**CY5200 Security Risk Management and Assessment**

**Module 7 Assignment**

**By: Kalp Shah**

**002232460**

**Note: Part I, III, IV is submitted in Excel submission link. (III and IV is combined)**

**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.

**Network Risk Management Implementation controls**

**Enclave Protection**

Enclaves are isolated networks restricted to use for the authorized personnels only that contains organization’s private, confidential, and sensitive data meant for internal use.  
  
**Network Segmentation** – It divides the network into segments providing isolation limiting the impact of any malicious activity.  
**Endpoint Protection** – The endpoints are the location/devices like server, PC etc. and protecting them is one of the crucial tasks as all of them are assets to an organization.  
**VPN** – A tunneling service that provides secure and encrypted communications between devices or system ensuring confidentiality.  
**Access Control** – Managing access to the infrastructure and system components of an organization and allowing only authorized and authenticated users only.  
**SIEM** – A tool and an ecosystem to monitor, identify, detect, manage, analyze and log the communications and connections between the systems.  
**Demilitarized Zone (DMZ)** – Secure isolated zone to protect and prevent exposure from the external communications and entities. It contains sensitive, confidential and crucial data,  
**Test Access Ports (TAP)** – Device for monitoring and capturing the traffic for security purposes and troubleshooting.

**Firewalls**

Firewalls is a defensive measure exposed first to the incoming traffic and request from the external networks. The rules and measures are set in place to control, restrict, and allow required and desired connections and traffic.

**Web Application Firewalls –** Firewall system to protect web infrastructure of an organization. **Next Generation Firewalls –** State of the art firewall covering most of the digital infrastructure and securing it along with deep packet analysis and enhance security measures and configurations. **Monitoring and Logging –** Capturing the communications and connections between the device, analyzing it and continuously monitoring any suspicious activity. **Traffic Filtering –** Whitelisting and blacklisting the network traffic and only allowing whitelisted traffic that is deemed secure and normal for the infrastructure and don’t pose any malicious threat or impact. **Regular Updates –** The regular upgrades and patching of the firewall to secure from newly emerged threats and vulnerabilities. **Threat Reports and Intelligence –** Staying updated with the current threat maps and vectors in order to make suitable changes and monitoring the network infrastructure.  **Routers**

Routers publishes connections and transfers data packets within the networks.

**Proxies and VPN** - A tunneling service that provides secure and encrypted communications between devices or system ensuring confidentiality. Also, a proxy shadows the network infrastructure and prevents direct exposure from the external networks and connections.  
**Access Control and IP tables** – The list that defines who can access the specific restricted system or information. Also, IP tables consists of the IPs and protocols that are allowed or denied access to the resources.  
**Secure Configurations -** Settings and measures of the router to enhance the security posture of the network infrastructure. **Regular Updates –** Timely and periodically upgrades of the firmware to patch any known vulnerabilities within the devices.

**Network Topology of Ayurhealthybaby**

A diagram of computer 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.

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

**Enclave Protection**

**Network Segmentation** – It divides the network into segments providing isolation limiting the impact of any malicious activity.  
**Access Control** – Managing access to the infrastructure and system components of an organization and allowing only authorized and authenticated users only.

**Firewalls**

**Web Application Firewalls –** Firewall system to protect web infrastructure of an organization. **Monitoring and Logging –** Capturing the communications and connections between the device, analyzing it and continuously monitoring any suspicious activity. **Traffic Filtering –** Whitelisting and blacklisting the network traffic and only allowing whitelisted traffic that is deemed secure and normal for the infrastructure and don’t pose any malicious threat or impact. **Regular Updates –** The regular upgrades and patching of the firewall to secure from newly emerged threats and vulnerabilities.

**Routers**

**Access Control and IP tables** – The list that defines who can access the specific restricted system or information. Also, IP tables consists of the IPs and protocols that are allowed or denied access to the resources.

**Regular Updates –** Timely and periodically upgrades of the firmware to patch any known vulnerabilities within the devices.

