Episteme: an online interdisciplinary, multidisciplinary & multi-cultural journal
Bharat College of Arts and Commerce, Badlapur, MMR, India
Volume 6, Issue 2 **September 2017**

SECURITY AND ITS IMPORTANCE IN DATABASE MANAGEMENT SYSTEM

By Krupali Bhatvedekar

Abstract

Data is the most important treasure in today's world as it is used by single user as well as an organization. For the easy access and availability of data it is placed in database System. Database system is a new concept compare to the programming language and operating systems. Databases are very important for the business and government organizations, to make the retrieval and maintenance of their data easy and efficient .Database organization and its contents are valuable assets that must be carefully protected because attacking databases are a favorite task for the hackers and attackers. The rapid development of Information technology has offered many opportunities for business operations. It has enabled business to enhance their efficiency and effectiveness in various operations like customer care, sales, human resources, etc. However, these developments lead to security issues. Many firms are becoming victims of cyber crimes. The has paper focuses on security issues that related to the database system, threats to the database and the how to maintain database security.

Keywords

Threats of database, database integrity, database security techniques.

Introduction

Security of database is a decisive operation that an organization should focus in order to run their activities smoothly. It is a willful effort to protect its data against threats like accidental loss, destruction or misuse. Threats pose a challenge to the organization in terms of integrity of the data and its access. The threat can result from in loss such as hardware theft or loss of confidence in the organization activities. Many database store sensitive information which can be vulnerable to hacking and misuse. Therefore, organization has enforced controls and checks on their database to maintain the integrity of the information and ensure that their systems are monitored closely to avoid violations by intruders.

Threats of database

The databases are targeted by the hackers because they are at the heart of any organization, as they store customer records and other confidential business data. The reason for the databases to be vulnerable to attack is that organizations are not protecting these crucial assets well enough. According to IDC, less than 5% of the $27 billion spent on security of database. When hackers or malicious insiders gain access to sensitive data, they can quickly extract value, cause damage to the data, or impact business operations.

Some of the threats to database are:

- **Inappropriate or unused Privileges**

  When the organizations grant their employee database privileges that exceed the requirements of their job, these privileges can be abused. Further, when the role of the employee is changed within an organization, his or her access rights to the sensitive data are not updated to remove rights no longer necessary for their new role**.** When these workers depart from the organization on bad terms, they can use their old privileges to steal high value data or inflict damage.

  Certain "Privileged Users" may abuse database privileges for unauthorized purposes. The two main privileges users are: first DBAs who have unlimited access to all data in the database. For the security purpose, DBAs should not access the application data directly from the database administrating the database. When a DBA accesses data directly instead of the application interface, he bypasses the application logging and retrieval limitations and

avoids the application permissions and security mechanism. Second Developers often have full access to production databases. In both cases, sensitive data is vulnerable to abuse.

- **SQL Injection**

  SQL Injection attack can give an attacker an unrestricted access to an entire database.

- **Malware**

  Cybercriminals use advanced attacks that blend spear phishing emails and malware – to penetrate organizations and steal sensitive data.\

- **Weak Audit Trail**

  Failure to collect detailed audit records of database activity is a serious organizational risk at many levels. Organizations with weak or sometimes non-existent database audit mechanisms will find that they are at odds with industry and government regulatory requirements. Audit responsibilities should be separate from both database administrators and the database server platform to ensure strong separation of duties

- **Storage Media Exposure**

  Backup storage media often remain completely unprotected from attack. As a result, various security issues have involved the theft of database backup disks and tapes.

- **Buffer Overflow vulnerabilities**

  The most common security problem of the databases, is when a program tries to copy too much of data in a memory buffer, causing the buffer to 'overflow' and overwriting the data currently in memory. This vulnerability is especially dangerous threat to databases holding sensitive info, as it could allow an attacker to exploit the vulnerability to set unknown values to known values.

Database Integrity

Integrity is crucial aspect of database security, because it ensures that only the correct people will be able to see company privileged information. The integrity of a database is enforced using a User Access Control system which defines the permissions for who can access which data.

The integrity is more than simple permissions. Security implementations like authentication protocols, strong password policies, and ensuring unused accounts (like of employees that have left the company) are locked or deleted, to strengthen the integrity of a database.

Database Security Techniques

Fig: Database security

There are various ways based on different aspects of securing the database. To remove the security threats organization must have a security policy which has be implemented for sure. In this policy authentication plays a vital role because if authentication is proper than there is less chances of threats. Different users have different access rights on different database objects. Access Control Mechanisms deal with managing the access rights. It is the basic technique to protect the data objects in the databases.

- **Access control**

  It is one of the fundamental services that any DBMS has to provide. It protects data from unauthorized read and write operations. Controlling through access rights may help in reducing the risks that may precisely impact the security of the database on the main servers. Access Control systems include:

  1. File permissions 2. Program permissions 3. Data rights

- **Authentication**

  A basic security requirement is that the users must be known. Identify the user so that you their actions upon the data can be audited. User can be authenticated in many ways.. Database authentication includes both identification and authentication of users.

- **Encryption**

  Encryption is the process of converting plain information into a code in such a way that it is not readable to all other people except those who have a key for the cipher text. The cipher text or encoded text is called as encrypted data.

- **Auditing**

  Auditing is the monitoring and recording of database actions, from both database users as well as non database users. Audit checks are needed to ensure physical integrity of the data which requires defined access to the databases and that is handled through auditing. If a user s managed to authenticate them successfully and tries to access a database, both successfully and unsuccessfully their attempts should be monitored by the system, and the record of same should appear in the audit trail files.

- **Don't Use a Shared Server**

  Avoid using a shared web server if the database holds sensitive information. While it may be easier, and cheaper, to host your site with the help of hosting provider you are placing the security of your information in the hands of someone else. If you have no other option, make sure to review their security policies and speak with them about what are their responsibilities.

Conclusion

Organizations rely on data to make decisions on various businesses operations to enhance their operations. Therefore, it is necessary to keep sensitive information away from unauthorized access. The research paper has attempted to explore the issues of security threats that may be poised to database system. The paper has also discussed the steps to protect database management system. Securing database is a prime responsibility of all the organization in order to keep their confidential information safe.

References

- Kumar Managing Cyber threats: Issues, Approaches and Challenges Springerublishers, 2005.
- http://www.imperva.com/downloads/Top Ten Database Security Threats.pdf
- P, Singh Database management system concept V.K (India) Enterprises, 2009
- https://globaljournals.org/GJCST_Volume12/3-Security-in-Database-Systems.pdf
- https://www.ijsr.net/archive/v3i4/MDIwMTMxMjc3.pdf
- "Security in Computing" 4th edition Mr.Charles P.Pfleeger-Pfleeger Consulting Group, Shari Lawrence Pfleeger

Bio

Ms. Krupali Bhatvedekar is an Asst. Professor in Department of Computer Science and Information Technology, Bharat College of Arts and Commerce . She can be contacted at krupalibhatvedekar@gmail.com