International Journal of Engineering Inventions
e-ISSN: 2278-7461, p-ISSN: 2319-6491
Volume 6, Issue 2 [Feb. 2017] PP: 25-27

Database Security: Threats and Solutions

Ayyub Ali[1] , Dr.Mohammad Mazhar Afzal[2]
Department of Computer Science and Engineering, Glocal University, Saharanpur

Abstract:- Securing data is a challenging issue in the present time. There are many ways a database can be compromised. Data security refers to protective digital privacy measures that are applied to prevent unauthorized access to the important information. Data security also protects data from corruption. Security goals for data security are Confidential, Integrity and Authentication (CIA). Security threats and solutions are discussed in this paper.

Keywords – *CIA Triad, Attacks, Data Protection, Threats*

I. INTRODUCTION

The rising abuse of computers and increasing threat to personal privacy through database has stimulated much interest in the technical safeguard for data. There are a large number of independent risks to confidential data stored in databases. Now a days, Issues around data confidentiality and privacy are under greater focus than ever before as ubiquitous internet access exposes critical corporate data and personal information to new security threats. Security breaches are typically categorized as unauthorized data observation, incorrect data modification, and data unavailability.

II. CLASSICAL SECURITY CONCERNS OF DATABASE

Confidentiality, integrity and availability, also known as the CIA triad, is a model designed to guide policies for information security within an organization. Confidentiality is a set of rules that limits access to information, integrity is the assurance that the information is trustworthy and accurate, and availability is a guarantee of reliable access to the information by authorized people.

Confidentiality:- Its means that the data is only available to authorized subjects. Confidentiality is roughly equivalent to privacy. Measures undertaken to ensure confidentiality are designed to prevent sensitive information from reaching the wrong people, while making sure that the right people can in fact get it: Access must be restricted to those authorized to view the data in question.

Integrity:- Its means data is only modified by authorized subjects. It involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle. Data must not be changed in transit, and steps must be taken to ensure that data cannot be altered by unauthorized people.

Availability:- Its mean data is available when needed. Availability is best ensured by rigorously maintaining all hardware. Redundancy, failover, RAID even high-availability clusters can mitigate serious consequences when hardware issues do occur. Extra security equipment or software such as firewalls and proxy servers can guard against downtime and unreachable data due to malicious actions such as denial-of-service (DoS) attacks and network intrusions**.**

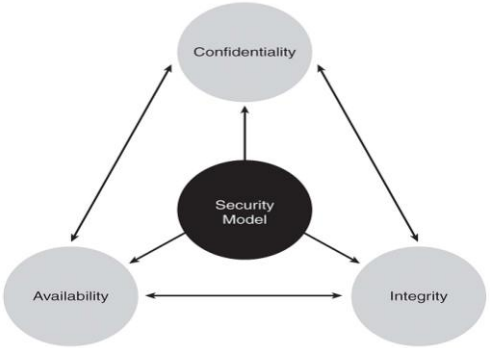

Fig CIA triad

III. DATABASE SECURITY THREATS

Excessive privileges:- When users (or applications) are granted database privileges that exceed the requirements of their job function, these privileges may be used to gain access to confidential information. The solution to this problem is query-level access control. Query-level access control restricts privileges to minimum-required operations and data*Privilege abuse:* Users may abuse legitimate data access privileges for unauthorized purposes. The solution is access control policies that apply not only to what data is accessible, but how data is accessed. By enforcing policies for time of day, location, and application client and volume of data retrieved, it is possible to identify users who are abusing access privileges.

Unauthorized privilege elevation

Attackers may take advantage of vulnerabilities in database management software to convert low-level access privileges to high-level access privileges.

Platform vulnerabilities

Vulnerabilities in underlying operating systems may lead to unauthorized data access and corruption. For example, the Blaster worm took advantage of a Windows 2000 vulnerability to take down target servers. IPS tools are a good way to identify and/or block attacks designed to exploit known database platform vulnerabilities.

SQL injection

SQL injection attacks involve a user who takes advantage of vulnerabilities in front-end web applications and stored procedures to send unauthorized database queries, often with elevated privileges. Using SQL injection, attackers could even gain unrestricted access to an entire database.

Denial of service

Denial of service (DoS) may be invoked through many techniques. Common DoS techniques include buffer overflows, data corruption, network flooding and resource consumption.