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

|  |  |
| --- | --- |
| Control | Status |
| **Enclave Protection** | |
| Network Segmentation | Present |
| Endpoint Protection | Absent |
| VPN | Absent |
| Access Control | Present |
| SIEM | Absent |
| Demilitarized Zone (DMZ) | Absent |
| Test Access Ports (TAP) | Absent |
| **Firewalls** | |
| Web Application Firewalls | Present |
| Next Generation Firewalls | Absent |
| Monitoring and Logging | Present |
| Traffic Filtering | Present |
| Regular Updates | Present |
| Threat Reports and Intelligence | Absent |
| **Routers** | |
| Proxies and VPN | Absent |
| Access Control and IP tables | Present |
| Secure Configurations | Absent |
| Regular Updates | 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/Not Fully Present Controls** | **Vulnerability** |
| **Enclave Protection** | |
| Endpoint Protection | Sensitive Information Disclosure, Unauthorized Access, Weak Network Security, Inadequate security policies and compliance |
| VPN | Unauthenticated Access, Weak Network Security, Inadequate security policies and compliance |
| SIEM | Weak Network Security, Inadequate security policies and compliance |
| Demilitarized Zone (DMZ) | Information Theft, Weak Network Security, Inadequate security policies and compliance |
| Test Access Ports (TAP) | Inadequate security policies and compliance |
| **Firewalls** | |
| Next Generation Firewalls | Weak Network Security, Application based vulnerabilities |
| Threat Reports and Intelligence | Weak Network Security |
| **Routers** | |
| Proxies and VPN | Information Theft, Weak Network Security, Inadequate security policies and compliance |
| Secure Configurations | Default credentials and configurations, Weak Network Security, Inadequate security policies and compliance, Unauthenticated Access |

**List of Potential Vulnerabilities:**

1. Unauthenticated/Unauthorized Access
2. Sensitive Information Disclosure
3. Information theft and breach
4. Application Based vulnerabilities
5. Weak network security
6. Poor security policies and compliance

**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, Impostor, Disclosure of Information |
| Printers | Interruption of operations |
| Reputation | Disclosure of Information, data breach, data theft, Market loss |
| Clinical Materials and Hardware | Physical theft, Interruption of operations |

**List of potential threats**

1. Disclosure of Information
2. Information theft and breach
3. Denial of Service
4. Malware and virus
5. Interruption of Operations
6. Impostor and physical theft

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

|  |  |
| --- | --- |
| **Missing/Not Fully Present Controls** | **Risk** |
| **Enclave Protection** | |
| Endpoint Protection | Unauthorized access, network attacks, prone to malware and viruses |
| VPN | Unauthenticated and unauthorized access, Information Disclosure, unencrypted channels |
| SIEM | Lack of detection and incident response |
| Demilitarized Zone (DMZ) | Unauthorized access, network attacks |
| Test Access Ports (TAP) | Unauthorized access, lack of security testing |
| **Firewalls** | |
| Next Generation Firewalls | Weak network security, Lack of application-level security |
| Threat Reports and Intelligence | Lack of detection and incident response |
| **Routers** | |
| Proxies and VPN | Unauthenticated and unauthorized access, Information Disclosure, unencrypted channels |
| Secure Configurations | Unauthenticated access, Data breaches, interruption in operations |

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

1. Unauthorized access to the network infrastructure.
2. Insecure and unencrypted network channels
3. Lack of detection and incident response.
4. Weak network security.
5. Prone to malware and virus attacks.
6. Lack of application-level security.
7. Interruption in operations.
8. Information Disclosure and data breach.

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

**Enclave Protection**

* Implement access control policies for authorized and authenticated access of the enclave infrastructure.
* Harden the endpoints of the enclave network to restrict the discovery and access from an unauthorized user.
* Add VPN layer to the network for encrypted communication and authentication purposes.
* Implementation of SIEM for continuous monitoring and logging of the network connections.

**Firewalls**

* Establish next-generation firewalls for deep packet analysis and application-level security.
* Regular update the firewalls to detect and block malicious connections that are found in the near time-frame.
* Check the threat and incident report to stay updated on the current threat vectors and attacks to secure the infrastructure.

