UDC 004.658.2 **doi: 10.20998/2522-9052.2018.1.13**

V. Pevnev, S. Kapchynskyi

National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine

DATABASE SECURITY: THREATS AND PREVENTIVE MEASURES

The **subject matter** of the article is the variety of different threats and vulnerabilities which can occur while developing, managing and maintaining different databases and database management systems. The **goal** is to analyze the described threats and provide the most appropriate solutions. The **tasks** to be solved are: analyze the variety of different threats and vulnerabilities and select the most common and problematic ones, propose the most appropriate preventive measures or solutions for each of items selected. Ensuring database security is very critical for the organizations. As the complexity of the databases increases, we may tent to have more complex security issues of database.

Keywords: security; threats; risks; preventive measures; database; database management systems.

Introduction

In recent years, security incidents, including sensitive data leakage, has been seen more frequently. Much of this sensitive data is processed and maintained using the help of database management systems (DBMS). Considering that, for the different organizations, their data security is crucial, it is essential to take different actions and use various practices in order to protect the data present in the database. Secure databases are the ones who's been ready to take appropriate measures in case of possible database attacks. There are variety of security models required to maintain stored data in integrity [1][2]. They may be different in many aspects as they are targeted on prevention of the different problems in database security. Also, they can differ because the definition of database security is not strict, which leads to many various issues for engineers, who seek for creation of the secure infrastructure for sensitive data storage.

Database is a collection of data that is stored somewhere on the physical machine [3]. Any user, who is authorized to communicate with database can perform different read-write on the data stored within. Databases could not manage themselves, as they are responsible only for the data storage. Systems, which are created especially for database management and maintenance are called database management systems (DBMS).

DBMS interacts with authorized users, other applications and database itself to capture and analyze the data. It is responsible for restructuring the data for better performance and to lower the storage consumption.

DBMS can be accessed in parallel way and it should handle all the requests correctly and without any issues. Also, it can be responsible for storing snapshots for the databases using the "backup and restore" functionality.

Now a day's the databases are required to store any type of data needed, because they are much more efficient in terms of processing speed. Also, the costs for database maintenance is more than affordable for any kind of business. Modern databases could handle the bulk operations with millions of data items in a second [4]. For example, there is no need to manually write and calculate the warehouse re-stock report, because hand held barcode scanners can be used to write information directly into the database.

When the database is used in offline mode only, with only one concurrent connection at max, then there is no need perform any actions to ensure database security.

But in cases, when the database communicates with many different concurrent connections and external applications, the next question arises: "Is data secured using the database?". Security in today's world is one of the most important and challenging tasks that people are facing all over the world in any aspects of their lives.

With passage of time, the databases become much more complex to maintain.

Without up-to-date documentation, database engineer will hardly keep up with all places, where the sensitive data is contained.

Database security is the use of a wide range of data security controls to protect databases against any attacks (internal or external), against compromises of database confidentiality, integrity and availability.

The **goal** of this article is to perform analysis for different existing vulnerabilities related to databases and to propose appropriate counter measures for them.

Database Threats

Modern databases are subjects to breach using various attack, aimed to receive unauthorized access or to corrupt the date integrity or availability. Before we start describing the preventive measures of different attacks and vulnerabilities, there is necessary to describe some of the risks related to them, and, if there are an ability to, provide examples of the consequences.

Excessive privileges. When users (or applications) are granted database access privileges that exceed the requirements of their job function, these privileges may be abused for malicious purpose. For example, a university administrator whose job requires only the ability to change student contact information may take advantage of excessive database update privileges to change grades. A given database user ends up with excessive privileges for the simple

reason that database administrators do not have the time to define and update granular access privilege control mechanisms for each user. As a result, all users or large groups of users are granted generic default access privileges that far exceed specific job requirements [5].

Countermeasures. Do not grant access privileges that far exceed specific job requirements for the user. Implement good audit trails, so database administrators could handle with privilege abuses in timely manner.

Example. According to a survey from security firm BeyondTrust, which focuses on privilege management issues, more than 47 percent of the 728 survey participants said users in their organizations have elevated privileges not necessary for their roles.

Twenty percent reported that more than three-quarters of their user base run as administrators. In addition, 33 percent said their organizations had no policies for privileged password management [5].

Input injections. Input injections is a code injection technique, used to attack data-driven applications, in which nefarious database query statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker).

Countermeasures. Validate input data received from the user. Do not blindly use the input data provided.

This may be achieved by adding an additional interpretation level into the application, which will handle the database query construction.

