Data Leak Incident Report

Date: August 2, 2024

Incident: Accidental Disclosure of Internal Documents on Social Media

Prepared By: Junaid Shakoor, Security Analyst

Summary:

On August 1st, a sales manager shared access to a folder containing internal-only documents with their team during a meeting. The folder included pre-release product information, customer analytics, and promotional materials. While the manager verbally cautioned the team against sharing the information without approval, they did not revoke access to the folder after the meeting. Subsequently, a sales representative mistakenly shared a link to the entire folder with a business partner during a video call. The business partner, assuming the link was for approved promotional materials, posted it on their company's social media page, leading to public exposure of the confidential documents.

Root Cause Analysis:

- **Overly Broad Access:** The sales team's access to the entire folder violated the principle of least privilege.
- **Lack of Automated Controls:** Reliance on verbal warnings without automated safeguards increased the risk of human error.
- **Inadequate Review Process:** The absence of a formal review and approval process for sharing external materials contributed to the miscommunication.

Security Control Analysis:

The current security plan references NIST SP 800-53: AC-6, which emphasizes the importance of access controls to protect information systems and data. However, the incident demonstrates a need for stricter implementation of least privilege principles.

Recommendations:

To mitigate the risk of future data leaks, the following recommendations are proposed:

1. **Granular Access Controls:** Implement role-based access controls that restrict access to sensitive information based on individual job responsibilities. Regularly review and update permissions to reflect changes in roles or projects.
2. **Automated Access Revocation:** Utilize automated tools or scripts to revoke access to sensitive data after a predetermined period or upon project completion. This will prevent lingering access and reduce the risk of accidental sharing.

3. **Formal Review and Approval Process:** Establish a formal review and approval process for sharing any materials with external parties. This process should include verification of the recipient's identity, the sensitivity of the data, and the purpose of sharing.

Justification:

These recommendations directly address the root causes of the incident. Granular access controls prevent oversharing by limiting access to only necessary information. Automated access revocation eliminates the risk of lingering access due to oversight. A formal review and approval process reduces the likelihood of human error and miscommunication when sharing data externally.

Conclusion:

By implementing these recommendations, the company can significantly strengthen its data security posture, uphold the principle of least privilege, and minimize the risk of future data leaks. This will not only protect sensitive information but also enhance the company's reputation and build trust with customers and partners.

Next Steps:

1. Implement the recommended control enhancements within a defined timeframe.
2. Conduct regular security awareness training for employees to reinforce data handling best practices.
3. Periodically review and update security policies and procedures to adapt to evolving threats and vulnerabilities.