**CYBER SECURITY WEEK 7 ASSIGNMENT (ASSETS, THREATS & VULNERABILITIES)**

**OLANREWAJU ADESINA FE/23/10260344**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Asset** | **Threat** | **Likelihood** | **Impact** | **Priority** | **Justification** | **Recommendation** |
| Customer Records | Data Breach | 2 | 3 | 6 | Likelihood for this threat is moderate due to these reasons   * 3rd party software development company manage data. * No data encryption or compliance policy in place. * Too many people can access customer records. | * Employee security awareness and practices. * Customer records should be encrypted. * Use of strong password. * Adopt principle of least privilege and Multi factor authentication. * Access to records should be on a need-to-know basis. |
| Central database | Unauthorized access | 2 | 3 | 6 | Likelihood for this threat is moderate due to these reasons   * Access to database through Web application is managed by employees and 3rd party software development team. * IT infrastructure is in place. * Data is not backed up and encrypted. * Employee laptop is not protected. * There is no security awareness in place.   The impact of this threat is high as it could lead to reputational damage, financial loses and lawsuits. | ACG should:   * Create awareness and enforce strong password policies. * Keep software up-to-date and create regular database backup. * Adopt principle of least privilege and manage user access rights. * Make use of Antivirus, SIEM tools, IDP/IPS for monitoring and log analysis. * Encrypt and hash data and network traffic |
| Website and Web based application | Security logging & monitoring failures | 2 | 2 | 4 | Likelihood for this threat is moderate due to these reasons   * Web application is managed and protected by 3rd party software development team. * Application is open to attack from threat actors. * SIEM tools and IDS/IDP are not in place to identify/prevent malicious attack.   The impact of this threat is moderate as data from the 3rd party software development company can be used for monitoring failures | ACG should:   * Log analysis and prevention tools should be used for comprehensive logging and alert. * Masking of sensitive information in logs. * Secure coding practices. * Conduct security assessments and audits |
| Main servers | Distributed Denial of Service (DDOS) | 3 | 3 | 9 | Likelihood for this threat is high due to these reasons   * No access control measure on the main site where server housed. * No web based antivirus, encryption and firewall in place. * There are no logging attempts monitoring. * There is no backup for servers in case of successful attacks.   A successful DDOS attack will have a high impact on ACG by leading to financial loss, make resources unavailable and damage the company’s reputation. | ACG should:   * Employee awareness on how to prevent social engineering attack. * Encrypt email communication, block communication from outdated or unused ports, protocols & apps. * Web application firewall to filter malicious HTTP traffic. * Ensure secure communication by using VPNs and monitor logging attempts with IDS/IPS. |
| Business records | Unauthorized access | 3 | 2 | 6 | Likelihood for this threat is high due to these reasons   * Too many access to business and transactional activities * Stolen employee laptops can be used to access sensitive information * No backup for business records. * No firewall, encryption and adequate access to business records   The impact of unauthorized access on ACG is moderate as it can damage reputation, lead to financial loss but the company can still continue existing. | * Business records should be encrypted and hashed. * Access to records should be on a need-to-know basis. * Employee laptop and connection should be secured with VPN for secure communication. * Strong password policy should be enforced with adequate employee training awareness. |
| Third Party Software Development Team | Insider Threat | 1 | 3 | 1 | Likelihood for this threat is low because   * The third party team is responsible for accounting and securing sensitive information and resources.   The impact of this threat is high because access to sensitive information can damage the ACG’s reputation and lead to financial loss. | ACG should   * Conduct regular audit, access control and implement principle of least privilege. * Regularly update website software, implement web security best practices. |