Volume XXIII 2020
ISSUE no.2
MBNA Publishing House Constanta 2020

Scientific Bulletin of Naval Academy

SBNA PAPER • OPEN ACCESS

Methodology for ensuring computer security for vulnerable systems

To cite this article: Violeta Nicoleta Opriș, Scientific Bulletin of Naval Academy, Vol. XXIII 2020, pg.185-190.

Available online at www.anmb.ro

ISSN: 2392-8956; ISSN-L: 1454-864X

doi: 10.21279/1454-864X-20-I2-025

Methodology for ensuring computer security for vulnerable systems

Violeta Nicoleta Opriș
Ph.D., Teaching Assistant
Titu Maiorescu University Bucharest
violeta.opris@gmail.com, violeta.opris@prof.utm.ro

Abstract: Risk assessment is a process that provides cloud users with useful data for understanding the impact. We define a security incident as an event that attempts unauthorized access to databases. It is similar to an attack on the integrity and confidentiality of information.

1. Introduction

In this paper a methodology for incident management is proposed. It has been developed to define how to handle information security incidents within databases. Database security incidents detected by the innovative system after scanning are XSS attacks and SQL injections. These will be treated according to the severity level using the Create Knowledge Labels within the system.

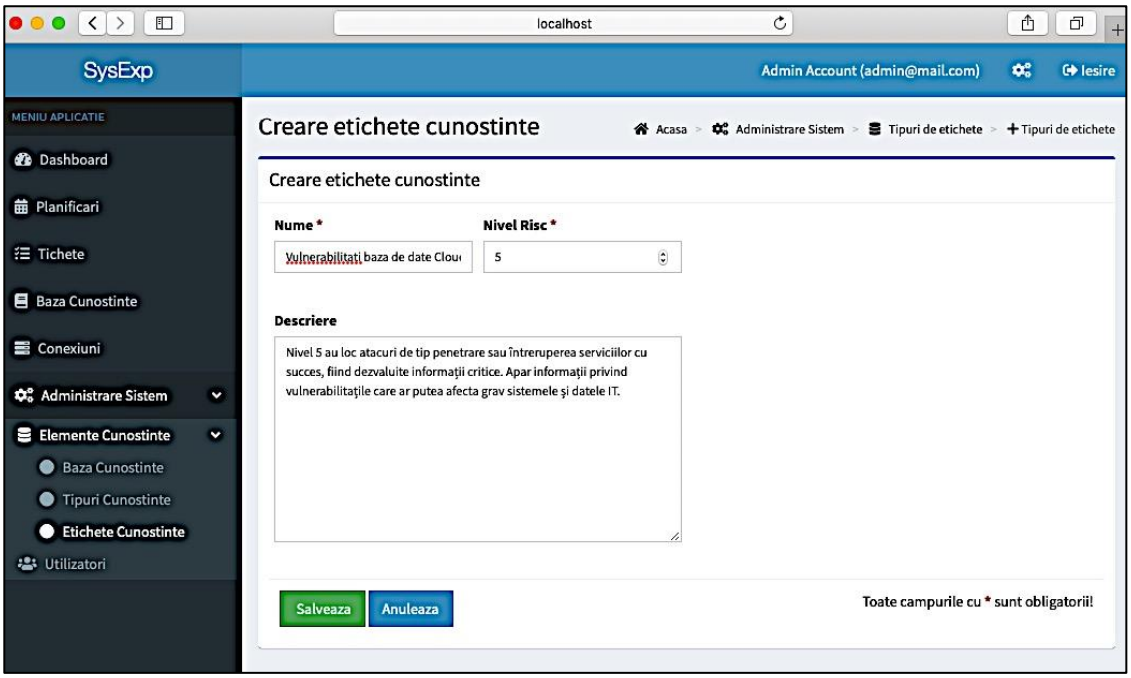

Figure 1. Create Knowledge Labels

Resolving incidents involves preparing, detecting, alerting, sorting, responding, recovering, and continuing. The purpose of the systematic approach to handling security incidents is to resume operations in the cloud as soon as possible. It is possible to keep incident information for analysis and to improve the overall security of the databases.

The preparation phase is the process of establishing policies, procedures and agreements regarding the management and response to security incidents. The alerting phase is the process of awareness of a potential security incident. Also, its reporting is part of this phase.

The sorting phase is the process of examining the available information regarding an event, to determine whether or not a security incident has occurred. The alerting phase is the awareness of a potential security incident and its reporting. The response phase is the process of trying to limit the proportions of a security incident.

