# Access controls worksheet

| | Note(s) | Issue(s) | Recommendation(s) |
|---|---|---|---|
| **Authorization /authentication** | **Objective:** Make 1-2 notes of information that can help identify the threat:<br>● *Who caused this incident?*<br>● *When did it occur?*<br>● *What device was used?*<br><br>***MY RESPONSES:***<br><br>● *The incident occurred on 10/03/2023 at 8:29:57 AM.*<br>● *The user is Robert Taylor Jr, a contractor with administrative privileges, accessed the payroll system despite his contract expiring in December 2019.*<br>● *The device used was Up2-NoGud, and the IP address of the login attempt is 152.207.255.255, where the user account was still active* | **Objective:** Based on your notes, list 1-2 authorization issues:<br>● *What level of access did the user have?*<br>● *Should their account be active?*<br><br>***MY RESPONSES:***<br><br>● *Robert Taylor Jr., a contractor and Admin of the system, should have had limited access to business resources and should have been removed from the system following his contract's end in 2019. This is beucase his account accessed payroll* | **Objective:** Make at least 1 recommendation that could prevent this kind of incident:<br>● *Which technical, operational, or managerial controls could help?*<br><br>***MY RESPONSES:***<br><br>● *User accounts should automatically expire after 30 days of contract end or employment termination. This policy would ensure that contractors or temporary employees do not maintain access beyond their contract or employment period.* |

| | Note(s) | Issue(s) | Recommendation(s) |
|---|---|---|---|
| | *and accessed the event through that IP address.* | *systems in 2023 when it should not due to the expiration.*<br>● *However, his admin-level account remained active for over three years, granting him access to sensitive company data and payroll systems.* | ○ *Contractors should have limited access to business resources.*<br>● *Additionally, Multi-factor Authentication (MFA) should be enabled for all users, particularly those with admin-level access, to add another layer of security in case of unauthorized logins*<br>● *Implement a system for automatic deactivation of accounts after the end date of a contractor's contract, ensuring no unauthorized access occurs post-contract.*<br>● *Moreover, it would be beneficial to restrict contractors' access to critical business resources unless absolutely necessary, and this access should* |

| | Note(s) | Issue(s) | Recommendation(s) |
|---|---|---|---|
| | | | *be closely monitored.* |

NOTES:
**Scenario**

Review the scenario below. Then complete the step-by-step instructions.
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.
To do this, you'll need to do some accounting on the incident to better understand what happened. First, you will review the access log of the incident. Next, you will take notes that can help you identify a possible threat actor. Then, you will spot issues with the access controls that were exploited by the user. Finally, you will recommend mitigations that can improve the business' access controls and reduce the likelihood that this incident reoccurs.

Facts and notes for the case which is Accounting:

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

| Name | Role | Email | IP address | Status | Authorization | Last access | Start date | End date |
|---|---|---|---|---|---|---|---|---|
| Lisa Lawrence | Office manager | l.lawrence@erems.net | 118.119.20.150 | Full-time | Admin | 12:27:19 pm (0 minutes ago) | 10/1/2019 | N/A |
| Jesse Pena | Graphic designer | j.pena@erems.net | 186.125.232.66 | Part-time | Admin | 4:55:05 pm (1 day ago) | 11/16/2020 | N/A |
| Catherine Martin | Sales associate | catherine_M@erems.net | 247.168.184.57 | Full-time | Admin | 12:17:34 am (10 minutes ago) | 10/1/2019 | N/A |
| Jyoti Patil | Account manager | j.patil@erems.net | 159.250.146.63 | Full-time | Admin | 10:03:08 am (2 hours ago) | 10/1/2019 | N/A |
| Joanne Phelps | Sales associate | j_phelps123@erems.net | 249.57.94.27 | Seasonal | Admin | 1:24:57 pm (2 years ago) | 11/16/2020 | 1/31/2020 |
| Ariel Olson | Owner | a.olson@erems.net | 19.7.235.151 | Full-time | Admin | 12:24:41 pm (4 minutes ago) | 8/1/2019 | N/A |
| Robert Taylor Jr. | Legal attorney | rt.jr@erems.net | 152.207.255.255 | Contractor | Admin | 8:29:57 am (5 days ago) | 9/4/2019 | 12/27/2019 |
| Amanda Pearson | Manufacturer | amandap987@erems.net | 101.225.113.171 | Contractor | Admin | 6:24:19 pm (3 months ago) | 8/5/2019 | N/A |
| George Harris | Security analyst | georgeharris@erems.net | 70.188.129.105 | Full-time | Admin | 05:05:22 pm (1 day ago) | 1/24/2022 | N/A |
| Lei Chu | Marketing | lei.chu@erems.net | 53.49.27.117 | Part-time | Admin | 3:05:00 pm (2 days ago) | 11/16/2020 | 1/31/2020 |

**Step 3: Review the event log of this payroll incident**

Event logs contain information related to the operation and usage of a system. They can be utilized to identify suspicious activity, detect vulnerabilities, and track users.

Find the **Event log** tab of the *Accounting exercise* spreadsheet. Carefully review the event log of this incident to start your investigation. Notice the *Event Type*, *Date*, *Time*, and *IP Address* of the user in the log details.
Make **1-2 notes** of information that you learned about the user from reviewing the *Event log* details. Add your notes to the **Notes** column of the access control worksheet.

**Step 4: Identify access control issues that led to the incident**

Log details tell you a lot about a specific moment in time. You can find other useful details about an event by cross referencing that information with other sources.
This business has a range of different employees. They all currently manage company resources using a shared cloud drive.
Find the **Employee directory** tab of the *Accounting exercise* spreadsheet. Compare the information found in the *Employee directory* tab with the information in the *Event log* tab. Notice any similarities between the details in the *Event log* and the details in the *Employee directory*.
Then, list **1-2** issues that you discover with how the business handles employee access in the **Issues** column of the *Access control worksheet*.
Step 5: Recommend mitigations that can prevent a future breach

You've completed your accounting of the strange payment and discovered flaws with how the business handles their information.

Find the Recommendation(s) column of the Access control worksheet. Make at least 2 recommendations of mitigations the business can implement to prevent incidents like this in the future.

For example, one recommendation might be to have procedures in place to revoke access to files when an employee is no longer with the company. Be sure to include the following elements in your completed activity:

- 1-2 notes about the user
- 1-2 access control issues
- 2 recommendations for access control mitigations