Use parametrized statements if it's possible.

Use Data Access Control policies to manage the database user privileges (e.g. deny any modification requests for the certain resource).

Example. On October 1, 2012, a hacker group called "Team GhostShell" published the personal records of students, faculty, employees, and alumni from 53 universities including Harvard, Princeton, Stanford, Cornell, Johns Hopkins, and the University of Zurich on pastebin.com. The hackers claimed that they were trying to "raise awareness towards the changes made in today's education", bemoaning changing education laws in Europe and increases in tuition in the United States [6]. In October 2015, an SQL injection attack was used to steal the personal details of 156,959 customers from British telecommunications company TalkTalk's servers, exploiting a vulnerability in a legacy web portal [7].

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.

Countermeasures. Do not install any additional software without formal verification (antimalware tools, sandboxes, etc.) or services onto your database server. Provide an explicit and well-documented software installation policy for your organization members.

Weak audit trail. Automated recording of all sensitive and/or unusual data base transactions should be the part of the foundation underlying any database deployment. Weak database audit policy represents a serious organizational risk on many levels.

Counteremeasures. Configure your DBMS to generate log for desired security events. Use third-party network-audit tools.

Backup exposure. Backup database storage media is often completely unprotected from attack. As a result, several high-profile security breaches have involved theft of database backup tapes and hard disks [8].

Countermeasures. All database backups should be encrypted. In fact, some vendors have suggested that future DBMS products may not support the creation of unencrypted backups.

Encryption of on-line production database information is often suggested, but performance and cryptographic key management drawbacks often make this impractical and are generally acknowledged to be a poor substitute for granular privilege controls described above [7].

Weak authentication. Weak authentication schemes allow attackers to assume the identity of legitimate database users by stealing or otherwise obtaining login credentials. An attacker may employ any number of strategies to obtain credentials.

Countermeasures. Use strong authentication: two-factor mobile authentication, certificates, biometrics. In cases where additional authentication options are unavailable, enforce strong username/password policies (minimum length, character diversity, obscurity, etc.).

Example. Millions of accounts associated with video-sharing site Dailymotion, one of the biggest video platforms in the world, have been stolen. A hacker extracted 85.2 million unique email addresses and usernames from the company's systems, but about one-in-five accounts — roughly 18.3 million– had associated passwords, which were scrambled with the bcrypt hashing function, making the passwords difficult to crack. The hack is believed to have been carried out on Oct. 20 by a hacker, whose identity isn't known, according to LeakedSource, a breach notification service, which obtained the data [9].

DB vulnerabilities & misconfiguration. It is common to find vulnerable and un-patched databases or discover databases that still have default accounts and configuration parameters. Attackers know how to exploit these vulnerabilities to launch attacks against your organization.

Countermeasures. Do not use default credentials/accounts for the database communication. Integrate your database server authentication system with organization's domain system.

Example. MacKeeper Security Researcher Chris Vickery contacted DataBreaches.net to report that he had discovered yet another misconfigured MongoDB database. This one, 132 GB in size, appeared to contain voter registration data from 93,424,710 Mexican citizens [10].

Denial of service. Denial of Service is a general attack category in which access to network applications or data is denied to intend to user.

Countermeasures. Harden the TCP/IP stack by applying the appropriate registry settings to increase the size of the TCP connection queue, decrease the connection establishment period, and employ dynamic backlog mechanisms to ensure that the connection queue is never exhausted.

Use a network Intrusion Detection System (IDS) because these can automatically detect and respond to SYN attacks.

Example. On March 26, 2015, a very well-coordinated distributed denial of service (DDoS) attack was waged on GitHub, the heir apparent to the now-closing Google Code. GitHub characterized this as the largest DDoS in its history. The Electronic Frontier Foundation (EEF) and security researchers Netresec name the Chinese government as the culprits of the attack, which lasted until March 31, 2015 [12].

Loss of outdated storage devices. Because of rapid growth of computing power, different storage devices (hard disk drives, solid state drives and other data storage hardware) become outdated every 5-7 years and so they are replaced with new ones. Usage of embedded data destruction tool does not guarantee the inability to restore the data.

Countermeasures. Always perform full recycling of outdated storage devices with respect to the rules and standards of this process.

Limited security expertise & education. Non-technical security is also play an important role. Internal security controls are not keeping pace with data growth and many organizations are ill-equipped to deal with a security breach. Often this is due to the lack of expertise required to implement security controls, enforce policies, or conduct incident response processes.

Countermeasures. Hire or cultivate an experienced security professional.

