MONITORING AND CONTROLING THE ACCESS TO CLASSIFIED ECONOMIC DATA

ȘERBAN Mariuța[1], ȘTEFAN Raluca-Mariana[2], HURLOIU Lăcrămioara-Rodica[3]

[1] Doctoral Studies, Pitești University, Pitești, Romania
[2] Institute of Doctoral Studies Academy of Economic Studies, Bucharest
[3] Faculty of Financial Accounting Management, Spiru Haret University, Bucharest

***Abstract**:*

The need for information security level becomes more stringent, the number of companies that need secure channels increases and the number of people seeking information security is becoming more and research programs have arisen regarding security.

Regarded as an activity, control is reflected in researchers' attention for centuries while the current literature control is seen as one of the most important managerial functions.

As market economic relations were amplified, business managers are increasingly forced to address process control, process will have a direct impact on the future of the company. Control point conceptually covers all company activities. Making rational monitoring and control system within an institution is one of the most important activities.

***Keywords**:* security, authentication, authorization, access control, data classification

***JEL Classification**:* A12, C15, C38, C52, C53, C63, C88, E22, M41

[1] *Assistant Professor Ph.D. Student, Doctoral Studies, Pitești University, Pitești, Romania, mariuta_serban@yahoo.com*
[2] *Assistant Professor Ph.D. Student, Institute of Doctoral Studies Academy of Economic Studies, Bucharest, Romania, rstefan2012@yahoo.com*
[3] *Associate Professor Ph.D., Faculty of Financial Accounting Management, Spiru Haret University, Bucharest, Romania, hlacra@yahoo.com*

1. Introduction

To ensure security in an enterprise the security policy must be specified for the entire organization. The security rule is a policy of both the organization and management of information systems; it is considered a policy of information and marketing. It is good to establish first the security solution methods in some cases including risk analysis. An important part of security policy is the responsibility of every employee.

Any economic society whose data are stored in the database is set for different business relationships and they rely on trust between business partners. In achieving effective relationships it is the key to ensure data security and data groups.

Confidentiality is a crucial factor to protect the reading of certain economic documents such as invoices, conditions of sale or tariffs.

Data integrity is a major special factor in confidence; integrated data could not be altered or destroyed without authorization, which can be accessed only by authorized persons.

To ensure proper data security for data groups and databases it must be very well understand the fundamental concepts (what data must be protected and the possible attacks on them) in order to know technical details (operating systems, networking, programming and cryptography) and think like an attacker.

In order to implement a security model data from databases you should know and understand the importance of each security concept.

Authentication is the process of validation of a person from whom it determines whether it is allowed access to data in data base. Typically, authentication is done by placing the person in question has a user name and password. For better security in terms of authentication can be used for user password encryption techniques. In other words, the authentication process verifies the user's identity.

After authentication process begins authorization process. Authorization is the process that controls access to data; each user has the right to access only certain data for different criteria. Authorization does not require safe storage of user names and passwords nor outgoing ensure the security of the Internet.

To protect their data transfer or if authorization is not sufficient then

another concept of security, cryptography is used. Cryptography is the process of encoding data which makes them unreadable by an individual who does not have the encryption key.

A third method of verifying an individual or a trust company is using certificates. Certificates contain some information of the person wishing to access data, such as name, address, contact, industry, and the public key used for encryption even when checking signatures.

Using certificates to verify that a person is who he claims to ensure data security by using encryption technology transfer channel of communication, most often this is performed using certificates. Certificates content is verified by the certification authority (CA) that has the confidence of both parties to exchange information.

2. Unsupervised classification of data

In order to easily identify natural groups of data from a large set of data it exist the notion of classification of data. Classification of data is splitting the dataset into groups, clusters or classes of similar data are a fundamental data analysis method.

Division into classes is based on a set of features describing each object, time, resource.

Classification of data is used for pattern recognition, vector quantization, image segmentation, function approximation.

The action of classification identifies internal structures available for a variety of objects using a similarity measure. After grouping the data to obtain a fixed structure data are well determined to form groups that have a degree of membership for each object.

Knowing the sets of input and output data a model of the system can be developed, one of the methods used to identify the grouping data systems.

In the action of data group data should pursue two characteristics:

- Uniformity in group classes is as high similarity between objects of the same group;

- Heterogeneity between classes as large groups is the difference between objects in different groups.

