ISSN No:-2456-2165

A Relative Study on Different Database Security Threats and their Security Techniques

Swati Jain[1], Dimple Chawla[2]
Assistant Professor, Vivekananda Institute of Professional Studies

Abstract:- Looking the amount of data stored in a database and the importance of that data for any organization, it is crucial for the organisation to secure the data in the database. With the increase in number of reported cases of data breaches, cybercrime, exposure of sensitive information, disclosure of confidential data to unauthenticated users, data intrusion there is a need for industries dependent on databases to ensure their data security and to defend their data from all the security threats. This paper focuses on the most recent database security threats, their origin and security techniques for ensuring database security.

Keywords:- *Database Security, Threats, Breach, Access Control, Security Techniques.*

I. INTRODUCTION

Data has changed the face of 21st century. In today's time the data has become a strategic asset of high-value because of its ability to make new discoveries. Data has become an indispensable part of everyone's life from a person keeping track of his monthly expenses to an IT company trying to boost its revenues through data mining [14]. The collection of data related to each other, referred as a Database contains all the information pertinent to an organisation. Database has made it possible for businesses to add to the effectiveness of their operations and enhance its capabilities [2] [3]. Any organisation's success and failure probability depends upon the quality, quantity and level of security of their database [1]. However, these advancements come along with various security threats like malicious people targeting data and compromising data integrity, unauthorised access to data and lastly data critical to the industry getting leaked to the outside world. Since data held by database is of great significance, it is utmost important to secure the database. Database security refers to the process of preventing data from unauthenticated misuse, inadvertent mistakes, data loss and corruption or any unintended activity on the database [1] [2] [3]. Just like every tangible asset of the organisation is protected, organisation's data in the database is one of the key assets that needs to be secured. Data resides in the database at different levels namely physical, data, network, application and host level. Data security ensures all the levels of database are protected [15].

In this paper, a brief discussion on the various security threats to a database is given in section 4. Section 3 of the paper, different database security strategies that can be applied to confirm database security are given.

II. ASPECTS OF DATABASE SECURITY

The three main aspects of database security are: *Confidentiality*, *Integrity* and *Availability*, commonly known as CIA Triad is a model designed to develop security policies used in identifying potential threats and the appropriate solutions to ensure information security. Any solution to data security is complete only if it is able to provide all three following requirements:

Confidentiality: means assuring the privacy of data. Confidentiality protects the stored data from any illegitimate and unauthorized access. It is implemented using access control mechanism, enforcing different levels of access and encryption techniques in the database [4] [5].

Integrity: means only authorized users should be able to make any modifications in the database. Maintaining accuracy, consistency and trustworthiness of the data is the part of database integrity [4]. This can be ensured with the combination of access control along with integrity constraints on the database [5] [14].

Availability: means information is readily available whenever it is needed. It is possible by strictly maintaining all the hardware, software, access channels and mechanism components of the database. Availability also ensures speedy recovery from any hardware or software errors with consistent data in the database [4] [5].

III. ORIGIN OF SECURITY THREATS

Security threats can have various sources of origination such as *Internal*, *External* and *Partner*.

Internal: These are the security threats sources that exist within the organisation like some company executives who have high access and privileges of the database. Internal sources enjoy certain levels of trust and privileges [19].

External: Sources outside the organisation pose as the external threats to database. Hackers, cybercrime groups and other government entities are some examples of external sources of threats. No trust or privileges are invested in external sources [7] [19].

Partners: These are the people outside the organisation that share business relationship with them. Customers, vendors, suppliers and contractors are a few examples of partner groups of organisation that can be a source of threat for the database. Since the communication

ISSN No:-2456-2165

between both the parties are necessary for the functionality of business, moderate level of trust and privileges are associated with them [7].

On the basis of Data Breach Investigation Report (DBIR) 2016 [16], 2017[17], 2018[18] and 2019[19], where different origins of security threats such as Internal, External, Parties and Multiple parties [4] [5] were considered following chart Figure 1 has been derived. The conclusions made from the following graph [Figure 1] are:

- There was an increase in the percentage of security threats originating from within the organisation from 11% in 2016 to 34% in 2019.
- Threats originating from external sources decreased over the period of 2015 – 2019 from 86% to 69%.

