MS SQL DBA CAPSTONE PROJECT - 1

Problem Statement:

Company XYZ is a large pharmaceutical company that markets various medical products to smaller pharmaceutical companies worldwide. As SQL Server has a good track record with few vulnerabilities and weak points.

Company XYZ uses SQL Server as a main database technology. Its SQL Server databases store the company's confidential data such as customer information, card details and employee information. This data is originally ported from Excel spread sheets.

In recent years, however, Company XYZ has experienced significant growth in all areas of its business. Over the last year, the business has been in the press for the wrong reasons: leaked customer data, unauthorized access and other reasons caused by its unsecure SQL Server infrastructure.

How would you address all such security concerns?

Solution:

I understand that Company XYZ has experienced significant growth in all areas of its business and has been in the press for the wrong reasons due to leaked customer data, unauthorized access, and other reasons caused by its unsecure SQL Server infrastructure.

To address these security concerns, I would recommend the following best practices:

1. Use strong passwords: Ensure that all SQL Server logins and passwords are strong and complex. Passwords should be at least 8 characters long and should include a mix of uppercase and lowercase letters, numbers, and special characters.
2. Encrypt sensitive data: Use SQL Server's encryption features to encrypt sensitive data such as customer information, card details, and employee information. This will help protect the data from unauthorized access.
3. Implement access controls: Use SQL Server's access control features to restrict access to sensitive data. Only authorized users should have access to the data.
4. Regularly update SQL Server: Ensure that SQL Server is regularly updated with the latest security patches and updates. This will help protect against known vulnerabilities and exploits.
5. Regularly backup data: Regularly backup SQL Server databases to ensure that data can be restored in the event of a security breach or other disaster.

6.Monitor SQL Server activity: Monitor SQL Server activity to detect and respond to security threats in real-time. This can be done using SQL Server's built-in auditing and monitoring features. By following these best practices, Company XYZ can help protect its SQL Server infrastructure and the sensitive data stored within it.