Unit 4 Security Best Practices

**Corey Crooks**

**Purdue University Global**

**IT350 – Advanced Database Concepts**

**Jason Johnson**

**March 1st, 2023**

Security with any database is not a concept to dismiss easily. No matter the scale of your database, any information lost or stolen proves a risk to your operation. Because of this, there are many security features found within the Microsoft SQL Database suite to help mitigate concerns and vulnerabilities in our BikeStores database object. One such tool is data encryption (Microsoft, 2023). Encryption methods found within Microsoft SQL Database’s application is used in tandem with certifications in order to scramble and de-scramble data. This will ensure that should this data be stolen, the product may be un-usable to any malicious actor that may have their hands on it. Encryption itself is a trustworthy backup, but will not suffice as the only security measure implemented. A second tool to use would be the implementation of Views to retrieve data in the database (Microsoft, 2023). Views in SQL Server will allow the user to be presented with data relating to the product of the view without actually allowing them permission to access the underlying tables of the query itself. This works to help protect personal identifying information of clients or workers that may appear in such queries. A third mechanism to consider would be that of authentication (Microsoft, 2023). As not everyone in the world would need access to the BikeStores database, it is recommended to create administrative login credentials in order to provide a layer of security to the database itself. This ensures that anyone trying to access the database will need to know the proper credentials to use for it—barring access for those without those credentials. This works in tandem with the fourth security measure; assigning roles and permissions (Microsoft, 2023). In the last example, it was mentioned that not every individual on the earth requires manipulation access to the BikeStores database, so an unrestricted login isn’t viable. So too could a case be made that not every individual working on the BikeStores database needs access to the entire database. Roles and permissions kick in to ensure that not everyone is allowed to view every table that exists in the database. This will ensure that if the login credentials of a certain individual are compromised, the attacker likely will not have access to the entire database, and thus will have been limited in their potential damage to the company.

Securities and implementations are not exactly purely beneficial, however. They will come with some delicacies that will need to be handled with care. For instance, one issue to anticipate will be the added complexity. Should roles be assigned carelessly, it is entirely possible that an individual may be locked out of the sections of the database they need access to the most; and thus will be unable to continue their work. This presents challenges to both employee morale, and productivity. Given that they will need to be re-approved for the sections they require access to, further time will be spent by a governing figure to manually update the restrictions associated to the employee in question. This time would not need to be spent if these roles were not implemented. Another concern to be cognizant of would be that of data destruction due to careless encryption implementation. As encryption works by scrambling your data, in order to get usable data back, one would need to un-scramble that same data in a specific way. This can be done with a certificate and key mechanism hosted by Microsoft SQL Server. If one has an invalid key, however, they will be unable to read the data sent to them with any accuracy or efficiency. Further time and resources must be then spent to update the licenses and keys of the system in question in order to ensure that encryption runs back on track. A final concern to think about may be often overlooked. Maintainability of code, tables, and general data of the database may be simple enough while one is looking through unhindered, but security measures may make that process significantly harder. Managing roles, encryption, certificates, and even credentials can be a difficult task when a new engineer first has hands on the database to make simple adjustments. Because of this, documentation will be required to ensure that should new faculty be assigned to this project, they are knowledgeable enough to continue with the mechanisms implemented previously. Should knowledge not be transferred, the company runs the risk of needing to start over with a whole suite of new security measures that will take additional resources and skill to develop.

There are many ways to ensure that your database complies with some security measures and best practices for today’s standards. An example of this would be researching one of the many regulation certifications available for databases. The Gramm-Leach-Bliley Act (or the GLBA) comes in three parts (University of Southern California, n.d.). Firstly, the act details the handling of private information relating to client financials in order to ensure proper transfer of information to protect the clients involved. The second part details programs involved with the transfer of such information, and could be useful as a toolset to guide a database designer through meeting regulations for financial communications. The third and final part details under what conditions access to financial information is allowed, and may restrict this access at times. This is particularly helpful to ensure a user’s data only is shared when absolutely necessary, and will help mitigate the potential opportunities their data may be exposed to malicious actors. A second regulatory requirement may come in the form of the General Data Protection Regulation (East Carolina University, n.d.). This regulation is specific to the European Union, but will be required compliance should the BikeStores database wish to partake in commerce in Europe. This law regulates the communication of sensitive information to the outside of the European Union from within. This regulation is aimed to give citizens better control over their sensitive data, and choose how data is shared with third-party vendors. These laws go a long way to ensuring that data transitions and communication methods are safe and effective, while keeping citizens’ interests and needs at the forefront of database commerce wherever they may be aligned. Because of this, proper compliance will also ensure that our company will stand in a comfortable light by ensuring the people they work with that their safety is a top-priority, and their data will be as safe as the database engineers may be able to make it.

# **References**

East Carolina University. (n.d.). *General Data Protection Regulation (GDPR)*. Retrieved from gdpr.ecu.edu: https://gdpr.ecu.edu/

Microsoft. (2023, February 28). *Choose an Authentication Mode*. Retrieved from Microsoft Learn: https://learn.microsoft.com/en-us/sql/relational-databases/security/choose-an-authentication-mode?view=sql-server-ver16

Microsoft. (2023, February 28). *Grant a Permission to a Principal*. Retrieved from Microsoft Learn: https://learn.microsoft.com/en-us/sql/relational-databases/security/authentication-access/grant-a-permission-to-a-principal?view=sql-server-ver16

Microsoft. (2023, February 28). *Securing SQL Server*. Retrieved from Microsoft Learn: https://learn.microsoft.com/en-us/sql/relational-databases/security/securing-sql-server?view=sql-server-ver16

Microsoft. (2023, February 28). *Views*. Retrieved from Microsoft Learn: https://learn.microsoft.com/en-us/sql/relational-databases/views/views?view=sql-server-ver16

University of Southern California. (n.d.). *Protection of Consumer Financial Information—Under the Gramm-Leach-Bliley Act*. Retrieved from USC Policies and Policy Governance: https://policy.usc.edu/consumer-info-privacy/