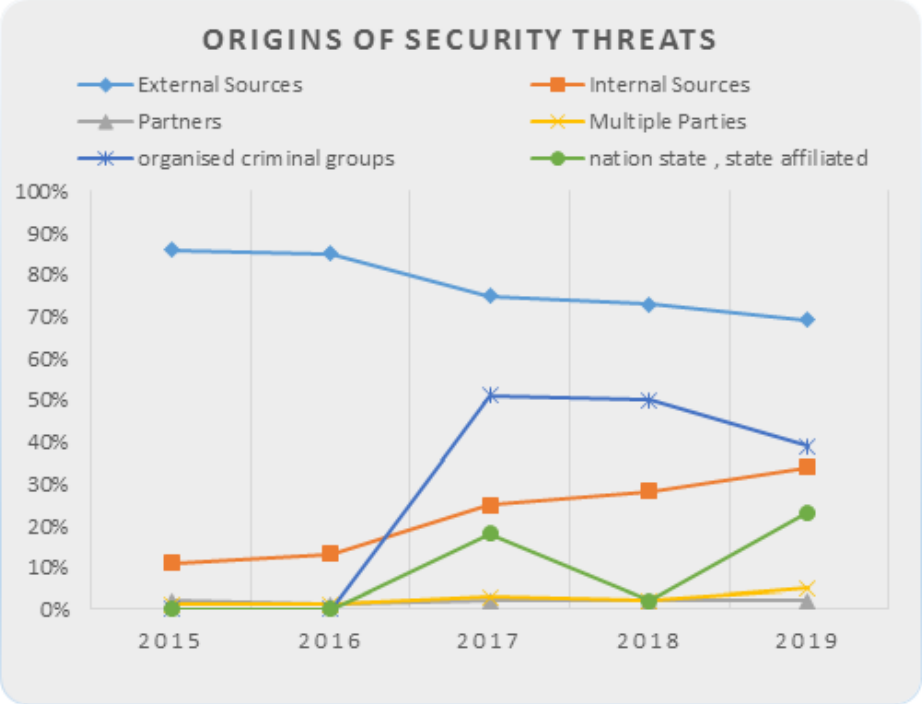

Fig 1:- Origins of Security Threats Chart

In addition to these security threats origin threats, 2 more origins namely organised criminal groups and actors identified as nation state, state affiliated were also noted from 2017 onwards which shows a decrease in threats originating from criminal groups over the period of 2017 – 2019 [17][18][19].

IV. SECURITY THREATS

According to IBM's 2019 Data Breach Report, Conducted by the Ponemon Institute, the cost of a data breach has increased by 12% over the past 5 years and is now $3.92 million on world average[20][9]. The financial consequences of the attacks on database are not only immediate but the cost impact is felt for years after the incident [9].

There are several security threats that can lead to data breach incidents. Top 10 threats over the past decade are:

A. Excessive and Inappropriate Privilege abuse:

Database management systems and their corresponding data structures are complicated which makes administrators granting excessive rights to the users so as to prevent any application failure due to lack of rights [2]. When users are given privileges more than what is required for their job functionality, these privileges can be used maliciously [12]. For example course coordinator for any university is given the right to upload marks of every student. This privilege can be misused to change the marks of any student or any subject. This misuse is the result of granting generic access rights to a certain group of users even when it exceeds their specific job requirements [12].

B. Legitimate Privilege Abuse:

This happens when a user is given only those privileges which are required by their job functionalities and these legitimate privileges are used for unauthorized purposes. User groups like Database System Administrator (DBA) and Developers have access to entire database due to their job requirements [2]. If a DBA tries to access the database data directly instead of application interface, all the application permissions and security mechanisms would be surpassed making the way for privilege abuse clear [2][7][12].

C. Privilege Elevation:

Users with low-level privileges may use the vulnerabilities in the database to convert their access rights to high-level privilege. This can lead to the availability of critical information to unauthorised users [3] [12].

D. Platform Vulnerabilities:

Any vulnerabilities in the underlying Operating System like Windows 2000, Windows XP, and Linux etc. can lead to privilege escalation, denial of service, data corruption and unauthorised access security threats [12]. For example, A potential security vulnerability in Intel WIFI Drivers and Intel PROSet/Wireless WiFi Software extension DLL with severity rating as High was patched in November 2019 platform update. Memory corruption issues in Intel(R) WIFI Drivers before version 21.40 may allow a privileged user to enable escalation of privilege, denial of service, and information disclosure via local access [8].

