Securing SQL Server: CHECK_Expiration for SQL Server logins

The CHECK_EXPIRATION option is a security feature of SQL Server that allows you to enforce password expiration for SQL Server logins. When this option is set to ON for a login, it requires the login to change its password after a certain period of time has passed.

Setting the CHECK_EXPIRATION option to ON for all SQL authenticated logins within the sysadmin role is an important security measure because it helps to ensure that the passwords of users who have administrative privileges on the database server are regularly changed. This can help to reduce the risk of password-related attacks, such as brute force attacks or password cracking.

To set the CHECK_EXPIRATION option to ON for all SQL authenticated logins within the sysadmin role, you can use the following T-SQL command:

```
USE [master];
GO
ALTER LOGIN [sysadmin_login] WITH CHECK_EXPIRATION = ON
```

This command will enable the CHECK_EXPIRATION option for the specified sysadmin login. It is important to note that this will not affect other logins, or logins that are not within the sysadmin role.

```
SELECT *
  FROM sys.sql_logins
 WHERE is_expiration_checked = 0
 AND name NOT LIKE '##%';
```

Setting the CHECK_EXPIRATION option to ON for all SQL authenticated logins within the sysadmin role is an important security measure that can help to ensure that the passwords of users who have administrative privileges on the database server are regularly changed. This can help to reduce the risk of password-related attacks and improve the overall security of your SQL Server installation.

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.