



foi

X

esiea

Database Security and Protection

Prepared by:

Ilan YAKOUBI

September 18, 2024



Introduction

Before we get into the details of database protection and security, it is important to understand what databases are and how they work. A database is an organized collection of structured information, or data, typically stored electronically in a computer system.

A database is usually controlled by a database management system (DBMS). Data within the most common types of databases in operation today is typically modeled in rows and columns in a series of tables to make processing and data querying efficient.

The data can then be easily accessed, managed, modified, updated, controlled, and organized. Most databases use structured query language (SQL) for writing and querying data. SQL is a programming language used by nearly all relational databases to query, manipulate, and define data, and to provide access control.


If you must remember one thing, databases help companies to accelerate their growth and improve their performance by managing their data effectively.

During this essay we will see how databases are protected to ensure database security, then we will see the current threats against companies. Finally, we will find solutions to counter the attackers. In the concluding section, I would give my opinion and vision on database protection.

Database security organization

Database security is the processes, tools, and controls that secure and protect databases against accidental and intentional threats. The objective of database security is to secure sensitive data and maintain the confidentiality, availability, and integrity of the database.

In addition to protecting the data within the database, database security protects the database management system and associated applications, systems, physical and virtual servers, and network infrastructure.



Common threats and challenges

Numerous configuration errors, vulnerabilities or patterns of neglect or misuse of software can lead to violations. An internal threat is a security threat from one of three sources with privileged access to the database: malicious internal employee, negligent internal employee who makes mistakes or a person outside the company who obtains in some way identifying information.

Human error is the most exploited nowadays, it's called social engineering. Accidents, weak passwords, password sharing and other reckless or misinformed behavior continue to account for nearly half (49%) of all reported data breaches.

Then there is the famous SQL attack, potential problems may arise because most web forms have no way to stop entering additional information into the forms. Hackers can exploit this vulnerability and use the form input boxes to send their own requests to the database.

There are also the attacks by buffer overruns, a buffer overflow occurs when a process tries to write more data into a fixed-length memory block than it is allowed to contain. Of course there is malware that is software written specifically to exploit vulnerabilities or damage a database in any way.

Organizations that do not protect backup data with the same stringent controls used to protect the database itself may be vulnerable to backup attacks. One well-known attack in the computer world is DoS.

In a denial of service (DoS) attack, the attacker overwhelms the target server (the database server) with so many requests that it can no longer respond to legitimate requests from real users and, in many cases, becomes unstable or fails.

The importance of database security

The harm to a company from a data breach depends on a number of consequences or factors. Intellectual property compromised, as IP information may be critical to the ability to maintain a competitive advantage in the marketplace, and in the event of theft or disclosure of IP information it can be difficult, It is impossible to maintain or recover competitiveness.

Brand damage is also a factor, as customers or partners may not want to purchase products or services if they feel they cannot be trusted to protect their data or their own.

Business continuity (or lack of continuity) is also a factor, as some businesses cannot continue to operate until a breach is resolved. In addition, there are fines or penalties for non-compliance because the financial impact of not complying with global regulations.

Such as the Sarbanes-Oxley (SAO) Act or the Payment Card Industry Data Security Standard (PCI DSS), the Health Insurance Portability and Accountability Act (HIPAA) or regional data privacy regulations such as the European General Data Protection Regulation (GDPR), can be devastating.

Fines may exceed, in the worst case, several million dollars per violation. Finally, there are the costs of repairing violations and notifying clients because in addition to the cost of communicating with clients.

An organization that is the victim of a violation must pay for investigation and investigation, crisis management, triage, repair of affected systems, etc.

Data risk prevention

Securing or "strengthening" a database server combines physical security, network and operating system to fix vulnerabilities and make it harder for hackers to access the system. Based on my extensive research, I will now explain the best defense solutions to ensure maximum security.

Data encryption makes it easier for organizations to secure their data: "always encrypted data" offers integrated protection against theft in transit, in memory, on disk and even during query processing. "Transparent data encryption" protects against the threat of malicious offline activity by encrypting stored data.

Alerts are created for suspicious activities, such as SQL injection attacks or potential data infiltration and brute force. It is recommended that users and applications use separate accounts to authenticate. This limits permissions to users and applications, and reduces the risk of malicious activity.

The principle of security of information with least privilege states that users and applications should be granted access only to the data and operations they need to perform their tasks. A zero-trust security model validates device identities and compliance for each access request to protect people, devices, apps and data wherever they are.

The principle of Trust Zero is "never trust, always check." What will help the protection of systems will also be to use powerful security tools set up by specialized companies such as Azure, IBM Guardium, AWS, Oracle Database or Imperva company.

In addition to implementing security controls, the law requires you to establish appropriate controls and policies for database access. Administrative controls to govern the installation, modifications and management of the database configuration. Preventive controls to

regulate access, encryption, semantic tagging and masking. Detection controls to monitor database activity and data loss prevention tools.

Conclusion

In the future , cyber attacks will multiply so it is essential to train future professionals. More than 3.5 million cybersecurity positions are open worldwide, according to the 2021 Global Digital Trust Insights study.

First, it is in teaching, the transmission of knowledge. If this teaching phase is successful, cybersecurity experts will be able to protect users.

Now let's talk more technical, the tools or practices of data security must be highly scalable in order to meet future needs in both the short and long term.

Database security policies should be integrated with and support your overall business objectives, such as protecting critical intellectual property data and your cybersecurity and cloud security policies.

Anticipation is an important element to consider. When an organization is better prepared in case of crisis, it knows how to react, this reduces the damage from a cyber attack.

More generally, the most worrying thing for the future is AI. It is a source of innovation in many areas, including medicine and transportation, but it also facilitates cybercrime. As for machine learning models, they could be used for illicit or devious purposes. Governments and organizations still lack the specialized knowledge to implement adequate monitoring and control systems.

In any case, we can never have a digital world without there being any loopholes. However, the goal of future cybersecurity experts is to minimize the dangers and always be ahead of attackers.

References

- *Oracle. "What Is a Database?" Wwww.oracle.com, 24 Nov. 2020,*
www.oracle.com/database/what-is-database/
- *Oracle. "Pourquoi Utiliser Une Base de Données." Oracle France, 21 June 2023,*
<http://www.oracle.com/fr/database/pourquoi-utiliser-base-de-donnees/>
- *Microsoft. "Database Security Best Practices and Solutions | Microsoft Azure." Azure.microsoft.com, 2024,*
azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-database-security
- *IBM. "Sécurité Des Bases de Données : Guide Essentiel | IBM." Wwww.ibm.com, 10 May 2023,*
www.ibm.com/fr-fr/topics/database-security
- *Kaspersky. "Qu'est-Ce Qu'une Injection SQL ? Définition et Explication." Wwww.kaspersky.fr, 9 Aug. 2023,*
<http://www.kaspersky.fr/resource-center/definitions/sql-injection>
- *(Microsoft, "Meilleures Pratiques et Solutions de Sécurité de Base de Données | Microsoft Azure")*
<https://azure.microsoft.com/fr-ca/resources/cloud-computing-dictionary/what-is-database-security>

