Digitalization and Innovative Development of Mining Processes

Dmitriy Stenin[1], *Natalya* Stenina[1], *Arman* Akanov[2], and *Kakim* Sagindikov[3]

[1]T.F. Gorbachev Kuzbass State Technical University, 650000 Kemerovo, Russian Federation
[2]Kazakh Humanitarian Juridical Innovative University, Semey, Kazakhstan
[3]L.N.Gumilyov Eurasian National University, Nur-Sultan, Kazakhstan

Abstract. This article discusses the issues of digitalization and using of information technologies, and in particular databases at all stages of the technological process of mining. In addition, the paper proposes options for protection against some of the possible attacks and information protection using countermeasures and control methods that exist at the present time. Database security is an important approach for planning and decision-making clear the security requirements of the database. Database security, especially for an industry such as mining, is a very important issue for companies. With increasing complexity of the databases, we may encounter with more complex problems related to information security.

1 Introduction

At the present time, digitalization is an integral part of innovation and long-term development of almost any sector of the economy. Of course, this trend could not ignore one of the most important industries for many countries and regions, as the mining industry. Moreover, digitalization has affected all stages of mining – it is the process of mining, transportation, enrichment, environmental safety and many others. One of the main stages and elements of the process of digitalization is the creation of databases, using which in the future it is possible to effectively use information technology in the development of mining technology. In today's world, data is generated at a very high speed, and the final destination of such data is the database. The data is stored in a database for a simple and efficient way to manage this data. All data manipulation and maintenance operations are performed using a database management system. Given the importance of data in the organization, it is absolutely necessary to ensure the security of the data present in the database. A secure database is one that is reciprocal from various possible database attacks. Security models need to be developed for databases. These models differ in many aspects because they deal with different database security issues. They may also differ because they accept different assumptions about what constitutes a secure database. Thus, it becomes very difficult for database security personnel to choose the right model to protect their information.

A database of any stage in mining technology can be defined as a set of data that is stored on the hard disk of a computer system. Databases allow any authorized user to quickly and easily access, enter and analyze data. It is a collection of queries, tables, and views. Data stored in databases are typically organized to model aspects that support processes that require information storage and retrieval. Most of the data is stored in a store called a database. The user interface for databases is called the database management system. DBMS is a software application that interacts with an authorized user, other applications and the database itself to collect and analyze data. It helps to organize data for better performance and faster searches by maintaining an index. DBMS performs the function of concurrency control. The DBMS also performs data recovery operations on the database. Today, mining companies need databases to store any type of data.

The problem of database security. The pace of development of information technologies over the past 20 years has contributed to the introduction of computer tools in all spheres of human activity. This in turn affected the reverse side of the process. That is, interest in data circulating within the information system (IP) arose not only from legal users and owners, but also from attackers. Therefore, the solution of the problem of information security of computer systems, including databases (DB), as the main element of IP, has become one of the priorities. In this case, database security remains one of the most difficult challenges facing the information security units. The problem of solving the latter is compounded by the fact that there is no clear methodology for its comprehensive solution, which would be applied in all cases. This is due to the variety of activities of enterprises, the structure of information networks, data flows, applications and processing methods, etc. Therefore, in each case, the problem should be solved individually [1].

The advantage of using databases in the mining industry is that it automates various procedures, saving resources and personnel.

For example, instead of entering information about stocks, production volumes, the availability of mined minerals in warehouses and many, many other data manually, the digitalization of the industry allows, by creating appropriate databases, to quickly manage and control all processes occurring at each stage of mining, their enrichment and delivery to their places of consumption. Manual scanners can be used to store information in a database. The database can provide efficiency and speed in a modern workplace. The next question for any organization is "is the information protected by a database". Information security in the modern world, including the mining industry, is one of the important and complex challenges that people face around the world at every stage of their lives. Databases are complex and many database security professionals do not fully understand the risks and security issues associated with different databases. According to it professionals and database administrators, many do not know which databases, tables, and columns contain sensitive data because they either process outdated applications or because there are no data model records or documentation. Even with full knowledge of database assets, protecting them is more difficult because there are unique implementations and procedures for databases. We can say that database security is the use of a wide range of security measures to protect databases from any attacks (internal or external), from compromising the confidentiality, integrity and availability of databases. Security includes various types of controls, such as technical, administrative and physical controls. Similarly, security in the electronic world is of great importance. The protection of sensitive data stored in the storage is actually the protection of the database [2].

2 Discussion

Databases today are faced with various types of attacks. Before describing database security methods, it is preferable to describe the attacks that can be performed on databases. Basic database attacks can be classified as shown in figure 1.