Summary

Databases are the core part for any modern information system. It is crucial to create environment, which will protect the data and the database itself. With the passage of time it becomes harder and harder to achieve this goal.

With the rapid growth of data production and consumption lead to an increase of data breaches and uncovered vulnerabilities [13].

This article aims to popularize the idea of data security as well as to provide a cumulative set of rules and actions which can decrease the risks related to data confidentiality, integrity and availability violations. Also, it covers different types of vulnerabilities which can occur while working with modern databases and database management systems.

As it follows from a brief review of the list of presented vulnerabilities, it's not hard to declare that the most crucial point of database security is the personnel which is responsible for managing and developing the database. This work had covered some of vulnerabilities related to databases and described the counter measures for them.

Usage of described recommendations will help to avoid the impact of the threats listed while developing, managing and using the databases. The threats described are not covering all the opportunities of potential violators.

In particular, various insider threats that occupy a sufficiently large niche in the list of threats to the database.

References

1. Common Criteria DBMS Working Group Technical Community (2015), *Base Protection Profile for Database Management Systems (DBMS PP) V 2.07, BSI-CC-PP-0088*, available at: https://www.commoncriteriaportal.org/files/ppfiles/pp0088b_pdf.pdf (last accessed January 29, 2018).
2. Database Security Consortium Security Guideline WG (2009), *Database Security Guideline V 2.0*, available at: http://www.db-security.org/report/dbsc_guideline_ver2.0_e.pdf (last accessed January 29, 2018).
3. Mubina Malik and Trisha Patel (2016), *Database Security – Attacks And Control Methods*, International Journal of Information Sciences and Techniques (IJST) Volume 6, No. 1 (2), Department of Computer Science & Applications, Kurukshetra University, Kurukshetra, available at: https://www.ijser.org/researchpaper/Database-Security--Attacks-and-Techniques.pdf (last accessed January 29, 2018).
4. Eugene Philipov (2016), "Comparing multiple rows insert vs single row insert with three data load methods", available at: https://www.red-gate.com/simple-talk/sql/performance/comparing-multiple-rows-insert-vs-single-row-insert-with-three-data-load-methods/ (last accessed January 29, 2018).
5. Andras Cser, Stephanie Balaouras, Laura Koetzle, Merritt Maxim, Salvatore Schiano, and Peggy Dostie (2016), *The Forresetr Wave: Privileged Identity Management*, Forrester Research, Inc., Cambridge. available at: https://www.beyondtrust.com/wp-content/uploads/forrester-wave-for-privilege-identity-management-2016.pdf?1467996373 (last accessed January 29, 2018).
6. Nicole Perloth (2012), "Hackers Breach 53 Universities and Dump Thousands of Personal Records Online", New York Times, New York, available at: https://bits.blogs.nytimes.com/2012/10/03/hackers-breach-53-universities-dump-thousands-of-personal-records-online/ (last accessed January 29, 2018).
7. ICO (2016), "TalkTalk gets record £400,000 fine for failing to prevent October 2015 attack", Information Commissioner's Office, Wilmslow, available at: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/10/talktalk-gets-record-400-000-fine-for-failing-to-prevent-october-2015-attack/ (last accessed January 29, 2018).
8. Amichai Shulman (2008), "Top Ten Database Security Threats: How to Migitate The Most Significant Database Vulnerabilities", available at: http://schell.com/Top_Ten_Database_Threats.pdf (last accessed January 29, 2018).

9. Dean Alvarez (2016), “Dailymotion loses 85 million users` details in data breach – Industry Reaction”, available at: http://www.itsecurityguru.org/2016/12/06/dailymotion-loses-85-million-users-details-data-breach-industry-reaction/ (last accessed January 29, 2018).
10. Chris Vickery (2016), “Massive Breach of Mexican Voter Data”, available at: https://mackeeper.com/blog/post/217-breaking-massive-data-breach-of-mexican-voter-data (last accessed January 29, 2018).
11. Mazhar Farooqui (2016), “Data of 34 million Keralites leaked in massive breach”, available at: http://gulfnews.com/xpress/news/data-of-34-million-keralites-leaked-in-massive-breach-1.1930317 (last accessed January 29, 2018).
12. James Sanders, “Chinese government linked the largest DDoS attack in GitHub history”, https://www.techrepublic.com/article/chinese-government-linked-to-largest-ddos-attack-in-github-history/ (last accessed January 29, 2018).
13. Michelle Leech (2017), “Data breach statistics 2017: First half results are”, available at: https://blog.gemalto.com/security/2017/09/21/new-breach-level-index-findings-for-first-half-of-2017/ (last accessed January 29, 2018).

