Data-Leak

Data Leak Incident Report

Incident Scenario

A **customer success representative** received access to a folder of internal documents from a **manager**. The folder contained files related to a **new product offering**, including **customer analytics** and **marketing materials**.

However, the **manager forgot to unshare the folder** after the task was completed, leaving it accessible. Later, during a **sales call**, the representative intended to share a **specific marketing file** with a **business partner**, but accidentally shared a **link to the entire folder** instead.

The business partner then **accessed all the internal documents** and **posted the link publicly on their social media page**, resulting in a **data leak** of confidential internal information.

Issue:

The manager failed to revoke access to a shared folder, violating the principle of least privilege. The employee unintentionally shared the entire folder instead of one file. Lack of access control and oversight resulted in public exposure of internal documents.

Review:

The NIST SP 800-53: AC-6 control emphasizes enforcing the *principle of least privilege*, allowing users only the minimum access necessary to perform their duties. It supports role-based access and regular access reviews to reduce the risk of data exposure or misuse.

Recommendations:

1. **AC-6(1) – Least Privilege | Authorize Access to Security Functions**
   Restrict access to critical folders and security functions to only authorized administrators or users based on job roles.
2. **AC-6(9) – Least Privilege | Auditing Use of Privileged Functions**
   Implement auditing and monitoring of privileged access to sensitive folders and files to detect and respond to improper sharing or misuse.

Justification:

Implementing role-based access ensures that only authorized personnel can view sensitive folders, minimizing accidental exposure. Auditing privileged access allows the company to monitor user activity and detect policy violations early, reducing the likelihood of internal data leaks caused by oversight or misuse.