**CY5200 Security Risk Management and Assessment**

**Module 10 Assignment**

**By: Kalp Shah**

**002232460**

**I. IDS Calculations**

Sensitivity (SE) = 99%

Specificity (SP) = 95%

M: Malware packets permitted to enter : False Negative

N: Packets labelled as Negative by IDS : False Negatives + True Negatives

L are the legitimate packets

**False Negative**

P(N | M) = (1 - SE) \* M = (1 - 0.99) \* 0.4 = 0.004

**True Negatives**

P(N | L) = SP \* L = 0.95 \* 0.6 = 0.574

**Conditional Property**

P(M | N) = P(N | M) \* P(M) / P(N) + P(N | L) \* P(L) / P(N)

P(M | N) = (0.004 \* 0.4) / (0.004 \* 0.4) + (0.57 \* 0.6) = 0.7%

**II**

**Company Name –** Ayurhealthybaby

**Description –** Ayurhealthybaby is a health organization and clinic catering to the needs of customers regarding infertility problems. It contains 55 employees including doctors, staff, IT team, and management with presence in Gujarat, India and provides online services. It also has research development infrastructure that studies and creates different methods based on Garbhasanskar.

**Application Risk Management Implementation Plan**

**List of Cybersecurity controls**

**Application Data Handling:**

1. Encryption: Encryption algorithms to secure the data and the information sensitive in nature.
2. Access Control: Limiting access of the application to the authorized users.
3. Backup and Recovery: Regular backup the application state and create redundant applications to recover to ensure business continuity.
4. Secure communication protocol: SSL/TLS application to encrypt and secure the data and connections during transmissions.
5. Update and Patching: Regular update the application and implement necessary patches to limit the vulnerabilities exposure.
6. Monitoring: Monitor the application and analyze it to ensure it’s integrity.

**Authentication:**

1. Password Strength Policy – Implementation of strong password policies stating the length of the password and the mandatory inclusion of charset and symbols.
2. Multi-factor authentication – MFA enforcement ensures the authentication mechanism providing extra layer of security along with login credentials.
3. Server Authentication: Server Authentication using PKI credentials.
4. Signed Code Identification: Implementation of code signing mechanism using PKI credentials.

**Cryptography:**

1. Key Management: Generation, storage, distribution, destruction of key securely according to required standards and encryption algorithms.
2. Symmetric Cryptography: Fast and efficient method of encryption and decryption using a single key.
3. Data Tampering prevention: Implementation of MAC, Digital signature, and hashes.

**User Accounts:**

1. Access Control: Limiting access of the application to the authorized users.
2. Account Lockout: Policy implementation of locking user accounts after consecutive unsuccessful login attempts.
3. Session Management: Session management policies and procedures for multiple logon session, time limit, termination, and credentials and cookies.
4. Account Recovery: For account recovery, enforcing authentication of user via secret questions, one time code, and more.

**Input Validation:**

1. Input Validation: Ensuring validation of inputs to avoid injections, buffer overflows and other vulnerabilities.
2. SAST: Static testing of applications like code reviews to detect any vulnerabilities due to coding non-sanitization.
3. RACE condition handling: Minimizing RACE conditions through error handling and synchronization.

**Auditing:**

1. Log Protection – The logs should be protected using encryption and access control mechanisms from potential manipulation.
2. Review and Logging – Monitor the database changes and review it. Along, log the changes in the database.
3. Security Assessment – Perform security risk assessments in a timely manner to detect, mitigate, and forecast the database threats and vulnerabilities.
4. Alerts – Real time alerts should be in place to alert the administrator of the potential unwanted or suspicious activity or changes in the database.

**Configuration Management:**

1. Release Manager: Responsible for software configuration management to ensure secure deployment and compliance.
2. Software Configuration Management Process: Managing and controlling components of software and their relationship.
3. Change Management: Managing, testing and deploying any changes to the software configurations and system.
4. Review and Monitor: Periodically reviewing and monitoring controls and configurations to prevent vulnerabilities and unauthorized access.