According to the innovative attack management system on the databases, the levels of security incidents are described as follows (Figure 1) [1]:

- Risk level 1: a small number of samples are discovered. There are isolated cases of XSS attacks and SQL injections, which are eliminated by the innovative system designed;
- Risk level 2: this involves an unusual increase in XSS attacks and SQL injections. Vulnerabilities also occur, without the presence of an incident that would cause database disruption;
- Level 3 risk: the number of samples and scans of databases increases. Service interruption attacks, such as SQL injections, are discovered without causing an impact on normal services;
- Level 4 risk: penetration attacks occur, with limited impact on operations. Information is disclosed which could represent a risk from the point of view of the organization's image;
- Level 5 risk: successful database penetration or interruption attacks occur, critical information being disclosed. Vulnerability information appears, which could severely affect cloud services and limited data.

This paper has been elaborated to state the consequences of the attacks that occur every day in the cloud, but also to show the risks that may occur during the functioning of the innovative system. Figure 2. identifies the risk factors and how to deal with the problems, including assigning them to those responsible.

2. Consequences for information risks

This section has been elaborated to state the consequences of the attacks that occur every day in the cloud, but also to underline the risks that may occur during the functioning of the innovative system. Figure 2. identifies the risk factors and how to deal with the problems, including assigning them to those responsible.

This section is used to make decisions regarding the measures to be implemented, in order to reduce the level of risk existing in the databases detected to be vulnerable and to keep these risks at an acceptable level.

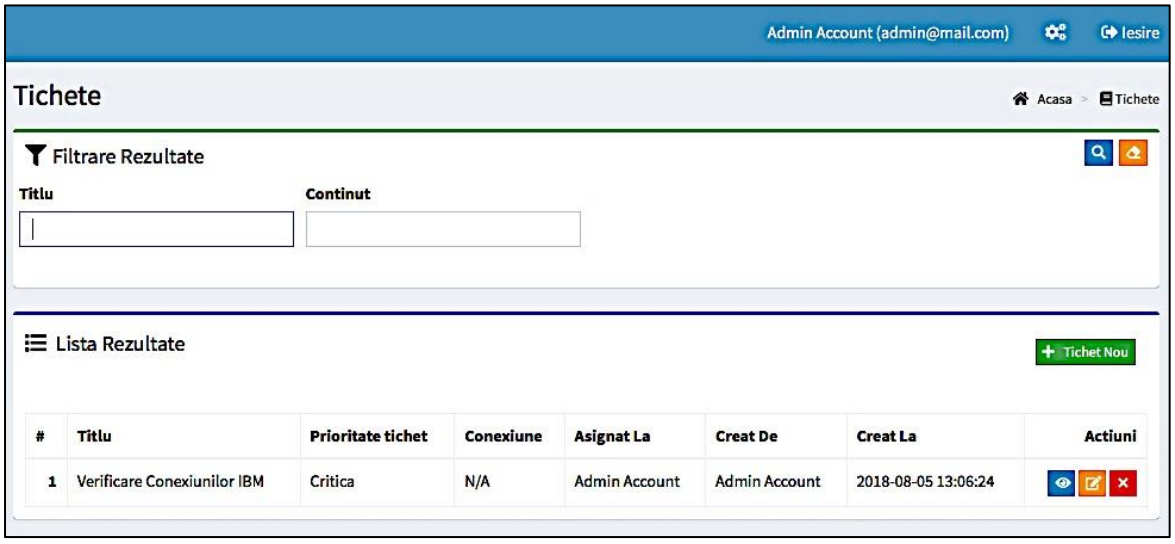

Figure 2. Risk assessment - Ticket mode

Risk assessment involves monitoring the likelihood of materialization of risks and the impact on cloud centers if they materialize. The probability of risks is estimated as follows:

- Reduced 1: it can manifest itself in the next three years;
- Average 2: it can manifest itself in the next two years;
- High 3: it can manifest itself in the following year.

The following are the risk factors that may appear in the cloud, the treatment method and the responsible person:

- Fires: backing up secret information from databases - cloud administrator;
- Access of unauthorized persons: video monitoring systems and third party legitimation when entering data centers - represented by security management;
- Improper use of information: information security training in data centers - represented by security management;
- Theft of information: confidentiality agreements will be drawn up - the director of the cloud center;
- Failures of cloud equipment: training of data center personnel and maintenance of equipment - cloud administrator;
- Loss of restricted information resources: backup to another cloud location - represented by security management;
- Emergency situation production: documentation of emergency plans for all emergency situations that can intervene at cloud level - represented by security management;
- Use of legal requirements: implementation of measures to restore the cloud and permanent updating of the legal - legal database;
- Insufficient staff: business continuity plan - representative of security management;
- Hardware failure of cloud systems: detailing the business continuity plan - network administrator;
- Compromising the communication infrastructure: testing the business continuity plan - representative of security management;
- Adopting the wrong decisions: training the personnel regarding the compliance with the provisions of the documents of the integrated management system - representative of the security management.

