

Methodology of vulnerability assessment for various types of cloud structures

Anatoly Tsaregorodtsev, Anna Zelenina, Eugen Ružický

Abstract:

Today organizations increasingly consider cloud computing as an alternative way of using information technology. At the same time, the use of different vulnerabilities of infrastructure components, network services and applications remains are the major threat to the cloud. The article proposes a methodology of vulnerability assessment for any type of cloud structures, which will allow to determine the coefficient of counter to possible attacks and to correlate the amount of damage to the total cost of ownership of IT-infrastructure of organization.

Keywords:

Cloud computing, information security threats, attack, damage, system vulnerability assessment, factor counteracting.

ACM Computing Classification System:

Distributed architectures, Cloud computing, Distributed systems organizing principles, Cloud based storage, Information flow control, Security requirements, Formal security models, Distributed systems security.

Introduction

Practically all technologies, which nowadays are components of cloud paradigm, existed before, but until now there was no supply on the market, which could combine perspective technologies in the single commercially attractive decision.

Only at the last decade cloud services emerged thanks to which these technologies became on the one hand available to the developer and on another hand comprehensive to the business community [1, 2].

Cloud computing is economically effective from the point of total ownership cost that allows cost reducing of technical maintenance. The enormous part of annual budgets in the majority of IT organizations goes for maintenance and structural amortization without any new additional cost.

Nevertheless cloud computing is a new form of distributed calculations which is still rudimental. Using the cloud computing paradigm organization declines a direct control of many security aspects and thereby creates unprecedented confidence level to cloud provider what can have ambitious plans for development of federal agencies systems, education institutions and other state organizations [3, 4, 16]. But many of the features that make cloud computing attractive may be in conflict with traditional models of information security [5, 6, 13].

An opportunity to use different vulnerabilities of infrastructure components, network services and applications is still the main threat to cloud services [7, 8, 9]. This aspect is serious danger to public PaaS- and IaaS-models where management of vulnerabilities, configuration and update are in responsibility zone of cloud client. In public cloud environment (PCE) the total security level is distributed between participants of all multiuser virtual structure. On the one hand management responsibility of vulnerabilities, configuration and update (VPC) of infrastructure lies on the provider, on the other hand cloud environment clients should understand exactly those VPC aspects which they are liable for [14].

Let us consider management features of vulnerabilities, configuration and update in the cut of service submission models and responsibility zones between a provider and a client.

1 Management of vulnerability, configuration and update

The vulnerability management is an important possible threats control element for defence of the host, network devices and applications against attacks (Figure1). Organizations which care about information security provision introduce vulnerability management procedures consisting of standard scanning of systems connected to the network, risk analysis of vulnerability appearance and modification process for risk elimination. Organizations taking into account standard ISO/IEC 27002 use technical vulnerability management opportunities which bases on attainment principle of acceptable risks, arising during exploitation. The vulnerability management must be realized in the form of effective and systematic procedure with an opportunity to measure its effectiveness.

Similarly to vulnerability management, management of update and rectification is an important control element of possible threats on the level of host, network devices and applications where actions of unauthorized users are focused on exploitation of known vulnerabilities.

SaaS-providers must assess new vulnerabilities and correct hardware and software of every system which is distributed to clients.