**Testing:**

1. Web Application Vulnerability Scanners: Scanners to detect vulnerabilities through crawling in the application.
2. Fuzzy Testing: Testing unvalidated and random data to detect and mitigate potential privilege escalation, crash, or unexpected response.
3. Code Reviews: Reviewing and testing code of application to detect and mitigate vulnerabilities and code quality.
4. Automation: Implementing automation techniques and tools to perform SAST, DAST, IAST analysis.
5. Test Plans and Procedures: Generate and update the test plans and procedures as per evolving advanced testing methodologies and tools.

**Deployment:**

1. Deployment Documentation: Instructions and guidelines for deploying software into the environment.
2. Secure Deployment: Implementing pre and post deployment risk assessments and monitoring to ensure secure environment for the application.

**Network Topology of Ayurhealthybaby**

**A diagram of a network

Description automatically generated**

The above image represent the topology of Ayurhealthybaby. Here the PC(s), printers and CCTV(s) are connected to the router. The router is connected to the internet as is defended by firewall. Additionally, the server and database of Ayurhealthybaby is also connected to the router. Moreover, VPN is established to provide encryption, authentication, and encapsulation for the communications.

**List of all Network Risk Management Implementation controls at Ayurhealthybaby**

**Application Data Handling:**

1. Encryption: Encryption algorithms to secure the data and the information sensitive in nature.
2. Access Control: Limiting access of the application to the authorized users.
3. Backup and Recovery: Regular backup the application state and create redundant applications to recover to ensure business continuity.
4. Secure communication protocol: SSL/TLS application to encrypt and secure the data and connections during transmissions.
5. Update and Patching: Regular update the application and implement necessary patches to limit the vulnerabilities exposure.

**Authentication:**

1. Password Strength Policy – Implementation of strong password policies stating the length of the password and the mandatory inclusion of charset and symbols.
2. Multi-factor authentication – MFA enforcement ensures the authentication mechanism providing extra layer of security along with login credentials.
3. Server Authentication: Server Authentication using PKI credentials.

**Cryptography:**

1. Key Management: Generation, storage, distribution, destruction of key securely according to required standards and encryption algorithms.
2. Symmetric Cryptography: Fast and efficient method of encryption and decryption using a single key.

**User Accounts:**

1. Access Control: Limiting access of the application to the authorized users.
2. Account Lockout: Policy implementation of locking user accounts after consecutive unsuccessful login attempts.
3. Session Management: Session management policies and procedures for multiple logon session, time limit, termination, and credentials and cookies.
4. Account Recovery: For account recovery, enforcing authentication of user via secret questions, one time code, and more.

**Input Validation:**

1. Input Validation: Ensuring validation of inputs to avoid injections, buffer overflows and other vulnerabilities.
2. SAST: Static testing of applications like code reviews to detect any vulnerabilities due to coding non-sanitization.

**Auditing:**

1. Log Protection – The logs should be protected using encryption and access control mechanisms from potential manipulation.
2. Review and Logging – Monitor the database changes and review it. Along, log the changes in the database.
3. Alerts – Real time alerts should be in place to alert the administrator of the potential unwanted or suspicious activity or changes in the database.

**Configuration Management:**

1. Release Manager: Responsible for software configuration management to ensure secure deployment and compliance.
2. Software Configuration Management Process: Managing and controlling components of software and their relationship.
3. Review and Monitor: Periodically reviewing and monitoring controls and configurations to prevent vulnerabilities and unauthorized access.

**Testing:**

1. Web Application Vulnerability Scanners: Scanners to detect vulnerabilities through crawling in the application.
2. Fuzzy Testing: Testing unvalidated and random data to detect and mitigate potential privilege escalation, crash, or unexpected response.
3. Code Reviews: Reviewing and testing code of application to detect and mitigate vulnerabilities and code quality.
4. Test Plans and Procedures: Generate and update the test plans and procedures as per evolving advanced testing methodologies and tools.

**Deployment:**

1. Deployment Documentation: Instructions and guidelines for deploying software into the environment.
2. Secure Deployment: Implementing pre and post deployment risk assessments and monitoring to ensure secure environment for the application.

