Securing SQL Server: Disable CLR

CLR (Common Language Runtime) is a feature of SQL Server that allows you to create and run managed code within the database engine. Enabling CLR on SQL Server allows you to create stored procedures, triggers, and functions using languages such as C# and VB.NET.

While CLR can be a useful feature, it can also be a security risk if not properly managed. This is because CLR allows you to execute arbitrary code within the database engine, which can potentially be exploited by attackers.

To mitigate the security risks associated with CLR, it is important to carefully manage the permissions of users who are allowed to create and execute CLR assemblies. This can be done by granting the necessary permissions only to trusted users, and by carefully reviewing and testing any CLR assemblies before they are deployed to the database server.

In addition, it is important to enable the "CLR strict security" option, which allows you to specify which CLR assemblies are allowed to be loaded into the database engine. This can help to prevent malicious assemblies from being loaded into the database.

To disable CLR on a SQL Server instance, you will need to use the sp_configure system stored procedure. To do this, follow these steps:

Connect to the SQL Server instance using SQL Server Management Studio or another tool that allows you to execute Transact-SQL statements.

Run the following command to enable the advanced options:

```
EXEC sp_configure 'show advanced options', 1;
RECONFIGURE;
```

Run the following command to disable CLR:

```
EXEC sp_configure 'clr enabled', 0;
RECONFIGURE;
```

Run the following command to disable the advanced options:

```
EXEC sp_configure 'show advanced options', 0;
```

```
RECONFIGURE;
```

Restart the SQL Server service to apply the changes.

After you have disabled CLR, users will no longer be able to create or modify CLR objects in the database. If you need to re-enable CLR, you can use the same steps, but set the value to 1 instead of 0 in step 3.

It's important to note that disabling CLR will not affect any existing CLR objects in the database. These objects will continue to function as normal until they are dropped or modified. However, you will not be able to create new CLR objects or modify existing ones until CLR is re-enabled.

CLR is a powerful feature of SQL Server that can be a security risk if not properly managed. It is important to carefully manage the permissions of users who are allowed to create and execute CLR assemblies, and to enable the "CLR strict security" option to help prevent the loading of malicious assemblies into the database.

Want to learn more about securing your SQL Server, take a look at my free white paper on sever steps to help harden your SQL Server.

Securing SQL Server Whitepaper.