or many information security risks depending on amount of interconnected factors (frequency and influence). Both indexes (frequency and influence) can be defined with quantitative estimation metric basing on data from public sources, one of which is NVD Common Vulnerability Scoring System Support (CVSS) [14].

The frequency of malicious use and its influence can be presented in the form of quantitative indexes: certain number of appearances during time interval or possibility of malicious use appearance in certain time period. The influence can be presented in the form of financial reputation losses [10, 12].

3. DEFINITION OF MALICIOUS USE FREQUENCY AND CORRESPONDING INFLUENCE ON THE BASIS OF CVSS

We use general prepositions of CVSS method for definition of two key variables influencing on risk estimation [14]. For this purpose let's combine indexes of basic, temporary and infrastructural metrics in a special way. The higher level of vulnerability to exploit use the more chances an attacker has to provide a successful attack and the higher is the index of malicious use frequency (F). Let us calculate this index for every vulnerability presented in the risk model of a cloud environment with assumption that fundamental vulnerability characteristics are described by the basic metric, and an index accounting of temporary metric will allow to decrease the probability of successful exploit use. The same principle is referred to the damage (influence): potential damage depends on confidentiality, availability and integrity requirements defined in infrastructural metric.

Tables 2 and 3 describe indexes chosen for analysis with corresponding CVSS weights.

Table 2. CVSS indexes for malicious use frequency calculation

Metric group	Index	Index meaning	Weight
Basic	Access vector (AV)	Local access (L)	0,395
		Adjoin network (A)	0,646
		Network (N)	1
	Complexity vector (AC)	High (H)	0,35
		Medium (M)	0,61
		Low (L)	0,71
	Authentication (Au)	Reusable	0,45
		Disposable	0,56
		Absent	0,704
Temporary	Indexes of code and exploit techniques availability (Au)	Theory (no proof) (U)	0,85
		Experiment (POC)	0,9
		Functional (F)	0,95
		High (H)	1
	Indexes of solution readiness level (RL)	Official patch (OF)	0,87
		Temporary decision (TF)	0,9
		Decision based on advice or recommendations (W)	0,95
		Absent (U)	1
	Indexes of information reliability level (RC)	Conjectural character (UC)	0,9
		Unregulated (UR)	0,95
		Accepted (C)	1

Table 3. CVSS indexes for malicious use influence calculation

Metric group	Index	Index meaning	Weight
Basic	Influence on confidentiality (C)	No (N)	0
		Partial (P)	0,275
		Complete (C)	0,66
	Influence on integrity (I)	No (N)	0
		Partial (P)	0,275
		Complete (C)	0,66
	Influence on availability (A)	No (N)	0
		Partial (P)	0,275
		Complete (C)	0,66
Infrastructural	Confidentiality requirements (CR)	Low (L)	0,5
		Medium (M)	1,0
		High (H)	1,51
	Integrity requirements (IR)	Low (L)	0,5
		Medium (M)	1,0
		High (H)	1,51
	Availability requirements (AR)	Low (L)	0,5
		Medium (M)	1,0
		High (H)	1,51
	Concomitant potential damage (CDP)	Low (L)	0,1
		Low-Medium (LM)	0,3
		Medium-High (MH)	0,4
		High (H)	0,5

3.1. Definition of malicious use frequency.

Using of three basic metric indexes and three temporary metric indexes allows evaluating malicious use frequency (how often vulnerability is the subject to exploit influence). Basic metric describes vulnerability characteristics and its liability to exploit influence because these indexes are chosen for determination of primary frequency.

$$F_{н} = \int P(AV, AC, Au). \quad (1)$$

It is considered that the primary frequency can be updated. Temporary metric indexes include indirect factors of vulnerability in question. Update consists of two steps: calculation of update factor (UF) (2), then this factor is used for the primary frequency to estimate total exploit use frequency (3).

$$F_{UF} = \int P(E, RL, RC), \quad (2)$$

$$F = \int (F_{н} \times F_{UF}). \quad (3)$$

Then received estimation must be normalized to receive values within interval [0; 1], what allow interpretation of received values as it is presented in table 4.

