**Advanced Executive Program in Cybersecurity**

Virtual Internship Project Problem Statement



**Security Analyst**

**Problem Statement:**

You are working as a security analyst for El Banco Bank, where your primary responsibility is to implement best practices to secure the organization’s assets.

You are reviewing the password policy for internal users and realize that it is outdated and has not been updated in the last five years. Therefore, it does not align with the latest recommendations published by PCI DSS, NIST, and CIS.

The organization currently does not use multi-factor authentication. Users are encouraged to use password managers authorized by the organization to store passwords.

Your goal is to review and update the organization’s password policy settings to comply with the latest security requirements. Since the bank processes credit cards, you need to ensure that the password policy complies with Payment Card Industry Data Security Standard (PCI DSS) security requirements.

However, PCI DSS encourages referring to other industry standards. Therefore, you have decided to compare PCI DSS requirements with NIST and CIS recommendations.

**Background of the problem statement:**

El Banco Bank is one of the fastest-growing banks in Europe with more than 1200 branches across the country and manages €200 billion in assets.

Handling millions of dollars of banking transactions per day, its customers hugely depend upon the security of their banking data. The recent surge in cyber attacks and data breaches has become a significant issue for every organization.

According to the latest reports, 81% of successful cyberattacks are due to compromised usernames or passwords.

**Reference Documents:** <https://github.com/Simplilearn-Edu/AEPCS-Capstone-Project>

**Expected Deliverables:**

**TASK 1:**

As a security analyst, you have to review the documents published by PCI DSS, NIST, and CIS for password guidelines and determine the recommendations for the following policy. Use **NA** (Not Applicable) if the policy is not explicitly mentioned.

|  |  |  |  |
| --- | --- | --- | --- |
| **Policy** | **NIST Recommendations** | **CIS Recommendation** | **PCI DSS Recommendation** |
| **Minimum password length** | At least 8 characters | 8 characters | 12 |
| **Password history (number)** | No specific recommendation | 24 | Retain previous password |
| **Complexity (Enabled/Disabled)** | disabled | Enabled | Enabled |
| **Password expiration (days)** | Only, when necessary, organizations have a password policy that allows to be 60 -90 days old at max. | 60 | 90 |
| **Minimum password age (days)** | Not fixed expiration period | 60 | 90 |
| **Session idle time-out (mins)** | No specific | 15 | 15 |
| **Suspend/remove/disable inactive user accounts (days)** | 90 | 45 | 90 |
| **Limit failed login attempts by locking out the user (attempts)** | 10 attempts | 5 tries | 6 attempts |

**TASK 2:**

Review the Password Policy configured in Active Directory and determine if the given default policy is compliant with the NIST, CIS, and PCI DSS recommendations.

**Note:** To access the Password Policy, launch the **Local Group Policy Editor** by pressing Windows+R, typing **gpedit.msc** into the box, and then pressing the **Enter** key. Next, navigate to **Computer configuration > Windows settings > Security settings > Account policies > Password policy**.

Make relevant changes to ensure the password policy settings are compliant with the given recommendations. Use 0 if the value is NA.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **NIST** | **CIS** | **PCI DSS** |
| **Enforce password history** | 365 days | 60 days | 90 days |
| **Maximum password age** | No specific period | 60 | 90 |
| **Minimum password age** | 24 hours | Not prescribed | Not specific |
| **Minimum password length** | 8 characters | 7 characters | 7 characters |
| **Password must meet complexity requirements** | Requires Only 8 characters password, Not having specific complexity | Yes | Yes |
| **Store passwords using reversible encryption** | Yes | Yes | Yes |

**TASK 3:**

To ensure that the organization’s cloud resources are also compliant with the PCI DSS requirements, review the IAM Password Policy on AWS (as shown in the screenshot) to determine if the account password policy meets the PCI DSS requirements.

Graphical user interface, text, application, email

Description automatically generated

Make the relevant changes to ensure that the IAM policy is compliant with PCI DSS requirements.

|  |  |  |
| --- | --- | --- |
| **Parameters** | **Description** | **Default Value** |
| **Require Uppercase Characters** | Contain Combination with Uppercase | A to Z |
| **Require Lowercase Characters** | Contain Combination with Lowercase | a to z |
| **Requires Symbols** | Contain Unique symbol | Any symbol present in keys |
| **Require Numbers** | Contain Combination with Numeric characters | 0, 1 all numbers |
| **Minimum Password Length** | 12 characters | For e.g. Pas@w1awWD!5 |
| **Password Reuse Prevention** | Last four passwords |  |
| **Max Password Age** | 90 days to reduce the risk of unauthorized access due to compromised credentials |  |

**TASK 4:**

As a security analyst for the bank, review the **PCI DSS v3.2.1 Quick Reference Guide** to determine the following:

1. Review firewall configuration rules at least every 6 **Months.**
2. Purge unnecessarily stored data at least **Quarterly.**
3. Install critical security patches within **48-72 hours** of release.
4. Scan internal and external network vulnerabilities at least **once a quarter** and after any significant change in the network.
5. Retain visitor logs for at least **3 months** unless otherwise restricted by law.
6. Perform critical log reviews at least **daily.**
7. Retain audit trail history for at least **one year.**
8. Common Vulnerability Scoring System (CVSS) base score for external scans of the components in the cardholder data environment must not be equal to or higher than **4.0**.
9. Service providers using segmentation must confirm PCI DSS scope by performing penetration testing on segmentation controls at least every **six months** and after making changes to these controls.
10. Review security policy at least **annually**.
11. Perform a risk assessment process at least **annually** and upon significant changes to the environment that identify critical assets, threats, and vulnerabilities and result in a formal assessment.
12. Conduct reviews at least **once every three months** to confirm personnel is following security policies and operational procedures.