E. Weak Audit Trails:

Automated recording of any database transactions involving sensitive data should be a part of every database deployment. Failure to monitor transactions and collect audit details of database activities poses risk to the organisation on many levels [2]. Many organisations rely on native audit tools provided by the database but the native audit tools do not record sufficient contextual information necessary to ensure security, detect attacks and provide incident forensics. Another reason native audit tools are not reliable is that users with administrative rights either legitimate or escalated can turn off database auditing to hide malicious activities [12] [14]. Therefore database responsibilities and audit capabilities should be separate from both database server platform and database administrator to ensure strong separation of duties policy [11].

F. Denial of Service (DoS):

This is a general category attack in which the legitimate users like employees, members or account holders are deprived of database services or resources which they require. This is done by shutting down the machine or the network making it inaccessible for its intended users. This can be done in two ways either by flooding the destination with excess traffic or by sending them information that results in a crash [12]. Even though Dos doesn't directly result in data theft, loss or corruption they can cost a significant amount of time and money to handle.

G. Unsecured Storage Media:

Backup storage media is often less secured compared to the other database assets. This consequence to several high profile data breaches involving theft or incidental exposure of database backup tapes and hard disks. Many regulations have made it mandatory to protect backup copies of sensitive data. One of the possible solutions to this is encryption of all the backup data [2] [7].

H. SQL Injection Attack (SQLIA) [1]:

This is an attack which gives a potential attacker complete control over your database through the insertion of unauthorised or malicious SQL code in the database query. There can be multiple types of SQLIA:

- Injection by passing malicious strings in for user input in web forms.
- Through cookies; modifying cookie fields so that they contain attack strings.
- Through server variables where headers are modified to contain attack strings.
- Second Order SQLI; where the attack is designed to run at a later stage and not immediately [12].

I. Database Communications Protocol Vulnerabilities:

Proprietary protocols are created by database vendors for the communication between database client and servers through data and commands. Vulnerabilities in these protocols can lead to various fraudulent activities like unauthorized data access, denial of service, data corruption [4] [12]. In addition to these threats, what makes them worse is the fact that no record of these fraud activities will be there in the native audit trail since these protocols are covered by database native audits. Attacks based on protocols can be prevented by using protocol validation [12] which audits and protects against attacks by comparing live protocol to expected protocol structure [7][12].

J. Weak authentication:

If the authentication procedure of any database is weak, attacker can acquire the identity of a legitimate database user by using any of the following techniques: Brute force, social engineering and direct credential theft [12]. Two step authentication procedures is a must for database security [4].

V. SECURITY TECHNIQUES

Database is the backbone of any organisation. Therefore it is important for the organization to implement any security solution. The security technique must ensure the safety of not only the data inside the system but also the database hardware, software and human resources. Database security techniques can be broadly classified into four categories, namely: Access Control, Techniques against SQLIA, Data Encryption and Data Scrambling [1].

A. Access Control (Mechanism):

Data confidentiality can be ensured by using Access Control Mechanism. Most users are assigned or have authorized privileges to specific database resources and every time a user tries to access any data from the database, the access control mechanism will compare the required privileges to assigned privileges. Through this technique users can only access that data object for which they are adequately authorized. For example, for a university database teachers and students can be two categories of users with different access privileges. A student can only read grades and course offered and the teacher can update grades of students. A student can't make changes in the grades obtained whereas a teacher can't make changes in the courses offered.

➢ *Access Control in databases can be maintained in different ways such as:*

- **Discretionary Access Control (DAC):** DAC grants or restricts the access to a data object based on an access policy created by the owner of data object. It is discretionary because the owner can transfer the authenticated objects and information access to other users. Object's owner group has complete control over the access of the object [6].
- **Mandatory Access Control (MAC):** MAC allows a user to access a data object only when the authority level of the user matches the security level of needed data item. Access control in MAC is based on the following two principles:

✓ *No read up:* User can only read a data object when the access class of user is higher than the access class of that object.

✓ *No write down:* User can write a data object only if the access class of object is higher than that of the user.

- **Content Based Access Control:** In this model, the access control decisions are based on the contents of data objects [12]. For example, Employee table has salary details of all the employees of the organization. So only those employees of accounts department who are working on employee salary part should be able to access that data. This approach is implemented using views. Users are presented with the temporary view of the table with only those data they are authorized to access and not the complete table itself.
- **Fine Grained Access Control (FGAC):** General access control for database is coarse grained, i.e. it grants access to all the rows of the table or none at all. In contrast to this is fine grained access control that implements access control at the tuple level of the database. It enforces access control at the granular level. In this scheme each data object is given its own access control policy. This is implemented using specialization of views [12]. Oracle Virtual Private Database (VPD) is one such database implementing FGAC.