Table 4. Values of exploit use frequency

Value	Interpretation
0	Vulnerability is unavailable for exploit use
[0; 0,5]	Opportunity to use exploit is low
[0,5; 1]	Opportunity to use exploit is high
[1]	Vulnerability will be used accurately

3.2. Detection of damage under successful use of exploit based on basic and infrastructural metric.

Let us introduce new index I, which will describe damage to an organization with successful realization of exploit. This index will also be used for vulnerability grouping into a certain transitional model condition in the form of service level. For this purpose it is considered to use three attributes of basic metric (C, I, A) and four attributes of infrastructural metric (CR, IR, AR, CDP), the description is presented in table 3. Infrastructural metric indexes depend on vulnerability use context specific; include possible damage to confidentiality, integrity and availability in a cut of security requirements and potential concomitant damage of certain model condition. Basic metric indexes describe a value of effect on every certain security component, which subsequently is considered in frames of a certain context of infrastructural indexes. Similarly to index of exploit use frequency, basic metric is used for evaluation of primary damage, which represents vector of confidentiality integrity and availability:

$$I_{нач} = [C, I, A]. \quad (4)$$

Infrastructural metrics are used for updating primary damage to receive resulting estimation on vector components. Updating consists of two steps: Firstly security component vector is updated by the index of concomitant potential damage:

$$I_{CDP} = \int CDP[C, I, A]. \quad (5)$$

Then estimation vector is updated by a security requirement data received in the infrastructural metric:

$$I_{ENV} = [CR, IR, AR]. \quad (6)$$

Resulting vector is described by the following expression:

$$I = \int I_{CDP} \times I_{ENV} . \quad (7)$$

Index calculated by the formula (7) represents the seriousness of concerned vulnerability. Exactly this information is necessary for detection of required service level and for vulnerability assignment to service level during risk-model description.

3.3. Detection of service levels.

Let us represent service levels in the form of condition transition model (Markov process). The first condition represents the absence of damage to confidentiality, integrity and availability and can be described in the form of [0,0; 0,0; 0,0]. The last condition represents maximum damage to confidentiality, integrity and availability taking into account infrastructural metric indexes. Condition [1,0; 1,0; 1,0] is absorbing condition and describes the absence of opportunity to use patch in frames of the model. Thus the first condition corresponds to complete service level SL0, the last represents the absence of service SLx. All conditions between boundary levels can include complete service list as well as any number of services with lower level or the absence of services depending on the model in question [9, 11, 15].

4. DEFINITION OF RISK LEVEL BASING ON DAMAGE AND FREQUENCY INDEXES

For risk level dimension let us introduce a notion of service level presented in the form of Markov process with continuous time. Service levels depend on project decision and information system' realization variant functioning on the basis of cloud computing technologies, framework of such information system and application list, in other words on the way of information system' using.

Firstly we define a vulnerability list according to public data, for example to official messages about vulnerabilities, databases (NVD) or by launching special scanner (Nessus).

As it was already mentioned, the damage from successful exploit use describes a seriousness of the vulnerability. But this does not mean that two vulnerabilities leading to the same damage have the similar seriousness level for described environment and lead to commensurate decrease of service maintenance. In this connection it is necessary to solve the task of vulnerability seriousness level intervals determination with the following determination of service levels for them. As a result we obtain service level list beginning with level without service presentation and ending at complete service list, described in the form of condition model. Service level we define as not empty list of vulnerabilities having influence level from the same interval.

Secondly condition transition model is explored, which was received during the first step and is supplemented by transition intensity. The transition intensity defines the opportunity when a transition from one condition to another is possible and with what probability it is possible to be in this condition at a certain time interval t. In the risk level estimation model every condition refers to the total level of vulnerability list seriousness. Thus a condition transition model describes different risk levels typical for considered environment at the moment of time t. For definition of transition intensity it is necessary to consider aggregate frequency of exploit use at the certain time interval.

5. CONCLUSIONS

Suggested approach to information security risk estimation allows conduction of cloud environment security functioning in conditions of considered vulnerability class influence and also an effectiveness of measure and facility complex to withstand these vulnerabilities [16, 17]. On the basis of received estimation an opportunity to choose between different variants of cloud computing environment configuration and choose more appropriate way according to security requirements arises.

REFERENCES

[1] Werner O. "Clouds", the virtual infrastructure and information security. M.: *"Elvis-Plus" Publish*, 2012.

[2] How to stay safe in the cloud storage. 06.03.2017. URL: http://topobzor.com/kak-obespechit-bezopasnost-v-oblachnyx-xranilishhax/.html.

[3] Kachko A.K., Lavrynenko M.M., Tsaregorodtsev A.V. The approach of secure hybrid cloud construction. *Safety of information technology*. 2014. #1, pp. 22-27.

[4] Security Issues cloud environments. URL: http://dehack.ru/news/2012_06_30_10_29_00.

[5] Radin P.K., Zubarev I.V. The main threats to the security of information in virtual environments and cloud platforms. *Cybersecurity*. 2014. 2 (vol. 3).

