Cliq Service Risk Assessment.

**The Assets Inventory.**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Asset ID | IT Asset | Cost of Ownership | Cost On Reputation | Impact on Mission | Assets Weight |
| A1 | Currency Exchange. | 3 | 3 | 8 | 14 |
| A2 | Cliq Website | 3 | 4 | 6 | 13 |
| A3 | Customers. | 10 | 9 | 8 | 27 |
| A4 | Personal Data. | 10 | 9 | 9 | 28 |
| A5 | Online Services. | 7 | 7 | 8 | 22 |
| A6 | API | 10 | 10 | 9 | 29 |
| A7 | Payment Card Industry PCI | 5 | 5 | 5 | 15 |
| A8 | Cliq Access | 10 | 10 | 10 | 30 |
| A9 | Firewalls | 6 | 5 | 7 | 18 |
| A10 | Network Admin | 7 | 7 | 7 | 21 |
| A11 | Web Server | 8 | 8 | 8 | 24 |
| A12 | NAC | 6 | 5 | 5 | 16 |

A1- Currency Exchange 🡪 is used when transferring from one bank to another that takes 1% from the transferred amount. Which is used to indicate the cost of ownership as a scale from 10.

A2- Cliq Website 🡪 is represent a basic component that won’t affect the mission of CLIQ to perform its functionality as if the Cliq Access was down. It might be affected if it’s used on the web rather than the mobile app.

A3, A4 and A6 🡪 represents the most important assets in the payment system, that requires protection.

|  |  |  |
| --- | --- | --- |
| Threat ID | Threat Description. | Threat Rank As a scale from 5 |
| T1 | The lack of strong password policy that allow the creation of weak passwords can cause password cracking. | 4 |
| T2 | Responding to Phishing emails that claims the need to verify the user account. That happened because of lack of operational controls which we need to use to increase the awareness of the users as well as we could engage them into programs such as SETA. | 4 |
| T3 | Insecure Connection such as using the HTTP connection in which the credentials can be transmitted in plaintext that can be captured such as using Wireshark and might cause catastrophic results. | 4 |
| T4 | Theft Of Personal Data. | 5 |
| T5 | Forces Of Nature. | 3 |
| T6 | Dos OR DDos attack | 3 |
| T7 | Malware attacks | 3 |

Note 🡪 the Threats were Ranked based on scale from 5 based:

* Financial Loss.
* Reputation Loss.
* Cost to protect.
* The loss of the competitive advantage loss.
* The frequency of occurrence.

**Vulnerability Inventory.**

|  |  |  |
| --- | --- | --- |
| Vulnerability ID | Assets that it Affects | The Vulnerability Description. |
| V1 | A3,A4, A8 | Absence of email policies that filters the emails by using MDO |
| V2 | A3,A4 | Using SSL V1 method. |
| V3 | A3,A4 | Weak Passwords |
| V4 | A3,A4 | Lack of Training and Awareness. |
| V6 | A2,A11 | Hosting website on local web server |

**TVA Spreadsheet**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Asset/Threat | Currency Exchange | Cliq Website | **Customers** | **Personal Data** | Online Services. |
| Password Cracking |  |  | T2V1A3  T2V2A3  T2V3A3  T2V4A3 | T2V1A3  T2V2A3  T2V3A3  T2V4A3 |  |
| Phishing Emails |  |  | T2V1A3  T2V2A3  T2V3A3  T2V4A3 | T2V1A3  T2V2A3  T2V3A3  T2V4A3 |  |
| Insecure Connection |  |  |  |  |  |
| Theft of personal data |  |  | T2V1A3  T2V2A3  T2V3A3  T2V4A3 | T2V1A3  T2V2A3  T2V3A3  T2V4A3 |  |
| Forces of nature |  |  |  |  |  |
| Dos |  | T6V1A2 | T6V1A3 | T6V1A4 |  |
| Malware |  |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Asset/Threat | API | PCI | **Cliq Access** | Firewall | Network admin | Webserver | NAC |
| Password Cracking. |  |  |  |  |  |  |  |
| Phishing Emails. |  |  | T2V1A8 |  |  |  |  |
| Insecure connection. |  |  |  |  |  |  |  |
| Theft of personal data. |  |  | T4V1A8 |  |  |  |  |
| Forces of nature |  |  |  |  |  |  |  |
| DOS |  |  |  |  |  | T6V6A11 |  |
| Malware |  |  | T7V1A8 |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Priority of effort | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | ……… |

|  |  |  |  |
| --- | --- | --- | --- |
| Asset | Vulnerability | Impact | Likelihood |
| Personal data  28 | * Weak Passwords. * Improper SSL version. * Lack of training and awareness. * Improper Security policies as well as lack of filters and email policies that are provides by Microsoft defender for Office 365. | * Password Cracking. * Phishing emails. * Theft of personal data that results in loss of financial revenue as well as the loss of reputation of the organization. * DOS by lack of policies and guidance in the organization. | 0.9 |
| Cliq Access 30 | * Lack of proper security policy. That is related for strengthen the password as well as filtering the inbox from the email. | * Phishing email. * Theft of personal data * Malware which is known as the software attack. | 0.5 |
| Web server 24 | * Hosting the website on local webserver. | * DOS or DDOS attack | 0.4 |
| Customers 27 | * Weak Passwords. * Improper SSL version. * Lack of training and awareness. * Improper Security policies as well as lack of filters and email policies that are provides by Microsoft defender for Office 365. | * Password Cracking. * Phishing emails. * Theft of personal data that results in loss of financial revenue as well as the loss of reputation of the organization. * DOS by lack of policies and guidance in the organization. | 0.6 |

|  |  |  |  |
| --- | --- | --- | --- |
| The Inherit Risk | Controls if any | The associated Risk. | Recommendations to apply to avoid the risk. |
| 37.8 | Firewall | 32.76 | Setting a good password security that enforce the creation of strong password, engaging the employees in awareness and education programs such as SETA program and use more than one way of authentication such as MFA. |
| 22.5 | None | 22.5 | AV, more enhanced authentication techniques and Education and awareness programs. |
| 15 | Firewall | 13 | Acceptable. |
| 24.3 | None | 24.3 | The same controls as above. |

**Final Documentation.**