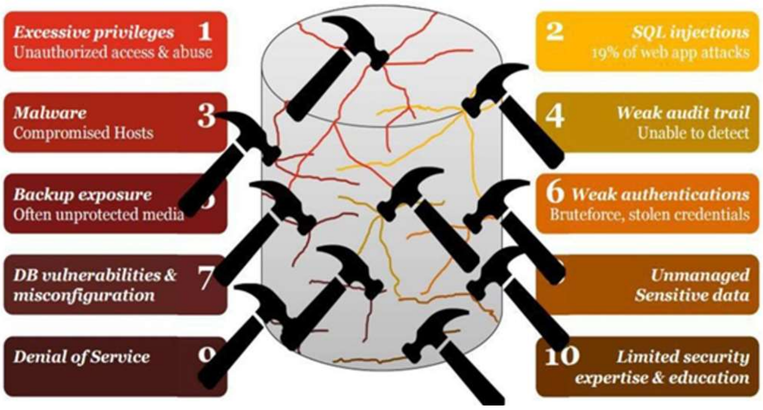

Fig. 1. Database threats.

Database privileges can be used in many ways. The user may abuse the privileges for unauthorized purposes. Abuse of privileges can be of different types: excessive privilege abuse, legitimate privilege abuse and misuse of unused privileges. This type of threat is most dangerous because authorized users are using data for other purposes. These privileges can be abused and create unnecessary risk.

Granting excessive permissions is problematic for two reasons. About 80% of attacks on these companies are actually carried out by employees or former employees. The granting of too many privileges, or the untimely revocation of those privileges, makes it too easy to carry out their offences. Some of these actions may even be performed unintentionally or without being perceived as illegal.

Abuse of legitimate privileges can be considered a database vulnerability if a malicious user abuses their database access privileges.

The information security management system (ISMS) has become more important for any organization to securely manage its information assets. ISMS is a management system that includes the management of people, processes, and technologies to create, implement, operate, monitor, analyze, maintain, and optimize information to preserve the confidentiality, integrity, and availability of information. However, the IMS is a complex management system and therefore it is not easy for the organization to establish its own IMS and for staff to work in accordance with the IMS [3-4].

Countermeasures for abuse of privileges include

1. Access control policy: do not grant unnecessary privileges to the user.
2. Legitimate abuse of privileges can be stopped by ensuring good auditing.

Database systems are used for backend functionality. User-provided data as input is often used to dynamically construct SQL statements that directly affect databases. Input injection is an attack aimed at undermining the original intent of an application by passing the attacker-provided sql statements directly into the backend database.

There are two types of input:

1. SQL-injection
2. NoSQL Injection.

SQL injection: designed for traditional database system. This attack typically include the introduction of unauthorized applications into the input fields of applications.

NoSQL Injection: designed for large data platforms. This type involves the insertion of malicious statements in such large data components like Hive, MapReduce.

In SQL and NoSQL, a successful data entry attack can give an attacker unrestricted access to the entire database.

Countermeasures of input injection

1. Use a stored procedure instead of implementing direct queries.
2. Implementation of MVC architecture.

Malicious

Cybercriminals, government-sponsored hackers and spies use sophisticated attacks that combine various tactics, such as copying phishing emails and malware, to infiltrate organizations and steal sensitive data. Don't know that malware has infected their device; legitimate users become a channel for these groups to access your networks and sensitive data.

Malware countermeasures

Turn on the firewall and install antivirus.

Weak audit trail

Weak audit policies and technologies present risks in terms of compliance, deterrence, detection, forensics and recovery.

Automatic recording of database transactions with sensitive data must be part of any database deployment. Failure to collect detailed audit records of database activities poses a serious organizational risk at many levels. Organizations with weak database audit mechanisms are increasingly finding that they are in conflict with industry and government regulatory requirements. Most auditing mechanisms do not know who the end user is because all actions are associated with the web application account name. Reporting, visibility and forensic analysis are difficult because there is no reference to the responsible user. Finally, users with administrative access to a database obtained in a legitimate or malicious way can disable built-in database auditing to hide fraudulent activity. Audit capabilities and responsibilities should ideally be separate from database administrators and the database server platform to ensure strict segregation of duties [5].

3 Results

Weak audit countermeasures

1. Network auditing tools are a good solution. Such devices should not affect the performance of the database, work independently of all users and provide detailed data collection.

Backup copying

Backup media is often fully protected from attack. As a result, numerous security breaches have led to the theft of disks and backup tapes of the database. In addition, failure to audit and monitor the actions of administrators who have low-level access to sensitive information can put your data at risk. Taking appropriate measures to protect your confidential data backups and monitor your most privileged users is not only a best practice in the field of data security, but also a mandatory requirement of many regulations.

Backup countermeasures

1. Database encryption. Store data in encrypted form, as this helps protect both production and database backups, and then verify activity and control access to sensitive data from users who access databases on the operating system and storage tiers. By using database auditing along with encryption, organizations can monitor and control users both inside and outside the database.

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. The implementation of passwords or two-factor authentication is mandatory. For scalability and ease of use, authentication mechanisms must be integrated with the enterprise directory / user management infrastructure.

Database vulnerabilities and misconfiguration

You can usually find vulnerable and nonproprietary databases, or you can find databases that still have default accounts and configuration settings. Attackers know how to exploit these vulnerabilities to launch attacks on your organization. Unfortunately, organizations often find it difficult to maintain the database configuration even with patches. Typical issues include high workloads and mount backups for associated database administrators, complex and time-consuming requirements for patch testing, and a search issue [6-7].