3. Security mechanisms for intrusions identified in databases

In this section, security vulnerabilities are proposed for vulnerabilities detected using the innovative system. These can be used individually or in combination. In order to increase the security level in virtualized systems, the following mechanisms are proposed:

- Encryption: modifying the data so that it can only be understood by authorized users of data centers;
- Access control: monitors the access of entities to cloud resources;
- Data integrity: ensures the integrity of the information units;
- Authentication: it is used to prove the identity of the users;

- Traffic filling: provides separate levels of defense against traffic analysis;
- Routing control: allows you to choose the most acceptable routes according to the security criteria;
- Notarization: determining a third party with the role of providing guarantees regarding data integrity.

4. Database security

The security of the database of the innovative system used in intrusion detection involves ensuring control over how it is accessed and used. This includes system security and data security.

System security involves mechanisms that monitor system entry and database usage. Data security involves mechanisms that monitor the entry and use of the database at the object level.

The architecture of the innovative system, including the database, will not be installed in the cloud virtualized data center, thus ensuring an optimal operating environment of the innovative system. The architecture is flexible and allows the installation of the future system also in the cloud if necessary.

It also connects to external systems through secure SSL connections to provide security for the data being transported or retransmitted (Figure 3.). SSL provides secure end-to-end connections and authentication of the connection between two network points.

The innovative system does not collect confidential information after trying to detect intrusions, but analyzes them using the algorithm, then they are deleted.

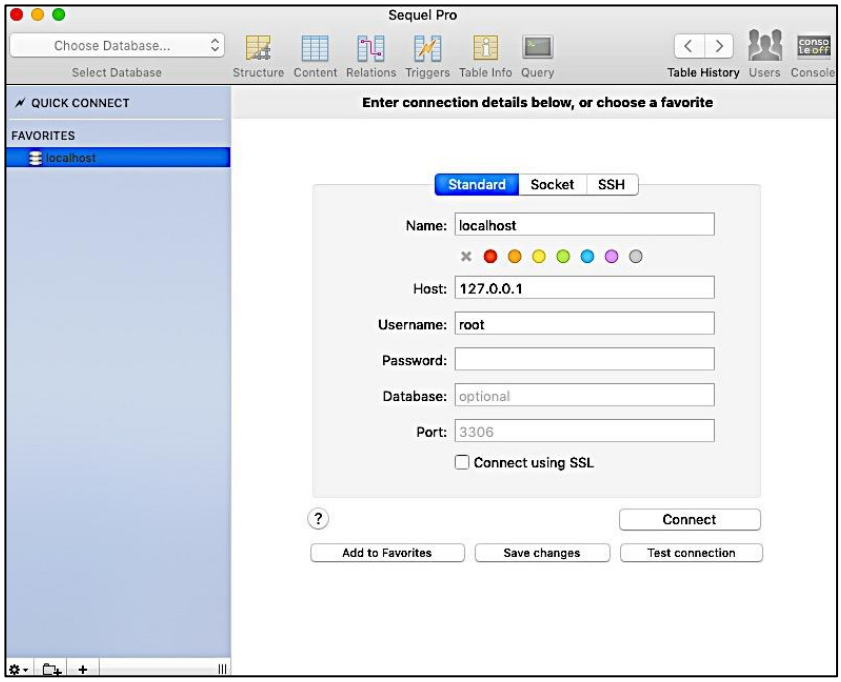

Figure 3. Database connection

5. Conclusion

The innovative management system for detecting database intrusions for systems in different locations in Cloud computing is scalable and will meet security requirements. The simulation was performed on the datacenter from the central location of the IT company, the infrastructure being completely classic. The system will not work in the cloud in test scenarios.

Innovative systems are a sub-branch of artificial intelligence technology. Taking into account the presentations of existing knowledge-based innovative systems, we can mention several advantages of them: they are databases with valuable information, they are useful in the absence of human expertise, they can be updated and expanded quickly, they can provide explanations in some cases.

The modules of the innovative system can be used according to the rights of the users, having an optimal flow of use. From the point of view of the algorithm, it has the ability to analyze and detect the vulnerabilities of a database. It also offers the possibility of extension according to the desired needs, in several cases. For example, the proposed system checks databases for two cases, if XSS attacks and SQL injections have occurred.

References

[1] Opriş,V.N., Building and modelling a sustainable expert system, using UML language, The 4th International Conference Sea-Conf, Academia Navală Mircea cel Bătrân, Constanța, 2018

[2] Dumitru, L.A., Eftimie S., Mihăilescu, M.I., Niță, S.L., Opriș,V.N, Răcuciu C., A Novel Architecture for Authenticating Scalable Resources in Hybrid Cloud, The 11th International Conference on Communications, București, 2016

[3] Opriş,V.N., Opriș,M.E., The expert system development technologies in cloud, The 3rd INTERNATIONAL CONFERENCE SEA-CONF, Academia Navală Mircea Cel Bătrân, Constanța, 2017

[4] https://getbootstrap.com

[5] https://www.php.net

[6] https://getbootstrap.com

[7] https://laravel.com