Malware

Cybercriminals, state-sponsored hackers, and spies use advanced attacks that blend multiple tactics – such as spear phishing emails and malware – to penetrate organizations and steal sensitive data. Unaware that malware has infected their device; legitimate users become a conduit for these groups to access your networks and sensitive data.

Storage Media Exposure

Backup storage media is often completely unprotected from attack. As a result, numerous security breaches have involved the theft of database backup disks and tapes. Furthermore, failure to audit and monitor the activities of administrators who have low-level access to sensitive information can put your data at risk. Taking the appropriate measures to protect backup copies of sensitive data and monitor your most highly privileged users is not only a data security best practice, but also mandated by many regulations.

Weak authentication

Weak authentication schemes allow attackers to assume the identity of legitimate database users. Specific attack strategies include brute force attacks, social engineering, and so on. Implementation of passwords or two-factor authentication is a must. For scalability and ease-of-use, authentication mechanisms should be integrated with enterprise directory/user management infrastructures.

IV. STRATEGIES FOR DATA PROTECTION

Protecting critical data involves creating a plan similar to a data recovery plan. When create a plan for protecting data there are a few things that have to be taken into consideration, as well as a few strategies that should be deployed to carry out data protection.

Determine Critical Data

Determine the importance of data and divide it into categories which include very critical, critical, inactive, and duplicate data. Obviously very critical data has the highest priority and duplicate data the lowest priority. Very critical data will require frequent backups and replication in the event of data loss, critical data should be backed up on a daily basis, inactive data should be retained for different compliancy reasons, and duplicate data can be deleted.

Data Access

Once the data is categorized and separated it is necessary to ensure that the end users have access to the data. The end users should be able to access the very critical and critical data as well as the inactive data that has been archived in the event of compliancy requests and other regulations.

Recovery Testing

Once you have a data recovery plan in place, it is important to test the recovery system on a periodic basis to ensure the organization can recover within a reasonable amount of time. When testing the recovery system, it is necessary to do a comprehensive test that reaches all the way to the application level.

Data Management

Most organizations do what is called an SRM (Service Resource Module) audit which monitors data categorization and data retention policies that are implemented within the data infrastructure. The audits help an organization to determine if the existing policies help to improve server and storage performance or hinder it. It also helps to determine the rate of improvement of data recovery speeds and reduced backup needs while at the same time decreasing overall costs of maintaining data management. Any company should consider cloud security; this will help keep important documents encrypted to people who are not allowed to view them

CONCLUSION

There are factors such as security concern evolution, the disinter mediation of data access, new computing paradigms and applications in which to apply and possibly extend current approaches to achieve data security. The security design for specific database system specify security administration and management functions. There are various types of security threats in database. Most of the threats mentioned above have their solutions. The different threats are discussed in this paper.

REFERENCES

[1] Mr. Saurabh Kulkarni, Dr. Siddhaling Urolagin, "Review of Attacks on Databases and Database Security Techniques", International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 2, Issue 11, November 2012.

[2] Iqra Basharat, Farooque Azam, Abdul Wahab Muzaffar,"Database Security and Encryption: A Survey Study", International Journal of Computer Applications (0975 – 888) Volume 47– No.12, June 2012.

[3] Emil Burtescu, "DATABASE SECURITY - ATTACKS AND CONTROL METHODS", Journal of Applied Quantitative Methods, Vol. 4, no. 4, Winter 2009.

[4] Erez Shmueli, Ronen Vaisenberg, Yuval Elovici, Chanan Glezer, "Database Encryption – An Overview of Contemporary Challenges and Design Considerations", SIGMOD Record, September 2009 (Vol. 38, No. 3).

[5] Ravi S. Sandhu, Sushil Jajodia, "DATA AND DATABASE SECURITY AND CONTROLS", Handbook of Information Security Management, Auerbach Publishers, 1993, pages 481-499. http://searchsecurity.techtarget.com/news/1048483/Buffer-overflow-attacks-How-do-they-work

[6] https://www.teamshatter.com/topics/general/team-shatter-exclusive/unpatched-databases/.

[7] http://www.appsecinc.com/downloads/Risks to Database Security in 2012.pdf.

[8] http://www.pciguru.com/2012/02/17/2012-database-threats/.

[9] http://www.channelinsider.com/c/a/Security/Database-Vulnerabilities-Top-10-Rules-IT-Shops-Break-772412/.http://www.bcs.org/content/conWebDoc/8852