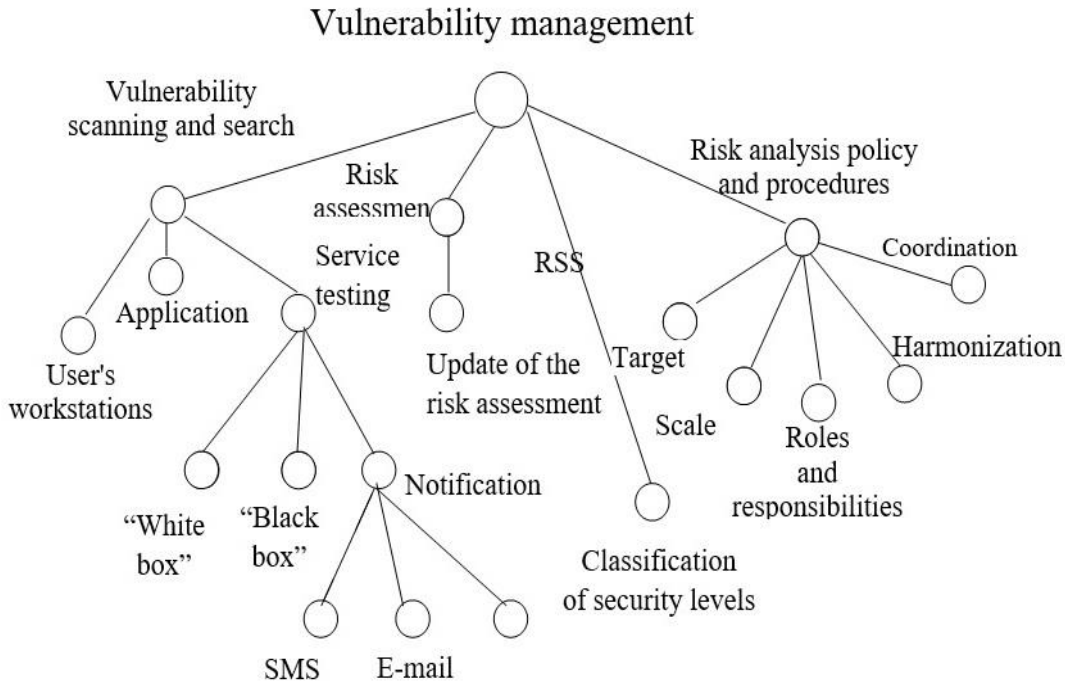

Figure 1. Vulnerability management target tree of cloud computing environment

Clients are free from update procedures in SaaS environment but are liable for patch management for full software stack (OS, applications, databases) installed and managed on IaaS platform. Clients are also liable for application rectification, deployed on PaaS platform.

Security configuration management is also one important aspect of threat management for network devices and units from unauthorized users, using every "narrow places" in the configuration (Figure 2). The defence of network configuration, node and application leads to control and management of access to critically important system and database of configuration files including OS, firewall, network options of local and remote data storage and database control [10, 12].

SaaS and PaaS service providers are liable for configuration management of their platforms, but IaaS clients are responsible for configuration management of OS, applications and databases.

2 Vulnerability estimation result analysis for different types of cloud environment

Using statistic information about main vulnerabilities of cloud computing environment let us calculate security level of every separate infrastructure based on metric «NVD Common Vulnerability Scoring System Support v.2» of the USA National Institute of Standards and Technologies [11, 15].

