How To Secure SQL Server

The SQL server is a widely renowned relational database management system and is regarded as one of the most prominent legacy software products launched by Microsoft.

With organizations storing valuable information in their database systems, they are often a prized target for cyber criminals that are on the lookout for any loopholes that they can exploit.

And so, this article will list down tips for securing your SQL server against cybersecurity threats;

Reduce Attack Surface Area

In essence, surface area reduction is an advanced security protocol that includes either stopping, or at the very least disabling, components that are not in use anymore.

In SQL servers, implementing surface area reduction helps improve security by narrowing down the number of avenues available for potential attacks on a system. The lesser the components on the server, the lesser the areas that hackers can access.

The most important part of limiting the attack surface area of an SQL server is to run the required services that have the 'least privilege' by only allowing appropriate usage rights to users and services.

Deploy Strict Permissions

Much like services in the database, users of the database should also only have access that is required to complete their assigned tasks; this principle is known as 'least privilege.'

In the SQL environment, this means that staying as far away as possible from enabling 'ALL' grants in MySQL and sysadmin role membership in MSSQL. Additionally, you can change read access allowed to employees by letting them see views instead of tables. This allows you to hide and protect any sensitive fields that may require protection.

Even automated tasks, such as stored procedures and maintenance plans, should be run as dedicated users that have the required permission. Regulated permission levels prohibit any one component from damaging the entire database if compromised.

Ensure Backup Security

Backups are extremely vital data deposits that allow you to store your data in a secure environment, ready to be used if something goes wrong with the primary database; this is why organizations need to ensure maximum security for their backup.

Since the SQL Server 2014, users can encrypt their database backups while they are creating a backup! Unlike conventional database backup encryption methods that require you to encrypt the entire backup once it is created, this method offers greater efficiency.

To encrypt the backup as it is being saved in the storage, you require two things in the SQL environment:

- **Encryption Algorithm**: This specifies the algorithm to follow for the encryption procedure. SQL server supports a wide array of encryption algorithms such as AES 128, AES 192, AES 256 and Triple DES.
- **Encryptor:** To secure the encryption – this can either be an asymmetric key or a valid certificate.

Protect Your Connections

The connections that have access to your database should be encrypted to avoid any unauthorized access from sabotaging your connection and getting to your data.

With SQL, you have the option to use Transport Layer Security (TLS) to encrypt data that is being transmitted across the server instance and a client application that has requested access. Performed within the protocol layer, this encryption is available to all supported SQL server clients.

While enabling this option surely increases the security of your data in transit, the additional layer of security comes with a number of prerequisites:

- An additional network roundtrip, initiated at every connect time instance.
- Any data packets that travel from the application to the SQL server are to be encrypted by the client's TLS stack and decrypted through the server TLS stack.
- The opposite is true for packets that travel from the SQL server to the application. They are encrypted by the servers TLS stack while the decryption process takes place at the client's TLS stack.

As the emphasis on database security continues to grow, organizations are increasingly investing in ways to secure their SQL server databases.

Experienced managed service providers, like Agio, help organizations implement advanced database management solutions and infrastructure support.

Interested in learning more? Contact us today.