Improve IAAA for Small Business

Scenario:

You’re the first cybersecurity professional hired by a growing business.

Recently, a deposit was made from the business to an unknown bank account. The finance manager says they didn’t make a mistake. Fortunately, they were able to stop the payment. The owner has asked you to investigate what happened to prevent any future incidents.

Access Control Worksheet:

Identification steps:

1. Fetch the event logs and filter the incident and detect the IP address, Computer (Device ID), name of user who carried out and when the incident was happend

Eg of Event log:

|  |
| --- |
| Event Type: Information |
| Event Source: AdsmEmployeeService |
| Event Category: None |
| Event ID: 1227 |
| Date: 10/03/2023 |
| Time: 8:29:57 AM |
| User: Legal\Administrator |
| Computer: Up2-NoGud |
| IP: 152.207.255.255 |
| Description: |
| Payroll event added. FAUX\_BANK |

1. Now we match those details with the employee directory and identify the name of the employee and check users validity and when it was last accessed

For Eg :

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Rob | Legal attorney | rt.jr@erems.net | 152.207.255.255 | Contractor | Admin | 8:29:57 am (5 days ago) | 9/4/19 | 12/27/19 |

1. We could see that the employee end date is out of validity and the user is still accessing the data, so misusing the credentials.

Issue:

* The Former employee's access is not being handled properly as a result a wrong transaction was carried out.

Recommendations:

* All access should be revoked, and the employee ID should be deactivated on the end date of the employee.
* Usage of multi-factor authentication for performing any transaction
* The transactions by employees should be carried out only with the office network.
* Monitoring of Events and user activities should be in place.
* Contractors should have limited access to business resources.