Encryption and Backup Proof-of-Concept Project

1. Project Overview

- **Objective:**
    - To define, test, and document the process of encrypting restricted data, backing up the data to the cloud, and successfully recovering the data on a new server.
    - To ensure the encryption certificates are securely backed up and protected, while also preventing unauthorized export of certificates and data, even if a workstation is compromised.

2. Scope of Work

- **Encryption:**
    - This PoC project will involve test/dummy data that will need to be generated. A demo dataset with all the required data fields is available.
    - Folders containing test data that need to be encrypted will already be identified. There will be 2-3 folders.
    - The data to be encrypted will be no more than 10 GB in total.
    - Encrypt the identified folders on the Windows 2019 Server test server.
    - EFS encryption (AES-256) should be used to encrypt the identified folders.
    - Encryption certificates may need to be installed on the Windows 11 test workstation if required to access encrypted data on the server.
    - Develop a secure process for backing up encryption certificates. This may involve storing the certificates in a secure key vault (recommendations) or using an encryption method for backup that ensures only authorized access.
    - Implement measures to prevent encryption certificates from being exported from compromised workstations.
    - Ensure that if a workstation is compromised, the attacker cannot use the encryption certificates to move sensitive data to an unprotected location.

    - Ensure that any access to the server's database from compromised workstations does not allow the attacker to copy or export data in an unencrypted format.
    - Implement restrictions that limit the ability to move or copy encrypted data, forcing all data interactions to occur in an encrypted state.
    - Develop a process to manage encryption certificates.
    - Propose a secure, centralized certificate management solution or key vault, for storing and managing the encryption certificates.
- **Backup:**
    - Backup the encrypted data to a designated cloud storage solution (Synology C2 Backup for Business). Access to test account will be provided.
    - Ensure that the backup process can be automated and tested periodically for successful completion. (The backup agent on the server can be configured to perform backups on a schedule.)
    - Confirm the integrity of the encrypted data after it is uploaded to the cloud.
- **Recovery:**
    - Simulate a disaster recovery scenario where a new server is provisioned. A new server will be configured in Azure for this test.
    - Retrieve the encrypted data from the cloud backup and restore it on the new server.
    - Test the successful decryption of data and ensure that the application and client software can access and function with the restored data.
- **Documentation:**
    - Create detailed documentation outlining the entire process, including steps for encryption, backup, and recovery.
    - The documentation should include:
        1. Software and tools used
        2. Configuration details
        3. Encryption keys management

4. Step-by-step recovery instructions
5. Testing results
6. Troubleshooting tips for potential issues during recovery

3. Technology Requirements

- **Server Environment:**
    - A basic Azure Lab environment is in place with a Windows 2019 Server and a Windows 11 Workstation. Further configuration may be required.
    - Information only: In the real production environment, the application resides on a server connected to a small network of workstations, with corresponding client software accessing the application data.
- **Cloud Backup Solution:**
    - The cloud backup solution is Synology C2 Backup for Business.
- **Encryption Tools:**
    - Windows EFS or third-party encryption software (open to any recommended third-party encryption software that does not use encryption certificates and is easier to manage without compromising data security).

4. Testing Criteria

- **Encryption:**
    - Data must be successfully encrypted without disrupting the operation of the application.
    - Test the scenario of a compromised workstation to ensure that:
        1. Encryption certificates cannot be exported.
        2. The attacker is unable to copy or move encrypted data to an unprotected location.
        3. The attacker is unable to copy or move the data in an unencrypted format.
    - Verify that encryption certificates are backed up securely, and test the recovery process to ensure that only authorized users can access the backup.
- **Backup:**

    - Backup integrity must be verified pre- and post-encryption.
    - Test backup schedules and automation to ensure periodic backups without data corruption.
- **Recovery:**
    - Data must be restored on a new server from the cloud, with successful decryption.
    - The restored data should be accessible and usable by the application without data loss or application issues.

5. Deliverables

- **Fully Documented Process:**
    - Detailed documentation of the encryption, backup, and recovery processes.
    - A finalized version of the documentation should include configuration steps, screenshots, software versions, and any relevant testing logs or results.
- **Test Report:**
    - Provide a report summarizing the PoC results, including any issues encountered during the encryption, backup, and recovery processes and how they were resolved.
- **Technical Writing Quality:**
    - Documentation must be clear, concise, and suitable for a technical audience who may need to replicate the process.
    - The freelancer should provide high-quality technical writing skills and demonstrate an ability to document technical procedures accurately.

6. Freelancer Qualifications

- **Technical Skills:**
    - Experience in server management, encryption, cloud backup, and recovery processes.
    - Familiarity with tools such as Windows Server, cloud storage providers (e.g., AWS, Azure), and encryption software.
- **Documentation Skills:**

- Proven experience in technical writing and creating clear, detailed, and organized documentation for technical processes.

7. Timeline and Milestones

- **Milestone 1:** Encrypt the data and document the encryption process.
- **Milestone 2:** Set up, test and the cloud backup process.
- **Milestone 3:** Simulate the disaster recovery, restore the data on a new server, and document the process.
- **Milestone 4:** Provide final documentation and testing report for review.