**List of all Network Risk Management Implementation PRESENT/ABSENT controls at Ayurhealthybaby**

|  |  |
| --- | --- |
| **Controls** | **Status** |
| **Application Data Handling** | |
| Encryption | Present |
| Access Control | Present |
| Backup and Recovery | Present |
| Secure communication protocol | Present |
| Update and Patching | Present |
| Monitoring | Absent |
| **Authentication** | |
| Password Strength Policy | Present |
| Multi-factor authentication | Present |
| Server Authentication | Present |
| Signed Code Identification | Absent |
| **Cryptography** | |
| Key Management | Present |
| Symmetric Cryptography | Present |
| Data Tampering prevention | Absent |
| **User Accounts** | |
| Access Control | Present |
| Account Lockout | Present |
| Session Management | Present |
| Account Recovery | Present |
| **Input Validation** | |
| Input Validation | Present |
| SAST | Present |
| RACE condition handling | Absent |
| **Auditing** | |
| Log Protection | Present |
| Review and Logging | Present |
| Security Assessment | Absent |
| Alerts | Present |
| **Configuration Management** | |
| Release Manager | Present |
| Software Configuration Management Process | Present |
| Change Management | Absent |
| Review and Monitor | Present |
| **Testing** | |
| Web Application Vulnerability Scanners | Present |
| Fuzzy Testing | Present |
| Code Reviews | Present |
| Automation | Absent |
| Test Plans and Procedures | Present |
| **Deployement** | |
| Deployment Documentation | Present |
| Secure Deployment | Present |

**Critical Assets List in $ that exist in Ayurhealthybaby:**

|  |  |  |
| --- | --- | --- |
| Asset Number | Asset Name | Value |
| A1 | Sensitive Documents | 100,000 |
| A2 | Personnel Information | 20,000 |
| A3 | Financial Documents | 10,000 |
| A4 | Server | 5,000 |
| A5 | Network Services and Database | 50,000 |
| A6 | CCTV Hardware and Server | 2,000 |
| A7 | PCs | 7,000 |
| A8 | Printers | 1,000 |
| A9 | Reputation | Intangible |
| A10 | Clinical Materials and Hardware | 70,000 |

**List of Potential Vulnerabilities for critical assets where cybersecurity Implementation Controls are missing**

|  |  |
| --- | --- |
| Missing Controls | Vulnerabilities |
| **Application Data Handling** | |
| Monitoring | Ineffective log analysis, Lack of Incident detection and response |
| **Authentication** | |
| Signed Code Identification | Lack of Authentication, Unauthorized Access |
| **Cryptography** | |
| Data Tampering Prevention | Information Disclosure, Data Tampering, Lack of Compliance, Lack of Integrity |
| **Input Validation** | |
| RACE condition handling | Data Corruption, Timing-based attacks |
| **Auditing** | |
| Security Assessment | Ineffective Log Analysis, Weak Audit Trail Protection |
| **Configuration Management** | |
| Change Management | Unauthorized changes, Security Misconfigurations |
| **Testing** | |
| Automation | False Negative, Missing vulnerabilities, Security Misconfigurations |

**List of Potential Vulnerabilities:**

1. Unauthenticated/Unauthorized Access
2. Poor security policies and compliance
3. Lack of encryption implementation
4. Inadequate access-control
5. Data Tampering
6. Lack of Data Integrity
7. False Negatives
8. Timing-based attacks
9. Ineffective log analysis
10. Lack of monitoring and logging
11. Lack of Incident Response
12. Security Misconfigurations
13. Data Exfiltration / Data Leakage
14. Weak Audit Trail Protection

**List of Potential threats on Critical Assets:**

|  |  |
| --- | --- |
| **Assets** | **Threat** |
| Sensitive Documents | Disclosure of Information, data breach, data theft |
| Personnel Information | Disclosure of Information, data breach, data theft |
| Financial Documents | Disclosure of Information, data breach, data theft |
| Server | Denial of Service, Malware, Interruption of operations |
| Network Services and Database | Denial of Service, Malware, Interruption of operations |
| CCTV Hardware and Server | Denial of Service, Malware, Interruption of operations |
| PCs | Malware, Disclosure of Information |
| Printers | Interruption of operations |
| Reputation | Disclosure of Information, data breach, data theft, Market loss |
| Clinical Materials and Hardware | Interruption of operations |

**List of potential threats**

1. Disclosure of Information
2. Information theft and breach
3. Denial of Service – DoS/DDoS
4. Malware and virus
5. Interruption of Operations
6. Man-in-the-middle attack
7. IP address hijacking
8. Eavesdropping