[6] Sidorova M. Conflicting Cloud. URL: http://www.itsec.ru/articles2/oborandteh/protivorechivie-oblaka.

[7] Threats to Cloud Computing and methods of their protection. URL: http://habrahabr.ru/post/183168.

[8] Winkler B. Cloud computing: security issues in virtual clouds. Adapted excerpt from the book "Securing the sloud" (Syngress, a division of the publishing house Elsevier). URL: http://technet.microsoft.com/ru-ru/magazine/hh641415.aspx.

[9] Tsaregorodcev A.V. Security risk analysis of data in corporate networks-bank financial institutions on the basis of cloud computing. *National interests: priorities and safety*. 2013. 39 (vol. 228), pp. 35-44.

[10] Tsaregorodcev A.V., Kachko A.K. Ensuring information security in cloud architecture of organization // *National Security*. 2011. #5. PP. 25-34.

[11] Tsaregorodcev A.V., Kachko A.K. One of the approaches to the management of information security in the development of information infrastructure // *National Security*. 2012. №1 (vol. 18), pp. 46-59.

[12] Accorsi R., Wonnemann C. Auditing Workflow Execution against Dataflow Policies. I*n Proc. BIS*, 2010. pp. 207-217.

[13] Mell P., Tim Grance T. The NIST Definition of Cloud Computing, Version 15, September 2011. URL: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

[14] NVD Common Vulnerability Scoring System Support v.2. (National Institute of Standards and Technology). URL: http://nvd.nist.gov/cvss.cfm?calculator&version=2.

[15] Trope R.L., Power E.M., Polley V.I., Morley B.C. A Coherent Strategy for Data Security through Data Governance. *IEEE Security & Privacy*, 2007, 3 (vol. 5), pp.32-39.

[16] Tsaregorodtsev A., Zelenina A., Ružický E. Methodology of vulnerability assessment for various types of cloud structures. *Information Technology Applications*, 2017, № 1, pp.51-59.

[17] Tsaregorodcev A.V. Classification of vulnerabilities of cloud environments in the problem of quantitative risk assessment/ A.V. Tsaregorodcev, A.N. Zelenina, V.A. Saveliev. *Modeling, optimization and information technology*, 2017, № 4 (19). URL: https://moit.vivt.ru/wp-content/uploads/2017/10/ZaregorodzevSoavtori_4_2_17.pdf

[18] Tsaregorodcev A.V. Two-stage procedure for quantitative assessment of information security risk of cloud computing/ A.V. Tsaregorodcev, A.N. Zelenina, V.A. Saveliev. *Modeling, optimization and information technology*, 2017. № 4 (19). URL: https://moit.vivt.ru/wp-content/uploads/2017/10/ZaregorodzevSoavtori_4_1_17.pdf

[19] V.F. Barabanov, O.J. Kravets, I.N. Kryuchkova, O.Y. Makarov, A.K. Pogodayev, O.N. Choporov. Discrete processes dynamics neural network simulation based on multivariate time series analysis with significant factors delayed influence consideration. *World Applied Sciences Journal*, 2013, № 23 (vol. 9), pp. 1239-1244.

[20] Aaron Zimba, Mwenge Mulenga. A Dive into the Deep: Demystifying WannaCry Crypto Ransomware Network Attacks Via Digital Forensics. *International Journal on Information Technologies and Security*, № 2, 2018, pp. 57-68.

[21] Orges Çiço, Zamir Dika, Betim Çiço. High Reliability Approaches in Cloud Applications for Business – Reliability as a Service (RaaS) Model. *International Journal on Information Technologies and Security*, № 3, 2017, pp. 3-18.

Information about the authors:

Tsaregorodtsev Anatoly Valerjevich - Doctor of Technical Science, Professor, Vice-rector for Education and IT of Moscow State Linguistic University, areas of scientific research - information security, Russian Federation
avtsaregorodtsev@linguanet.ru +7 (495) 6951420

Kravets Oleg Jakovlevich - Doctor of Technical Science, Professor**,** Voronezh State Technical University, Russian Federation
csit@bk.ru +7 (920) 4039886

Choporov Oleg Nikolaevich – Doctor of Technical Science, Professor, Voronezh State Technical University, Russian Federation
choporov_oleg@mail.ru +7 (473) 2205603

Anna Nikolaevna Zelenina – Candidate of Technical Sciences, Associate Professor of Voronezh Institute of High Technologies, Russian Federation
conference@vivt.ru +7(473) 272-76-74

Manuscript received on 28 August 2018