B. Preventing SQLIA - Fighting Techniques are

SQL injection attack gives complete control of our database to the attacker and thus it is one of the most dangerous security threats. The detection approaches for SQLIA can be categorized as

- *Pre-Generated:* Implemented during the testing phase of web application of database.
- *Post-Generated:* Used when the dynamic SQL generated by web application is analysed [1].

➢ *Post Generated Approaches:*

- **Positive tainting and Syntax Aware Evaluation:** In this technique valid input strings are provided to the system initially to detect SQLIA. Positive tainting here means identifying, marking and tracking of trusted SQL queries and differentiating malicious queries from the legitimate ones using taint marking. Syntax aware evaluation allows us to actually use taint marking to identify trusted queries for the database. It allows the use of untrusted input data in a SQL query as long as it does not lead to SQLIA. Syntax evaluation of a query string is performed before the string is sent to the database for execution [8].
- **Context Sensitive String Evaluation:** It works on simple classification of data, User based data is considered as unreliable and data given by application is considered as reliable. Un-reliable data is then sent for syntax evaluation where string and numeric constants are differentiated from each other and all unsafe characters are removed from the strings identified [1].
- **Parse Tree evaluation based on grammar:** This approach defines a predefined grammar which is used to parse all the queries generated from users. A parse tree is a data structure that represents a parsed statement. Parsing a statement requires the grammar of the language it was written in [9]. When a malicious user injects a SQL query into the database, the parse tree of the legitimate query and injected query will not match and this is how the SQLIA would be detected using parse tree.

➢ *Pre Generated Approaches:*

- **Pixy:** The first open source tool to statically detect cross-site scripting (XSS) [10]. It follows data flow analysis approach to create information and statistics for each program point. For example, the constant analysis computes for all program points, the values that variable can hold. After data flow analysis parse trees are created and taint analysis tool is applied to find out all the points in the database which are vulnerable to attacks and malicious data entry.
- **Program Query Language:** It is a language having pre-defined grammar to express pattern of events on data objects. It provided a static and dynamic program analysis to find the sequence of program as it runs. These are recorded in data logs which provide support for detecting malicious queries.

C. Data Encryption

The technique used to secure any kind of data or information can also be used to protect the data stored in database. Data encryption is a technique of transforming a plain text to intelligible form. This resulting information is known as encrypted data which can be converted back to its original form using encryption key. This technique can be used to secure the database by saving encrypted data in the database instead of plain text and converting the encrypted data to its original form when it is required for processing purposes. There are two different approaches to data encryption technique:

Symmetric Encryption: One common key is used for both encryption of data and decryption of data as well.
Asymmetric Encryption: Two keys are used, one key for encryption and the other for decryption.

There are three aspects to be considered while encrypting data for database security:

- **Encryption Algorithm:** First aspect of encrypting database is to identify the algorithm to be used. Various data encryption algorithms supported by DBMS are: AES, DES, Triple DES, RC2, RC4 and DESX. Second aspect is to identify the encryption level of database from the following:

  - File system Encryption – Encrypting the physical disk where the data is stored.
  - DBMS level Encryption – Encrypting tables, rows or fields.
  - Application level Encryption – A middleware is used to translate user query into new queries to work on encrypted data.
  - Client Side Encryption – It is used when the database is being used as a service and the organization outsources the complete database and data privacy is a major concern [14].

- **Place of encryption:** Second aspect is to identify different levels where Data encryption can be done. The encryption of data can be done either inside the database as its part or outside the database. When the encryption is carried out inside the database then the impact on the database application environment is less. One problem area of this approach is that the encryption keys are stored along with the database itself which can pose as a security concern. Another way to encrypt database is to perform it on separate encryption servers. The liability of encryption and decryption is now not on the database and done on independent servers thus maintaining the database performance [14]. In this approach Encryption keys and Data is stored separately and not on the same database.

- **Granularity of Encryption**: Third aspect is to identify the encryption level of the data to be encrypted. Different granularity levels of encryption can be Cell, Column, Tablespace and File with cell-level being the most specific level and File level being the most general level of encryption for the database. More granular level of encryption can result into performance degradation for the database. Column-level is the most commonly used encryption level since it includes less processing than that required at cell level and still provides encryption at a specific level of database.