**Routers**

* Add VPN layer to the network for encrypted communication and authentication purposes. Implement proxies to prevent direct exposure of the Ayurhealthybaby’s digital infrastructure.
* Review the security configurations on a timely basis.
* Update the credentials of the network infrastructure and maintain the access control list along with the IP tables.
* Restrict the connections to which are required.

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

**Enclave Protection**

* Create and establish incident response plan.
* Make strategy and implement for data recovery from the previous backup.
* Isolate the affected infrastructure to ensure least interruptions in operations.

**Firewalls**

* Redirect traffic to the redundant infrastructure and isolate the affected system.
* Shift firewalls to stealth mode for enhanced surveillance and logging.
* Implement malware and virus detection procedures in depth.
* Modify the firewall rules according to an attack.

**Routers**

* Rollback to the previous security configurations to nullify the malicious configuration changes.
* If the router is compromised, shift to the redundant router.
* Harden the security configuration and restrict the communication and protocol access as required.
* Implement network segmentation restricting the impact of an attack and ensure business continuity.

**Router Security Policy**

1. **Overview**

See Purpose

1. **Purpose**

This document describes a required minimal security configuration for all routers and switches connecting to a production network or used in a production capacity at or on behalf of Ayurhealthybaby.

1. **Scope**

All employees, contractors, consultants, temporary and other workers at Ayurhealthybaby and its subsidiaries must adhere to this policy. All routers and switches connected to Ayurhealthybaby production networks are affected.

1. **Policy**

Every router must meet the following configuration standards:

1. No local user accounts are configured on the router. Routers and switches must use TACACS+ for all user authentication.
2. The enable password on the router or switch must be kept in a secure encrypted form. The router or switch must have the enable password set to the current production router/switch password from the device’s support organization.
3. The following services or features must be disabled:
4. IP directed broadcasts
5. Incoming packets at the router/switch sourced with invalid addresses such as RFC1918 addresses
6. TCP small services
7. UDP small services
8. All source routing and switching
9. All web services running on router
10. Ayurhealthybaby discovery protocol on Internet connected interfaces
11. Telnet, FTP, and HTTP services
12. Auto-configuration
13. The following services should be disabled unless a business justification is provided:

a. Ayurhealthybaby discovery protocol and other discovery protocols

b. Dynamic trunking

c. Scripting environments, such as the TCL shell

1. The following services must be configured:
2. Password-encryption

b. NTP configured to a corporate standard source

1. All routing updates shall be done using secure routing updates.
2. Use corporate standardized SNMP community strings. Default strings, such as public or private must be removed. SNMP must be configured to use the most secure version of the protocol allowed for by the combination of the device and management systems.
3. Access control lists must be used to limit the source and type of traffic that can terminate on the device itself.
4. Access control lists for transiting the device are to be added as business needs arise.
5. The router must be included in the corporate enterprise management system with a designated point of contact.
6. Each router must have the following statement presented for all forms of login whether remote or local:

"UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action, and may be reported to law enforcement. There is no right to privacy on this device. Use of this system shall constitute consent to monitoring."

1. Telnet may never be used across any network to manage a router, unless there is a secure tunnel protecting the entire communication path. SSH version 2 is the preferred management protocol.
2. Dynamic routing protocols must use authentication in routing updates sent to neighbors. Password hashing for the authentication string must be enabled when supported.
3. The corporate router configuration standard will define the category of sensitive routing and switching devices, and require additional services or configuration on sensitive devices including:
4. IP access list accounting
5. Device logging
6. Incoming packets at the router sourced with invalid addresses, such as RFC1918 addresses, or those that could be used to spoof network traffic shall be dropped
7. Router console and modem access must be restricted by additional security controls
8. **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.

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

None.

1. **Definitions and Terms**

None.

1. **Revision History**

|  |  |  |
| --- | --- | --- |
| Date of Change | Responsible | Summary of Change |
| August 2021 | Kalp Shah | V 1.0 Updated rules on Web-Application based firewalls |