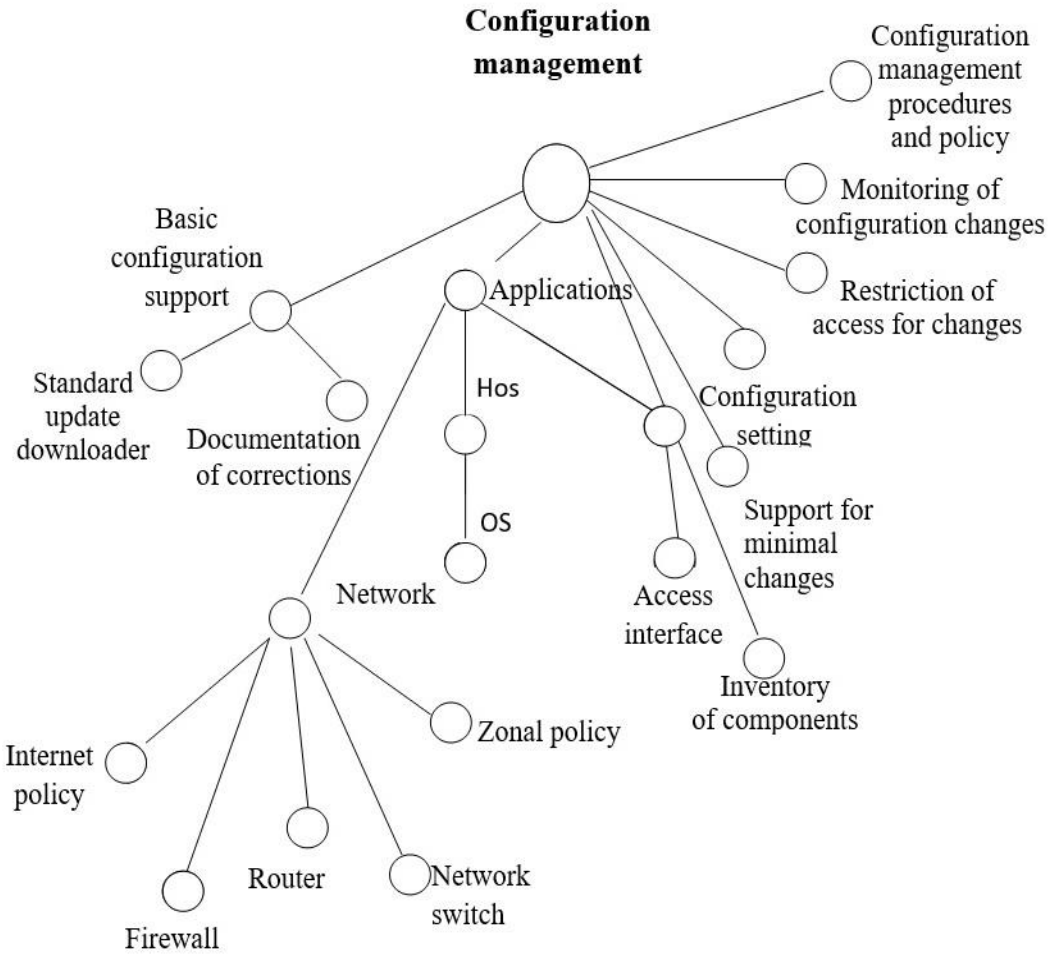

Figure 2. Configuration management target tree of cloud computing environment

The common vulnerability estimation system (CVSS) provides public architecture for obtaining of interconnections, features and vulnerability influence on IT-infrastructure in question. CVSS metric include calculations of three types: basic group, temporary group, environment factor [15]. Calculation result of every group is a numeric estimation from 1 to 10 and vector, consisting of a squeezed text description for received values.

Basic group presents internal characteristics of possible vulnerabilities. Temporary group presents vulnerability characteristics, which change with time passage. Environment factor group presents vulnerability characteristics which are unique for different environments. CVSS tools allow receiving the estimation of IT-vulnerabilities with different characteristics, including the estimation for different cloud computing environments. The CVSS metric list is presented on Figure 3 [15].

A result of vulnerability estimation according to CVSS method for private cloud environment (PCE), public cloud environment and hybrid cloud environment is presented in table 1.

Received estimations results of possible vulnerabilities for different cloud environments show that using of public cloud is inaccessible in case of critical data processing, so the golden mean is hybrid cloud environment.

