IT481 Unit 3 Discussion

Access roles should follow a least privilege policy. That is, you only grant the levels of access that are needed for any one person to complete their task. Roles that allow the ability to modify data are more restricted in terms of who receives such a role than roles that may have view-only or limited edit abilities. Therefore if an account with some role is compromised the strict policies assigned to it act as a barrier to lower-level functionality and help protect the system overall. Thus system roles can hinder if not block access to the database.

Another way to protect data is to do so while it is at rest by using encryption. Per Stouffer (2023) “Encryption converts sensitive information or data into a secret code to prevent unauthorized access”. In the event of unauthorized access encrypted data at rest requires a key in order for it to be decrypted.

It is important to protect data at rest as data can include personal information such as contact information and financial data. Encryption ensures only the intended recipient can access  the information (Stouffer, 2023). The access is granted via various means. For example, a simple user name and password for email clients where a device is typically “remembered” after the initial authentication, multi-factor authentication such as what is require for GitHub and even biometric access as might found in mobile banking applications and even laptop computers (incidentally, whole disk encryption is an option on today's computers).

Another reason to protect data at rest is that some laws require it. The Health Insurance Portability and Accountability act (HIPAA) is one such law. It requires healthcare provides to protect a patient’s medical information.

Another way to protect data at rest to conduct security reviews to ensure that the system configurations are in place as expected. As well reviewing logs – or setting alarms – for patterns of unusual activity can help uncover unauthorized access.

SecurityStudio (n.d.). *Principle of Least Privilege; Best Practice for Information Security and Compliance*. <https://securitystudio.com/principle-of-least-privilege/>

Stouffer, C. (2023, July 23). *What is encryption?* <https://us.norton.com/blog/privacy/what-is-encryption>