Access Controls Analysis Worksheet

Notes

- Date and time of incident: October 3, 2023 8:29:57 AM

- User account: Legal\\Administrator

- Suspicious activity: Payroll event added for "FAUX_BANK"

- Computer identifier: Up2-NoGud

- IP address: 152.207.255.255

- Event logged through AdsmEmployeeService

Access Control Issues

1. Administrator-level access was used from an account in the Legal department, which is unusual for payroll activity and could be privilege escalation or misuse

2. The computer name "Up2-NoGud" appears suspicious and may be an unauthorized or unmanaged device accessing the system

3. The action was performed without apparent multi-factor authentication or other verification protocols for payroll changes

Recommended Mitigations

Technical Controls

1. Implement role-based access control (RBAC) to:

- Restrict payroll changes to authorized Finance department personnel only

- Adequately segregate and track administrator privileges

- All departments have applicable access limitations

2. Use multi-factor authentication (MFA):

- Require MFA for all administrative tasks

- Include additional verification processes for banking and payroll modifications

- Set up notifications for any modification to payment information

Operational Controls

1. Establish a process for:

- Regular access review and elimination of inactive accounts

- Approval workflow for any payment data modifications

- Monitoring and alerting for suspicios activity (especially outside business hours)

2. Implement an asset management solution to:

- Inventory all authorized devices on the network

- Implement naming conventions for company devices

- Block access from unauthorized or unmanaged devices

Additional Recommendations

1. Logging and monitoring:

- Create detailed audit trails for all payroll activities

- Initiate automatic alerts for unusual patterns

- Regularly review access logs for unauthorized access

2. Define security policies:

- Formalize proper authorization procedures

- Create incident response procedures

- Provide regular security awareness training to all employees