Data Leak Analysis Report

Company: Confidential

Date: 2025-02-23

Prepared by: Zayn AK
Incident Type: Data Leak

1 Issue(s)

A **customer success representative** was mistakenly granted access to **internal documents** containing sensitive customer analytics and marketing materials. Due to an oversight, the folder remained **shared**. The representative **accidentally shared the wrong link** during a sales call, exposing the internal folder. The business partner **publicly posted** the link on social media, leading to an **unauthorized data leak**.

2 Review of NIST SP 800-53: AC-6

The **NIST SP 800-53: AC-6** standard enforces **least privilege** to prevent unauthorized access. It ensures that **users only receive access to the data necessary** for their roles. In this case, failure to **restrict access levels** and enforce **proper permission reviews** resulted in sensitive data exposure.

3 Recommendation(s)

Implement Role-Based Access Control (RBAC)
- Restrict access **strictly** based on job roles. Employees in sales should **only** have access to marketing materials, not sensitive analytics.

Enable Expiring Share Links & Audit Logging
- Shared links should **expire after a set period** to prevent accidental long-term access.
- **Automated auditing** should track document-sharing activity to flag anomalies.

Justification

Implementing **RBAC** ensures that employees only have the access necessary for their work, preventing **oversharing mistakes**. **Expiring share links** add an extra layer of security, reducing the risk of persistent access to sensitive documents. **Audit logging** provides visibility into shared file activities, allowing **quick detection** of improper access.

Conclusion: Strengthening **access controls** and **auditing shared files** will significantly reduce the risk of future data leaks. These enhancements align with **NIST SP 800-53 guidelines** and improve overall **information security**.