Надійшла (received) 24.01.2018
Прийнята до друку (accepted for publication) 11.04.2018

Безпека баз даних:
загрози та превентивні заходи

В.Я. Пєвнєв, С.Д. Капчинський

Є велика кількість різноманітних загроз та вразливостей, які можуть виникнути під час розробки, управління та підтримки різних баз даних та систем управління базами даних. **Метою** статті є проведення поглибленого аналізу описаних загроз та визначення найбільш оптимальних заходів для їх усунення. **Завдання:** провести поглиблений аналіз різноманітних загроз і вразливостей та вибрати найбільш розповсюджені та найпроблематичніші з них, проаналізувати та запропонувати оптимальніші з превентивних заходів або рішень для кожної з переглянутих загроз. Серед **проаналізованих загроз** були обрані: надмірні привілеї (excessive privileges), вхідні ін'єкції (input injections), зловмисне програмне забезпечення (malware), слабкий аудиторський слід (weak audit trail), недостатній рівень безпеки резервних копій (backup exposure), слабка аутентифікація (weak authentication), внутрішні вразливості баз даних та неправильна конфігурація (DB vulnerabilities & misconfiguration), некеровані конфіденційні дані (unmanaged sensitive data), відмова в обслуговуванні (denial of service), втрата списаних носіїв інформації (loss of outdated storage devices), низький рівень експертизи з безпеки та низький рівень освіти працівників (limited security expertise & education). Для кожної з перерахованих загроз проаналізовані та визначені оптимальні заходи для їх усунення. **Висновки.** Бази даних є основною частиною будь-якої сучасної інформаційної системи. Дуже важливо створити середовище, яке зможе захистити дані та саму базу даних. З часом стає важче досягти цієї мети. Швидке зростання створення та споживання даних призводить до збільшення порушення даних та виявлення нових вразливостей. Дана стаття націлена на популяризацію ідеї безпеки баз даних а також пропонує чіткий набір правил та дій, спрямованих на зниження ризиків, пов’язаних з конфіденційністю, цілісністю та доступністю даних. Як випливає з огляду переліку представлених вразливостей, не важко замітити, що найважливішим пунктом безпеки баз даних є персонал, який відповідає за управління та розробку бази даних.

Ключові слова. безпека; загрози; ризики; превентивні заходи; система управління базами даних.

Безопасность баз данных:
угрозы и превентивные меры

В.Я. Певнев, С.Д. Капчинский

Есть большое количество угроз и уязвимостей, которые могут возникнуть при разработке, управления и поддержки различных баз данных и систем управления базами данных. **Целью статьи** является проведение углубленного анализа описанных угроз и определение наиболее оптимальных мер для их устранения. **Задача:** провести углубленный анализ угроз и уязвимостей и выбрать наиболее распространенные и самый проблематичные из них, проанализировать и предложить оптимальные из превентивных мер или решений для каждой из просмотренных угроз. Среди **проанализированных угроз** были выбраны: чрезмерные привилегии (excessive privileges), входящие инъекции (input injections), вредоносное программное обеспечение (malware), слабый аудиторский след (weak audit trail), недостаточный уровень безопасности резервных копий (backup exposure), слабая аутентификация (weak authentication), внутренние уязвимости баз данных и неправильная конфигурация (DB vulnerabilities & misconfiguration), неуправляемые конфиденциальные данные (unmanaged sensitive data), отказ в обслуживании (denial of service), потеря списанных носителей информации (loss of outdated storage devices), низкий уровень экспертизы безопасности и низкий уровень образования работников (limited security expertise & education). Для каждой из перечисленных угроз проанализированы и определены оптимальные меры для их устранения. **Выводы**. Базы данных является основной частью любой современной информационной системы. Очень важно создать среду, которая сможет защитить данные и саму базу данных. Со временем становится труднее достичь этой цели. Быстрый рост создания и потребления данных приводит к увеличению нарушений данных и выявлению новых уязвимостей. Данная статья нацелена на популяризацию идеи безопасности баз данных и предлагает четкий набор правил и действий, направленных на снижение рисков, связанных с конфиденциальностью, целостностью и доступностью данных. Как следует из обзора перечня представленных уязвимостей, нетрудно заметить, что важнейшим пунктом безопасности баз данных является персонал, отвечающий за управление и разработку базы данных.

Ключевые слова: безопасность; угрозы; риски; превентивные меры; система управления базами данных.