**List of Potential Risks for Critical Assets Due to Missing Controls:**

|  |  |
| --- | --- |
| Missing Controls | Risk |
| **Application Data Handling** | |
| Monitoring | Prone to malware and virus attacks, Interruption in operations, Reputation and financial loss |
| **Authentication** | |
| Signed Code Identification | Information Disclosure and data breach, Unauthorized Access, Interruption in operations |
| **Cryptography** | |
| Data Tampering Prevention | Information Disclosure and data breach, Reputation and financial loss |
| **Input Validation** | |
| RACE condition handling | Interruption in operations, Unauthorized Access |
| **Auditing** | |
| Security Assessment | Prone to malware and virus attacks, Interruption in operations |
| **Configuration Management** | |
| Change Management | Interruption in operations |
| **Testing** | |
| Automation | Prone to malware and virus attacks |

**List of Potential Risks due to missing Cybersecurity Implementation Controls:**

1. Unauthorized access.
2. Reputation and financial loss
3. Prone to malware and virus attacks.
4. Interruption in operations.
5. Information Disclosure and data breach.

**List of recommended policies for each security control as a part of risk prevention strategy**

**Application Data Handling:**

* Classify the data based on sensitivity and apply controls according to the level of classification.
* Encrypt the data during transit and at rest.
* Implement access control mechanisms for authorized access.
* Take backup of the data regularly and ensure that recovery of the data is possible.

**Authentication:**

* Lock the account after a certain number of failed login attempts.
* Strengthen password policies from time to time and implement them in a stringent manner.
* Implement PKI infrastructure of server and user authentication.

**Cryptography:**

* Implement digital signature, MAC and hashes to prevent data from manipulation.
* Make sure the key management policies and procedures are to the required standards,

**User Accounts:**

* Lock the account after a certain number of failed login attempts.
* Monitor user accounts login and important activities pertaining to account security.
* Configure roles of the user account’s properly to avoid unauthorized access.

**Input Validation:**

* Validate and sanitize all incoming inputs to the application.
* Perform code reviews and static testing methods to detect and mitigate any vulnerabilities.

**Auditing:**

* Perform regular security risk assessment.
* Implement effective log analysis measures and methods.
* Audit trails should be protected to prevent from data manipulation.

**Configuration Management:**

* Enforce change management procedures.
* Monitor and review the configurations. Update the configurations when needed.

**Testing:**

* Use automation tools to make the testing efficient and deeper.
* Perform both manual and automated test to avoid false negatives and cover missing vulnerabilities by either means of testing.

**Deployment:**

* Perform security risk assessment to the previous and post deployment phases.

**List of recommended policies for each security control as a part of risk resilience/response strategy**

**Application Data Handling:**

* Change classification of the data to more stringent level.
* Form and implement recovery plans to ensure business continuity.
* Change the access controls of the affected components.

**Authentication:**

* Lock the affected accounts and revoke all privileges and permissions of the user account.
* Change the user account passwords.

**Cryptography:**

* Change encryption configurations like size and algorithms to strengthen the data security.
* Enforce key rotation and revocation policies.

**User Accounts:**

* Lock the account after a certain number of failed login attempts.
* Revoke the access controls of the affected account.
* Enhance monitoring activities of potential critical accounts.

**Input Validation:**

* Perform mitigation strategies to reverse the injection, buffer overflow attacks.
* To ensure data integrity, roll back the data values to the latest backup and redundant values.

**Configuration Management:**

* Rollback to the previous configurations to void the malicious configurations.
* Reverse or overcome the effects on the application and accounts due to the misconfigurations.
* Change access control of the non-essential accounts to enforce zero trust policy and least user privilege.

**Testing:**

* Continuously test the application using wide range of tools and human workforce to detect the vulnerability.
* Implement IAST methodology to detect vulnerability faster.

**Deployment:**

* Conduct security risk assessment of the current environment and application to make decision on changes required to mitigate the vulnerability and lessen the chance of exploitation.

**Web Application Security Policy**

**1. Overview**

Web application vulnerabilities account for the largest portion of attack vectors outside of malware. It is crucial that any web application be assessed for vulnerabilities and any vulnerabilities be remediated prior to production deployment.

