Access Control Assessment: Unauthorized Payment Attempt

Project Overview

This project analyzes an access control failure that led to an unauthorized attempt to transfer company funds to an unknown bank account. Although the payment was stopped before completion, the event was investigated as a security incident to identify access control weaknesses and recommend mitigations to prevent recurrence.

Scenario

A growing business experienced a suspicious financial transaction in which a deposit was initiated to an unknown bank account. The finance manager confirmed they did not authorize the transaction. As the organization's first cybersecurity professional, I was tasked with reviewing system logs, identifying access control issues, and recommending improvements to reduce future risk.

Investigation Approach

The assessment followed a structured access control review process:

1. Reviewed event logs to identify details about the user activity associated with the transaction
2. Analyzed employee records to understand role assignments and access privileges
3. Identified access control weaknesses that enabled the incident
4. Recommended mitigations aligned with access control best practices

Key Findings

User Observations

- The transaction was initiated using valid credentials, indicating authorized access was misused rather than a technical system breach
- Log details suggested the activity did not align with expected finance manager behavior, raising concerns of credential compromise or improper access

Access Control Issues Identified

- Financial systems relied on overly broad access permissions rather than strict role-based access controls
- Shared resource management increased the risk of unauthorized actions and reduced accountability

Recommendations

- Implement role-based access control (RBAC) to ensure only authorized finance personnel can initiate or approve payments
- Enforce multi-factor authentication (MFA) for financial transactions to reduce the risk of credential misuse
- Conduct regular access reviews to revoke unnecessary or outdated permissions

Skills Demonstrated

- Access control analysis
- Log review and investigation

- Authorization and authentication concepts
- Risk identification and mitigation
- Governance and security process evaluation

Outcome

This assessment demonstrated how unauthorized actions can occur even when systems function as designed. By identifying access control gaps and recommending targeted mitigations, the organization can significantly reduce the likelihood of future financial security incidents.

	Note(s)	Issue(s)	Recommendation(s)

Authorization /authentication	**Objective:** List 1-2 pieces of information that can help identify the threat: ● An employee with the IP address of 152.207.255.255 accessed the user account Legal/Administrator to make an unauthorized account. The manager says it wasn't a mistake but the payment was made toward an unknown bank. Fortunately the payment was stopped in time. ● It occurred on 10/03/2023, 8:29:57 AM. ● The device used was a computer- Up2-NoGud.	**Objective:** Based on your notes, list 1-2 authorization issues: ● Robert Taylor Jr is an Admin. ● His contract ended in 2019, but his account accessed payroll systems in 2023.	**Objective:** Make at least 1 recommendation that could prevent this kind of incident: ● This business needs to implement the principles of least privilege and separation of duties. All employees—including full-time staff, part-time staff, and contractors—were granted administrative privileges, creating unnecessary risk. Security posture can be significantly improved by limiting credentials and access on a need-to-know basis and assigning authorization based on job role and title. Additionally, access should be immediately revoked when an employee leaves the company. Restricting file access to appropriate users reduces the risk of misuse and unauthorized exposure of sensitive data.