The distance between objects computed is considered to be the best measure of similarity between objects.

The action of grouping data, i.e. clustering, is the discovery of classes and data structures that are alike a whole set of data without involving data structures already known. Simply, it can say that the group is sharing data objects into clusters (groups).

Data classification is a generalization of known structure can be applied to other data. In other words, data classification assignment of a new object is one of the groups.

3. Attacks, vulnerabilities and security risks in economic databases

The notion of data security or classified data security represents banning access to certain data of different users or groups of data. This can be done by imposing two types of restrictions: restrictions on reading data or groups of data intelligence and data restrictions on modification of unauthorized users.

When data security or data groups are involved it refers to both intentional actions and random actions that are performed on certain resources, which are conducted by a person appointed attacker.

The security attack is any action on certain resources that compromise their safety.

According to specialists theories of attacks can be divided into three general models:

- Access users - the system requires access to privileged users. This type of attack requires the following steps:

a) Obtaining information is automated process tools aimed at a specific application, thorough search to identify security vulnerabilities. Vulnerabilities can be found in components and may occur due to leakage of system administrators or security poor policies.

b) Operation of a security breach for specific information system for their use in future attacks. Examples of such information are computer name or names of user accounts.

c) Damage is a result of the effects to be achieved after an attack. These include: modifying data or groups of data access certain information secret organization achieve permanent connections to view documents.

- Access components - an attack does not require access to a user's system. This type of attack sends improper requests after which the system faces denied certain services. Following the fall of the attack may be

weaker parts of the system or greatly slow processing. Steps to be followed in carrying out the attack to access the components are:

a) Obtaining information - choose a vulnerable component of the system and a communication port

b) Operation consists of sending inappropriate messages to a port chosen

c) Damage or overloading the disposal of a component of an application or a communication port.

• Application content - is an attack that sends bad data applications. In this type of attack as traffic is unaffected, however traffic is altered content and do not need to gain access to user. It follows the following steps:

a) Obtaining information - it sets the target application, the application can be both a network application (Web server) and a Microsoft Office application (via e-mail to transmit data applications)

b) Operation consists of sending content to the selected application directly or indirectly

c) Damage or export the files to delete user or change user account.

Attacks can be divided into two broad categories: external attacks and internal attacks.

Table 1: Actions taken by internal and external attackers

Type of attackers	**External attackers**	**Internal attackers**
1	It must get inside the perimeter of installed firewall	They can be found in the firewall perimeter
2	It navigates to an unknown network	They have authorization to access information
3	There are numerous external attacks but few of them are complete and affect database	They are the most dangerous and their attacks end with damage and high costs for the company

Often, external attackers are difficult to get into the system by firewalls installed by intrusion detection systems and the fact that you have to navigate a network access without authorization.

Internal attackers have these advantages (can be found in the perimeter firewall

and have access to information based on network topology).

Typically, organizations make their problems in relating to external attacks due to the number, but attacks coming from within are the most dangerous, entailing much greater damage.

A person who commits an informatics assault is called opponent.

Vulnerability can be defined as a system weakness exploited by a potential adversary. Computer vulnerabilities include: design weaknesses, vulnerabilities and implementation of fundamental vulnerabilities.

Once there is vulnerability, there is at least one opponent which entails the existence of a security risk. This equation can be written as follows:

Risk Security = Vulnerability + Opponent, called fundamental equation in security.

4. Monitoring and controlling access to classified data in economic databases

Ensuring safety standards is similar to vulnerability evaluation and only in vulnerability assessment usually reaches the safety standards that lead to continuous monitoring program.

Once secure database audit trails are generated and maintained for all activities that occur in the database that can alter the integrity or confidentiality of sensitive data or groups.

Auditors should have regard to the following events:

- Failed login attempts;
- Successful login attempts;
- Change configuration.

For better security it is recommended that data older than three months to be archived and retrieved when needed.

Also, every year, check the configuration database and compared with baseline. Any exceptions found are reported and will be classified as unauthorized changes or changes made by a user with access rights. As changes are made to configuration standards updated database.

To protect data or groups of data first method is the access to access what is achieved with combination of the following three security mechanisms: authentication, authorization and control user access to objects.

Anyone realizes the access control daily from a door lock when leaving the house or entering a card pin.

