Access Control 2024-09-10 #1

Emsa SA - Uruguay Avenue 370 - Posadas

Scenery

At the energy company EMSA SA, a deposit was recently made from the company to an unknown bank account. The manager of the affected branch says that they did not make any mistake. Fortunately, they were able to stop the payment. The board has asked him to investigate what happened in order to prevent future incidents.

To do this, some research will be done on the incident to better understand what happened.

\* The incident access log will be reviewed.

\* Notes will be taken that may help identify a potential threat actor.

\* Problems with access controls that were exploited by the user will be detected.

\* Finally, mitigations will be recommended that can improve the company's access controls and reduce the likelihood of this incident occurring again.

Review the Event Log

Event logs contain information related to the operation and use of a system. They can be used to identify suspicious activities, detect vulnerabilities, and track users.

The suspicious event log was saved in the spreadsheet. The event log for this incident was carefully reviewed to begin its investigation:

The event took place on 09/10/2024 at 8:29:57 AM

The user is Accountant. The IP address of the computer used to log in is 152.207.255.255

Identify the access control issues that caused the Incident

There are several different employees working at this company. Currently, they all manage the company's resources through a shared disk drive in the cloud.

The information found in the employee directory tab was compared with the information in the event log tab:

Roberto Daniel Gimenez was a contracted accountant with administrator access

His contract ended in 2023, but his account accessed the payroll systems in 2024

Recommend mitigations that can prevent a future breach

The investigation into the strange payment has been completed and flaws have been discovered in the way the company handles your Information:

User accounts should expire after 30 days

Contractors should have limited access to company resources

Multi-factor authentication (MFA) should be enabled

Access Control Worksheet

|  | Grades) | Issues) | Recommendation(s) |
| --- | --- | --- | --- |
| Authorization/Authentication | When did it happen?  The event took place on 10/09/2024  Who caused this incident?  The user is Accountant  What device was used?  The IP address of the computer used to access is 152.207.255.255 | What level of access did the user have?  Roberto Daniel Gimenez is an Admin    Should your account be active?  His contract ended in 2023 but his account accessed the payment systems in 2024 | What technical, operational or management controls could help?  User accounts should expire after 30 days of non-use  Contractors should have limited access to business resources  Enable MFA (Multi-Factor Authentication) |