**2. Purpose**

The purpose of this policy is to define web application security assessments within Ayurhealthybaby. Web application assessments are performed to identify potential or realized weaknesses as a result of inadvertent mis-configuration, weak authentication, insufficient error handling, sensitive information leakage, etc. Discovery and subsequent mitigation of these issues will limit the attack surface of Ayurhealthybaby services available both internally and externally as well as satisfy compliance with any relevant policies in place.

**3. Scope**

This policy covers all web application security assessments requested by any individual, group or department for the purposes of maintaining the security posture, compliance, risk management, and change control of technologies in use at Ayurhealthybaby.

All web application security assessments will be performed by delegated security personnel either employed or contracted by Ayurhealthybaby. All findings are considered confidential and are to be distributed to persons on a “need to know” basis. Distribution of any findings outside of Ayurhealthybaby is strictly prohibited unless approved by the Chief Information Officer.

Any relationships within multi-tiered applications found during the scoping phase will be included in the assessment unless explicitly limited. Limitations and subsequent justification will be documented prior to the start of the assessment.

**4. Policy**

4.1 Web applications are subject to security assessments based on the following criteria:

1. New or Major Application Release– will be subject to a full assessment prior to approval of the change control documentation and/or release into the live environment.
2. Third Party or Acquired Web Application– will be subject to full assessment after which it will be bound to policy requirements.
3. Point Releases– will be subject to an appropriate assessment level based on the risk of the changes in the application functionality and/or architecture.
4. Patch Releases– will be subject to an appropriate assessment level based on the risk of the changes to the application functionality and/or architecture.
5. Emergency Releases– An emergency release will be allowed to forgo security assessments and carry the assumed risk until such time that a proper assessment can be carried out. Emergency releases will be designated as such by the Chief Information Officer or an appropriate manager who has been delegated this authority.

4.2 All security issues that are discovered during assessments must be mitigated based upon the following risk levels. The Risk Levels are based on the OWASP Risk Rating Methodology. Remediation validation testing will be required to validate fix and/or mitigation strategies for any discovered issues of Medium risk level or greater.

1. High– Any high risk issue must be fixed immediately or other mitigation strategies must be put in place to limit exposure before deployment. Applications with high risk issues are subject to being taken off-line or denied release into the live environment.
2. Medium– Medium risk issues should be reviewed to determine what is required to mitigate and scheduled accordingly. Applications with medium risk issues may be taken off-line or denied release into the live environment based on the number of issues and if multiple issues increase the risk to an unacceptable level. Issues should be fixed in a patch/point release unless other mitigation strategies will limit exposure.
3. Low– Issue should be reviewed to determine what is required to correct the issue and scheduled accordingly.

4.3 The following security assessment levels shall be established by the InfoSec organization or other designated organization that will be performing the assessments.

1. Full– A full assessment is comprised of tests for all known web application vulnerabilities using both automated and manual tools based on the OWASP Testing Guide. A full assessment will use manual penetration testing techniques to validate discovered vulnerabilities to determine the overall risk of any and all discovered.
2. Quick– A quick assessment will consist of a (typically) automated scan of an application for the OWASP Top Ten web application security risks at a minimum.
3. Targeted – A targeted assessment is performed to verify vulnerability remediation changes or new application functionality.

4.4 The current approved web application security assessment tools in use which will be used for testing are:

* Burp Suite
* Wireshark
* …

Other tools and/or techniques may be used depending upon what is found in the default assessment and the need to determine validity and risk are subject to the discretion of the Security Engineering team.

**5. Policy Compliance**

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Web application assessments are a requirement of the change control process and are required to adhere to this policy unless found to be exempt. All application releases must pass through the change control process. Any web applications that do not adhere to this policy may be taken offline until such time that a formal assessment can be performed at the discretion of the Chief Information Officer.

**6. Related Standards, Policies and Processes**

OWASP Top Ten Project

OWASP Testing Guide

OWASP Risk Rating Methodology

**7. Definitions and Terms**

None.

**8. Revision History**

|  |  |  |
| --- | --- | --- |
| **Date of Change** | **Responsible** | **Summary of Change** |
| December 2023 | Kalp Shah | V1.0 = Implementation of Security Risk Assessment |