Access control

Access control is one of the main services that any data management system should provide. This is protected data from unauthorized read and write operations. Access control determines that all communications with the database and other system objects strictly follow the policies. Errors can be so serious that they can create problems in the work of the company. Access control can also help reduce risks that can accurately affect the security of the database on the primary servers. For example, if a table is deleted or access is changed accidentally, the results can be rolled back or for certain files, but by applying access control, deleting them can restrict.

Access control systems include:

1. File permissions – create, read, edit or delete files on the file server.
2. Program access rights – the right to run the program on the application server.
3. Data rights – the right to receive or update information in the database.

Output policy

It is very important to protect data at a certain level. It can be used when you want to prevent the analysis of certain data in the form of facts at a certain higher level of security. This helps you determine how to protect information from being published.

The purpose of output control is to prevent indirect disclosure. Typically, there are three methods of unauthorized disclosure:

1. Correlated data – typical channel, when the visible data X is semantically connected to invisible data Y
2. Missing data – the result of the query contains NULL values that mask sensitive data. The presence of this data can detect this.
3. Statistical inference is typical for databases that provide statistical information about objects.

User identification / Authentication

The basic security requirement is that you should know your users. You must identify them before you can determine their privileges and access rights so that you can verify their actions with the data.

A user can be authenticated in a variety of ways before being allowed to create a database. Database authentication includes both user identification and user authentication. External authentication can be performed by the operating system or a network service. Also user authentication can be defined using Secure Socket Layer (SSL), through enterprise roles, through middle-level server authentication, also known as proxy authentication.

This is the most basic security requirement because the identification process identifies the group of people who are allowed access to the data. To ensure security, the identity card is authenticated and it protects sensitive data from unauthorized alteration.

An attacker can use various approaches such as bypass authentication, default password, privilege escalation, brute-force password guessing, and rainbow attack when they attempt to compromise user identification and authentication [8-10].

Accountability and audit

Auditing is the monitoring and recording of configured database actions, from both database users and the users who are not database users. Accounting is the process of keeping a control log of user actions in the system. Accountability and audit checks are necessary to ensure the physical integrity of data that requires specific access to databases and that is processed through auditing and records management.

If a user has successfully authenticated and is trying to access a resource, the system should monitor both successful and unsuccessful attempts, and access attempts and their status should be displayed in the audit log files.

Encryption

Encryption is the process of converting information into cipher or code so that it cannot be read by anyone else except those who hold the key to the cipher text. Encrypted text or encoded text is called encrypted data.

There are two States of data protection in the database. The data can exist either at rest – the data can be stored in a database or on a backend tape, or during transmission – the data transmitted over the network dictate different solutions for encrypting the transmitted data. Data encryption can solve some problems with data at rest. For Data at Transit, you need to use solutions such as SSL / TLS.

4 Conclusion

To sum up, protecting access to information about the processes and stages of mining technology in databases starts with who can access the data and what types of data the attackers want to access.

There are many opportunities to improve the methods used to protect the database. According to the survey, 84% of companies believe that database security is adequate. 73% of the companies that forecast joining the database will grow day by day. 48% of attackers are authorized users. 48% of users abused their privileges. Issues related to database security are also discussed.

Submitted several proposals for discretionary and mandatory security models for the protection of conventional databases. However, there is no standard for developing these security models. The work presented in this article provides information about the various threats and security problems of the database used in all industries, including mining. It can be extended to define, design, and implement effective security policies in a database environment and provides a consolidated view of database security.

References

1. V. I. Esin, S. G. Rassomakhin, V. M. Grachev, N. G. Polukhina, Bulletin of the Lebedev Physics Institute, **41:5**, 123 (2014)
2. A. Fedorchenko, A. Chechulin, I. Kotenko, Proceedings of 23rd Euromicro International Conference on Parallel, Distributed, and Network-Based Processing, **559,** 24 (2015)
3. A. I. H. Suhaimi, Y. Goto, J. Cheng, Transactions on Information and Systems, **E97:6**, 1516 (2014)
4. H. Y. Zhao, X. Y. Liu, Z. Jing, Applied Mechanics and Materials, **397**, 2536 (2013)
5. N. V. Mostovaya, E. V. Lebedenko, Proceedings of the XXIV-th International Open Science Conference, **97**, 7 (2019)
6. O. Outhavong, *Security in a distributed object-oriented database in the context of a three-tier architecture illustrated with the implementation of a flight safety information system* (CKUF, Beijing, 2002)

7. A. Lehew, *Globalization of the enterprise database environment: a qualitative study of data security experience* (SMJS, Praha, 2005)
8. P. Horak, L. Brankovic, M. Miller, applied mathematics, **91:1-3**, 119 (1999)
9. S. H. Son, Journal of Systems Architecture, **46:4**, 397 (2000)
10. H. Min-Shiang, Y. Wei-Pang, Journal of Systems and Software, **31:3**, 257 (1995)