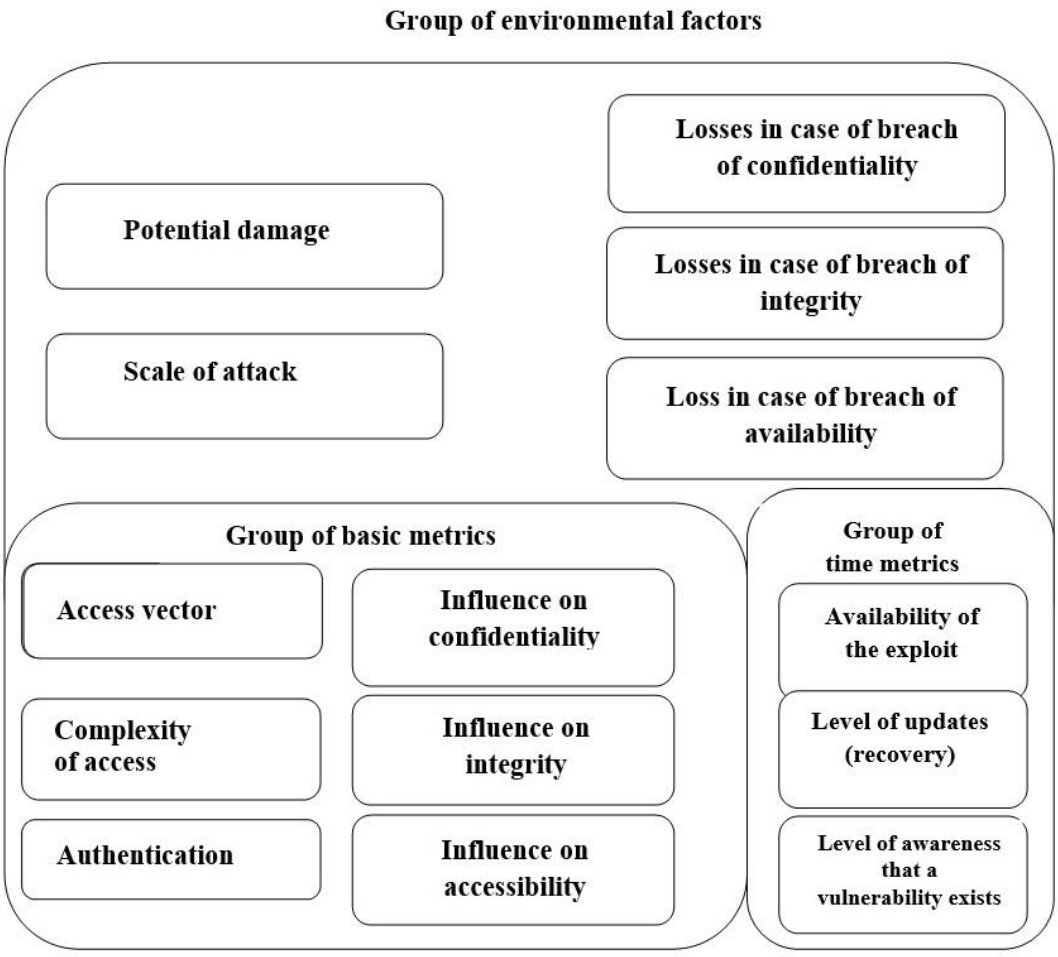

Figure 3. CVSS metric list

Table 1. Vulnerability estimation on the basis of CVSS metric

	PCE	**PrCE**	**HCE**
1 Basic metric group	9	3,4	7
1.1 Access vector	Public network	Local network	Hybrid network
1.2 Complexity of access	Low	High	Medium
1.3 Authentication	Single-factor	Multi-factor	Multi-factor
1.4 Confidentiality influence	Complete	Partial	Complete
1.5 Integrity influence	Complete	Partial	Complete
1.6 Availability influence	Complete	Partial	Complete
2 Temporary metric group	6,2	3,6	6
2.1 Exploit susceptibility	High	Functional	Functional
2.2 Update level (renovation)	Official fix (patch)	«Patch»	Temporary decision
2.3 Awareness level that vulnerability exists	Confirmed	Unverified	Confirmed
3 Environment metric group	6,1	1,5	2
3.1 Potential damage	High (Catastrophic damage)	High (Catastrophic damage)	High (Catastrophic damage)
3.2 Attack scale	High (25-75 % assets in danger)	Low (0-25 % assets in danger)	Low (0-25 % assets in danger)
3.3 Damage in case of confidentiality loss	High	High	High
3.4 Damage in case of integrity loss	High	High	High
3.5 Damage in case of availability loss	High	High	High
Total CVSS estimate:	6,7	1,5	2

Let us interpret the received results of vulnerability assessment into index of countermeasure to different vulnerability types basing on ratio that CVSS-estimation which is equal to 1,5 corresponds to 85 % security efficiency of cloud IT-infrastructure (table 2).

Table 2. Counteraction coefficient for cloud environments variants

Variant	Total CVSS estimation	Counteraction coefficient
PrCE	1,5	85 %
HCE	2	80
PCE	6,7	33 %

There are results of security mechanisms application in different cloud environments at the example of accident cost «Theft by unscrupulous employee of confidential information to which the access was not provided according to security policies (using privileges)» = 5 283 168,00 RUR (table 3).

Table 3. Counteraction coefficient for cloud environment variants

Cloud architecture variant	Effectiveness of confidential data security	Sum of saved money per 1 year, RUR	Damage value, RUR
PrCE	85 %	4 490 692,80	792 475,20
HCE	80 %	4 226 534,40	1 056 633,60
PCE	33 %	1 743 445,44	3 539 722,56

Provided experimental estimation of confidential data security effectiveness confirmed the necessity to apply additional methods of information security in examples in question for construction of cloud environment.

Conclusion

On the basis of common vulnerability estimation system, allowing estimation of information system exploit exposure considering environmental factors, a method of possible vulnerability estimation for different types of cloud environment is suggested.

The application of vulnerability estimation method for different types of cloud environment has allowed to reveal the coefficient of counteraction against possible attacks and correlate the damage value to total ownership cost of all IT infrastructure of an organization.

References

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

[2] Vlasov A. Overview protection in virtual environments // Jet Info. – 2012. – № 3.

[3] Vasiliev V. Security cloud environments // PC Week Review: IT Security, May 2012. URL: http://www.pcweek.ru/security/article/detail.php?id=139185.

[4] Protection clouds. URL: http://www.jet.msk.su/services_and_solutions/information_security/solutions_catalog/zashchita_oblakov_i_gadzhetov.

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

[6] 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.

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

[8] Radin P.K., Zubarev I.V. The main threats to the security of information in virtual environments and cloud platforms // Cybersecurity. – 2014. – № 2 (3).

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

[10] 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.

[11] 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 (228). – PP. 35-44.

[12] Tsaregorodcev A.V., Kachko A.K. Ensuring information security in cloud architecture of organization // National Security. – 2011. № 5. – PP. 25-34.

[13] 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 (18). – PP. 46-59.

[14] 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.

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

[16] 16. 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. – Vol. 5. – № 3. – PP. 32-39.

……

Anatoly Tsaregorodtsev
Doctor of Sciences (Engineering), Professor,
Dean of International Information Security Faculty,
Head of Information Security Department,
E-mail: AVTsaregorodtsev@linguanet.ru
Moscow State Linguistic University
119034, 38-1 Ostozhenka St., Moscow, Russia

Anna Zelenina
Candidate of Technical Sciences, Associate Professor,
Leading specialist of the project department,
E-mail: snakeans@gmail.com
Voronezh Institute of High Technologies
394043, 73A Lenina St., Voronezh, Russia

Eugen Ružický
Doctor of Sciences (Engineering), Professor,
Pan-European University, Bratislava, Slovakia
E-mail: eugen.ruzicky@paneurouni.com