

THREATS TO THE DATABASE AND TECHNOLOGIES FOR THEIR PREVENTION

Abdusamatova Shaxodat Khojiakbar's daughter

Informatics and information technology teacher at the academic lyceum named after Islam Karimov at the Almalyk branch of TDTU phone: +998(93) 375 – 42 - 15 e-mail: abdusamatovashahodat@gmail.com,

Mannonov Asliddin Akbar's son

Student of cyber security faculty of TATU named after Al Khorazimi, phone: +998(97) 960-03-02, e-mail: asliddinmannonov0980@gmail.com.

Abstract: *This article presents various risks to the database and the information contained in it, as well as modern technologies for their prevention.*


Key words: data warehouse, cyber attack, threat to information, technology

Digital data is becoming more and more important in our lives, which has improved the processes of storing, collecting, processing and transmitting them. The environment in which electronic information is stored is called a data warehouse, and it is designed differently according to the user's requirements. Any data warehouse certainly attaches great importance to the safety of the information contained in it, the protection of all rights of users at a high level, and does everything possible for this. Database security includes various measures used to protect database management systems from malicious cyber-attacks and illegal use. Database protection programs are designed to protect not only the data in the database, but also the data management system itself and every application that is part of it from misuse, damage, and attack. Database security includes the tools, processes, and methodologies that ensure security in a database environment. Many software vulnerabilities, misconfigurations, misuse, or carelessness can cause crashes. In order to properly design the data warehouse and ensure its security, it is necessary to know in advance various threatening factors and to take measures against them. Below are the factors causing these threats and their types:

An insider threat is a security risk from one of the following three sources, each of which has privileged access to the database:

- Malicious insider
- A careless person within an organization who exposes a database to an attack through careless actions





- An outsider who obtains credentials or has access to database credentials through social engineering or other methods

An insider threat is one of the most typical causes of database security breaches, often occurring because many employees have been granted privileged user access. How insider threats drive your data protection strategy.

Human error. Weak passwords, password sharing, accidental deletion or corruption of data, and other inappropriate behavior still account for nearly half of all reported data breaches.

Exploitation of vulnerabilities in database software. Hackers are always trying to isolate and target software vulnerabilities, and database management software is a very valuable target. New vulnerabilities are discovered every day, and all open source database management platforms and commercial database software vendors regularly release security patches. However, if you do not apply these patches quickly, your database may be vulnerable to attack.

SQL/NoSQL counterattacks. A database-specific threat involves the use of arbitrary SQL and SQL attack strings in database queries. Typically, these are requests created as extensions of web application forms or received via HTTP requests. Any database system is vulnerable to these attacks if the developers do not follow secure coding practices and the organization does not perform regular vulnerability testing.


Buffer overflow attacks. A buffer overflow occurs when a process tries to write more data to a block of memory than is allowed. Attackers can use redundant data stored in adjacent memory addresses as a starting point to launch attacks.

Denial of Service (DoS/DDoS) attacks. In a Denial of Service (DoS) attack, a cybercriminal overwhelms a target service, namely a database server, using a large number of fake requests. As a result, the server cannot handle the requests of real users and often crashes or becomes unstable.

In a distributed denial of service (DDoS) attack, spoofed traffic is generated by a large number of computers participating in a botnet controlled by an attacker. This generates very large volumes of traffic that are difficult to stop without a highly scalable defense architecture. Cloud DDoS protection services can be dynamically scaled to handle very large DDoS attacks.

Malware is software written to exploit vulnerabilities or damage a database. The malware can arrive through any endpoint device connected to the database network. Malware protection is important for any endpoint, especially database servers because of their high cost and vulnerability.





In order to prevent these dangerous factors, it is possible to apply the following measures:

- Strong passwords should be used - in case of possible or random access to the database;
- Password hashes must be configured and stored encrypted - this prevents password copying or distribution;
- Accounts should be blocked after several login attempts - this prevents unknown logins;
- If employees move to different positions, leave the company, or do not require the same level of access, accounts may be regularly audited and deleted, and other measures may be taken.

REFERENCES:

1. Michael Cobb "7 Best Practices for GDPR Compliance"
2. "Cyber security against cybercrime" Abdurasul IMINOV, head of the Department of Information Technologies of the Ministry of Internal Affairs, lieutenant colonel
3. "Guide to security technologies and trends in 2022" e-guide

