Cecilia Cuffe

4/18/2024

CPT 240

Security and Backup Plans

To ensure protection of all the sensitive data being stored within the database, several security and backup policies should be implemented. Of these, a few key plans to note are a password policy, an access policy, a backup policy, and a disaster recovery plan. These will not only ensure data is kept secure, but it will also make sure that in the event of any emergencies, data can be restored with as little loss as possible.

For a password policy, it is important to consider the length and complexity of the password as well as how passwords will be stored, managed, and how frequently they should be updated. In the case of this database, per the NIST password guidelines it is best practice to require passwords that are at least eight characters in length and include a variety of characters such as capital letters, lowercase letters, and special characters or symbols. These passwords should be properly encrypted through the use of hashing and salting with a private key so they are not stored in plain-text and require decryption to view. It is vital that database users do not share passwords with colleagues, and do not keep them written down or stored within their device to auto-fill. In general, passwords should be changed as they are compromised, however having password expiry periods can also ensure that they are consistently being changed to decrease the chances of a data breach through brute force or prolonged attacks.

The average database user does not require access to all tables and functions within a database. Having a strong access policy will prevent unauthorized users from having unnecessary access to the entire database. This prevents both malicious attacks and erroneous errors that would corrupt data within the database. Permissions should be granted to each user depending on how much access they need. Discretionary permissions are the best practice, as users can always ask for more access if needed but they will rarely notify an administrator if they have access to more information than they should. Only the database administrator should have full permissions over all tables, and no user should be able to delete any records.

Data backups can be categorized into onsite and offsite backups. A combination of both ensures that data is accessible when needed and safely stored in the event of any system failure. Daily incremental backups should be partial and only consisting of new data and immediate updates that would be stored onsite. Full backups should be performed weekly, with the data hosted on a cloud server to ensure that if there are power outages, damage to server equipment, or a theft of any hardware that data can be kept securely until it needs to be accessed again. These backups should be audited regularly to ensure accuracy of the data that is stored and reliability in accessing the data as necessary.