Access Control Incident Review, Payroll Transaction

1. Introduction

Access controls are critical for protecting sensitive financial operations and preventing unauthorized activity. This report documents an internal review of a payroll related security incident caused by weaknesses in authentication and authorization controls. The objective of this assessment is to analyze access log activity, identify control gaps, and recommend mitigations to reduce the likelihood of similar incidents in the future.

2. Incident Summary

A payroll deposit was initiated toward an unknown bank account and was later stopped before completion. The finance manager confirmed the transaction was not authorized. An investigation was initiated to determine how access controls were misused and to prevent recurrence.

3. Log Review and Findings

Access logs showed a successful authenticated login followed by payroll-related activity. The event originated from an IP address and device not typically associated with finance operations. This suggests misuse of valid credentials rather than a system malfunction or technical failure.

4. Access Control Issues Identified

The user account involved had authorization to initiate sensitive payroll actions without additional verification. Access controls did not enforce role-based restrictions or separation of duties, allowing a single account to perform high-risk financial operations.

5. Recommendations

To strengthen access controls and prevent future incidents, the following mitigations are recommended:

- Implement role-based access control (RBAC) to restrict payroll functions to authorized finance personnel only.
- Require multi-factor authentication and secondary approval for sensitive financial transactions, such as payroll changes or bank account updates.

6. Visual Summary

Category	Observed Issue	Recommended Mitigation
Authentication	Payroll activity was performed using valid credentials without additional verification.	Require multi-factor authentication for all payroll and banking transactions.
Authorization	User account had permissions exceeding job responsibilities, allowing payroll actions.	Apply role-based access control to restrict payroll functions to authorized finance roles.
Separation of Duties	A single account could initiate high-risk financial actions without independent review.	Enforce secondary approval for payroll changes and bank account updates.

Figure 1: Access control weaknesses and recommended mitigations

7. Conclusion

This assessment highlights how insufficient authorization controls can lead to unauthorized financial activity, even when valid credentials are used. Strengthening role-based access restrictions and enforcing multi-factor authentication with approval workflows significantly reduces the risk of payroll fraud and improves overall security posture.

Prepared by: Sambou Kamissoko

LinkedIn: https://www.linkedin.com/in/sambouk/