D. Data Scrambling

It is a process of deliberately changing or removing the data saved in the database so as to make sensitive data safer for wider visibility. It is also known as Data masking, Data sanitization and Data obfuscation. It is used in the scenario where a user has access to a certain data but still the data needs to be protected from the user. For example, testers and third party developers involved in working on the data in the database [1]. Even though they require working on the data but the actual values of data can be changed to hide the sensitive information. Basically, data is changed but the changed data resembles the actual data. Relationships between the columns in the original data would exist in the scrambled data as well. This way the actual sensitive information would be hidden from third party developers and they can still work with the data.

VI. CONCLUSION

Database management systems provide an easy and efficient way to manage and manipulate data. Protecting data and the DBMS from any attacks is the goal with the highest priority for any organization. In this paper, we have discussed about the origins of security threats for an organization and how the pattern has shifted from external sources to internal sources over the period of last 5 years. Top 10 security threats to database were also highlighted in the paper along with the strategies which are being used to prevent the data attacks.

REFERENCES

[1]. 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, pp. 253-263

[2]. White Paper on “Top 5 database security threats” © 2016, Imperva, Incorporated

[3]. Deepika, Nitasha Soni, “Database Security: Threats and Security Techniques”, International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 5, Issue 5, May 2015, pp.621-624

[4]. Ayyub Ali, Dr. Mohammad Mazhar Afzal, “Database Security: Threats and Solutions”, International Journal of Engineering Inventions, e-ISSN: 2278-7461, p-ISSN: 2319-6491, Volume 6, Issue 2, February 2017, pp. 25-27

[5]. Mohd Muntjir, Sultan Aljahdali, Mohd Asadullah, Junedul Haq, “Security Issues and Their Techniques in DBMS - A Novel Survey”, International Journal of Computer Applications (0975 – 8887), Volume 85 – No 13, January 2014

[6]. Aye Mon Win, Khin Lay Myint, “Database Security Model using Access Control Mechanism in Student Data Management”, International Journal of Trend in Scientific Research and Development (IJTSRD), Volume: 3 Issue: 3, e-ISSN: 2456 – 6470, Apr 2019, pp. 529-531

[7]. Nedhal A. Al-Sayid, Dana Aldlaeen, “Database Security Threats: A Survey Study”, 2013 5th International Conference on Computer Science and Information Technology (CSIT) ISBN: 978-1-4673-5825-5, pp. 60-64

[8]. INTEL-SA-00287, “The latest security information on Intel® products” Intel® WIFI Drivers and Intel® PROSet/Wireless WiFi Software extension DLL Advisory

[9]. Tresorit, “The Top 6 Takeaways from The 2019 Cost of a Data Breach Report”, 29 July 2019,

[10]. Nenad Jovanovic, Christopher Kruegel, and Engin Kirda, "Pixy: A Static Analysis Tool for Detecting Web Application Vulnerabilities (Short Paper)", https://www.auto.tuwien.ac.at/~chris/research/doc/oakland06_pixy.pdf
[11]. Mubina Malik, Trisha Patel, "Database Security – Attacks and Control Methods", International Journal of Information Sciences and Techniques (IJIST) Vol.6, No.1/2, March 2016, pp.175-183
[12]. Shivnandan Singh, Rakesh Kumar Rai, "A Review Report on Security Threats on Database", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3), ISSN: 0975-9646, 2014, pp. 3215 – 3219,
[13]. Ramandeep Kaur, Kiranpreet, Prince Verma "Survey on Database Security", International Journal of Computer Applications (0975 – 8887) Volume 105 – No. 10, November 2014, pp. 27-31
[14]. A.W Akanji, A.A. Elusoji and A.V. Haastrup, "A Comparative Study of Attacks on Databases and Database Security Techniques", IEEE African Journal of Computing & ICT, Vol 7. No. 5, ISSN: 2006-1781, December 2014, pp. 1-8,
[15]. Emil Burtescu, "Database Security - Attacks And Control Methods", Journal of Applied Quantitative Methods, Vol. 4 No. 4 Winter 2009, pp. 449-454
[16]. Verizon, 2016 Data Breach Investigations Report, https://enterprise.verizon.com/resources/reports/DBIR_2016_Report.pdf
[17]. Verizon, 2017 Data Breach Investigations Report 10th Edition, https://enterprise.verizon.com/resources/reports/2017_dbir.pdf
[18]. Verizon, 2018 Data Breach Investigations Report 11th edition, https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf
[19]. Verizon, 2019 Data Breach Investigations Report, https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf
[20]. Chris Brook, "What's the Cost of a Data Breach in 2019?",30 July 2019 , https://digitalguardian.com/blog/whats-cost-data-breach-2019