What is Database Security and how to secure the database effectively?

Database security refers to the measures taken to protect a business's data from unauthorized access, disclosure, alteration, or theft.

As information technology is increasingly developing, businesses are facing many challenges related to securing sensitive information from threats. At this time, database security is one of the most important issues. So how to secure the database, let's find out with ***TipsMake*** right through the article below.

What is Database Security?

In the simplest terms, database security refers to the measures taken to protect a business's data from unauthorized access, disclosure, alteration or theft. These security measures may include techniques, processes, etc. to ensure that the business's data is stored securely. This is especially important in the context of data being considered a valuable asset of each individual and business.

Database Security

How to secure your database yourself?

To secure your database yourself, you can apply some effective methods and measures. Here are some effective measures that you can take.

Ensure physical database security

To secure your database, the first thing you need to do is to ensure the physical security of your database. Make sure that the server that hosts your database is located in a safe location, away from natural threats such as storms, floods, and earthquakes.

You need to control who has access to the physical database. Only those with the right tasks and authority can access the servers.

Use appropriate permissions

It is important to define who has access to data and what their permissions are. Make sure each user only has access to the data they need to do their job. Determining appropriate permissions reduces the risk of unauthorized access being abused.

Regularly check and patch

To secure the database, we need to regularly check and update patches to fix errors and fix security holes that attackers can exploit. Create a specific testing schedule to avoid becoming a target of attacks.

Block public network access

Public Wi-Fi networks can pose serious security risks, so it's important to protect your personal information and important data. Prioritize using a VPN to encrypt your connection and set up a strong firewall to prevent unauthorized access.

Encrypt files and data backups

Stolen data is a disaster, but what's worse is having that data readable by an attacker. Protect your sensitive information by encrypting it from the start. This applies not only to data in use but also to backups. Don't let your hard work and information be stolen so easily.

Set up HTTPS server

Using the HTTPS protocol is an effective way to protect information transmitted over the network. This protocol uses SSL/TLS encryption to protect data when sent from the server to the user's browser, which will effectively protect personal information and enhance the reliability of the website.

Separate database servers

Use separate network architectures for database servers and application servers to enhance security. This way, even if the web server is attacked, the attacker cannot easily access the database.

Manage user access and passwords

Users should create strong passwords that include uppercase letters, lowercase letters, numbers, and special characters to protect their data. In addition, change your password regularly to minimize the risk of being

hacked. Or you can also use 2-factor authentication to further protect your account.

Regularly check database security

You should perform regular database security audits to detect vulnerabilities and weaknesses in your system. This includes testing fake attacks to determine the database's defenses. Once vulnerabilities are discovered, take immediate action to ensure data security.

Regularly check database security

Real-time database monitoring

Real-time database activity monitoring is one of the effective ways to detect and respond to threats quickly. By tracking unusual or unusual activities, you can detect potential attacks or incidents in a timely manner.

Using Web Applications and Firewalls

Using a web application firewall (WAF) is an effective way to protect your database from external attacks. A WAF monitors and filters HTTP traffic between your web application and the Internet, helping to protect your applications from a variety of attacks such as SQL injection, cross-site scripting, and other threats.

Deploying a WAF not only protects the database but also improves application availability by minimizing unwanted traffic, thereby improving operational performance.

Conclude

Applying the security measures shared above is a way to help you build a safe environment for your data. Remember that security is an ongoing process and needs to be reviewed, tested and updated regularly to deal with new threats. If done properly, you can rest assured that your database is being effectively protected.