Improve authentication, authorization, and accounting for a small business

Activity Overview

In this activity, you will assess the access controls used by a business. You’ll analyze their current process, identify issues, and make recommendations to improve their security practices.

Previously, you learned that **access controls** are security controls that manage access, authorization, and accountability of information. Authentication controls are used to verify who someone is, whereas authorization controls are used to grant a user permissions and set limits on the things they’re allowed to do. When done well, access controls are the key to decreasing the likelihood of a security risk.

Be sure to complete this activity before moving on. The next course item will provide you with a completed exemplar to compare to your own work.

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.

Step-By-Step Instructions

Follow the instructions and answer the question below to complete the activity. Then, go to the next course item to compare your work to a completed exemplar.

**Step 1: Access the template**

**Access control worksheet**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Note(s)** | **Issue(s)** | **Recommendation(s)** |
| **Authorization/Authentication** | **Objectives: Make 1-2 notes of information that can help identify the threat:**  **. Who caused this incident?**  **. When did it occur?**  **. What device was used?** | **Objective: Based on your notes, list 1-2 authorization issues:**  **. What level of access did the user have?**  **. Should their account be active?** | **Objective: Make at least 1 recommendation that could prevent this kind of incident:**  **. which technical, operational, or managerial controls could help?** |

**Step 2: Access supporting materials**

The following supporting materials will help you complete this activity. Keep them open as you proceed to the next steps.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 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 |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |

## **Step3: 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.

**Step4: 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.

Notes about the user:

The event log indicates that the user who initiated the deposit to the unknown bank account is identified as "Legal\Administrator."

The event took place on 10/03/2023 at 8:29:57 AM, with the IP address 152.207.255.255. This information can be useful for further investigation.

Access control issue:

The primary access control issue identified is the excessive access level granted to the "Legal\Administrator" user. They had the ability to initiate financial transactions, which seems beyond the scope of their role.

Another issue is the lack of timely account review or deactivation. It appears that the user's account was still active even though their access level was inappropriate for the actions they took.

Recommendation for access control mitigations:

Implement the principle of least privilege, which means that users should have access only to the resources necessary for their job. Review and restrict access rights for the "Legal\Administrator" role to prevent unauthorized financial transactions.

Establish a periodic access review process to ensure that user accounts are regularly reviewed and adjusted as necessary. Accounts that are no longer required or have inappropriate access levels should be promptly deactivated.

These recommendations will help improve access controls, prevent similar incidents, and enhance the overall security of the business.

Top of Form