Computers are used to replace mechanical data access control achieved. Instead of working with mechanical locks and keys, use of passwords and identification data is recommended. If the password is invalid after verification when the door is open for a period fixed a priori, monitoring and registering the actual transactions is needed. If the password is invalid, the door remains closed trying to access is recorded. The system also records the access time of that date has been exceeded.

Many database systems use in the authentication process a username and a password to restrict access to data or resources allocated to different privileges. Moreover, access control provides rights and privileges assigned to objects such as: tables, views, rows, columns, and rights and privileges to groups of data.

One of the security mechanisms that are designed to prevent or detect a security attack is the access control mechanism.

Access control policy consists of at least one of the following: a list of access rights, passwords, security labels, duration of access time test access (especially if failed) and route of access.

By controlling access to classified data from a database means an authority that controls access data from it.

For an efficient access control to classified data in a database two things are important:

- User identification to be correct;
- A user does not have the privilege to transmit their access rights to another user.

Access control can be represented by a logic function f (s, o, a) three arguments with values in the set consists of true or false. The interpretation of this function is the following: the right of access to the subject to the object can be true if the subject or user has the right to perform operations on that object and false, otherwise. Both subjects and objects are software entities and human users.

This function is implemented by the reference monitor. Sensitive requests are intercepted by the reference control and monitor it can decide whether they are to proceed according to law that he has assigned the subject to the object. Authorization process within database represents transactions that the subject can do on an object in the database.

Sets of permissions to be granted to subjects are combinations of three basic types of access: read, write, execute. By reading right subject can read

file contents and view the directory contents including the file list. By writing the right subject can change the contents of a file. Law enforcement is, for example, running a program by topic.

5. Conclusions

Due to the world permanent motion, methods of privacy and control continuously improve with security attacks and threats.

In order to ensure data or data groups' security for databases two important aspects should be followed: security requirements including managing and reviewing vulnerabilities and access management, focusing on public access given to database objects.

Role of audit tracks and records made from access control is to detect security violations.

6. References:

- Barnes, R. (2011) Database Security and Auditing: Leading Practices, Enterprise Auditing Solutions Applications Security.
- Băjenescu, T.I. (2003) Progresele informaticii, criptografiei şi telecomunicaţiilor în secolul 20, Editura Matrix Rom, Bucureşti.
- Crampton, J. (2009) Cryptographically-enforced hierarchical access control with multiple keys, The Journal of Logic and Algebraic Programming 78, p. 690-700.
- Fusaru, D. (2002) Arhitectura bazelor de date. Mediul SQL, Editura Fundaţiei România de Mâine, Bucureşti.
- Fusaru, D.; Şerban, M. (2010), Algoritmi de criptare a bazelor de date, Annals of Spiru Hart University, Economic Series, 1(10), p. 207-215.
- Hicks, J. (2008) Criptography in SQL Server.
- Available http://msdn.microsoft.com/en-us/library/cc837966%28v=sql.100%29.aspx
- Hsueh, S. (2008) Database encryption in SQL Server 2008, Enterprise Edition, February.
- http://msdn.microsoft.com/en-us/library/cc278098(v=sql.100).aspx
- Lesov, P. (2008) Database Security: A Historical Perspective, University of Minnesota, CS 8701.

- Mihai, C.I. (2010) Modele de atac, Securitatea-informaţiilor.ro, Criminalitatea informatică.ro
- Available http://www.securitatea-informatiilor.ro/tipuri-de-atacuri/modele-de-atac-113.html.
- Oltean, G. (2012) Sisteme cu logică nuanţată, note curs,
- Available http://www.bel.utcluj.ro/dce/didactic/sln/sln.pdf.
- Patriciu, V.V.; Ene-Pietroşanu, M.; Bica, I.; Văduva, C.; Voicu, N. (2001) Securitatea comerţului electronic, Editura All, Bucureşti.
- Srikanth, Radhakrishna (2011) Database security best practices
- Available http://databases.about.com/od/security/a/databaseroles.htm.
- Şerban, M., Ştefan, R.M., (2012) Security Solutions for Data at Rest, Revista Economică, 5 (63), p. 174-179
- Available http://economice.ulbsibiu.ro/revista.economica/archive.php
- Ştefan, R.M., Şerban, M., (2012) Neural Network Principles to Classify Economic Data, Revista Economică, 4-5 (63), p. 223-233
- Available http://economice.ulbsibiu.ro/revista.economica/archive.php.
- http://en.wikipedia.org/wiki/Database_security.