**CY5200 Security Risk Management and Assessment**

**Module 8 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**

**Ports, Protocols, and Services  
  
Service Hardening** – Periodically updates and patches of the network services to prevent any potential threats due to existing vulnerabilities.

**Secure Protocols** – Use HTTPS instead of HTTP, SFTP instead of FTP and more.

**Firewall** – Implement firewalls to restrict access to the services and port to only required purposes. Also, helps in preventing DoS/DDoS attacks.

**Protocols and Traffic Filtering** – Filter IPv4 and IPv6 along with the incoming traffic to reduce potential security risk and misconfigurations.

**Unicast Reverse Path Forwarding** - uRPF provides defense mechanism towards IP address spoofing.

**Device Management**

**VMS –** Used to create, manage and execute virtual machines for isolated environments to test security, flexibility, and efficiency.

**In-Band Management –** In-band management refers to using the same network for organization devices like router, switches etc.

**Out-Band Management -** Out-band management refers to using the different or multiple external network for organization devices like router, switches etc. providing isolation and grouping mechanisms according to the nature of tasks.

**Regular Updates –** Timely and periodic upgrades of versions, firmware, and configurations to patch vulnerabilities and improve performance.

**Device Monitoring**

**SNMP -** A protocol for managing and keeping an eye on network devices.

**Network Management Station -** Using SNMP or other management protocols, this central system is in charge of controlling and keeping an eye on network devices.

**SIEM -** Security system that gathers, correlates, and analyzes security-related data from several sources (such as logs, events, and alarms).

**Network Authentication, Authorization, and Accounting (Auditing)**

**Access Control -** The method of limiting user access to resources on the network according to their roles, identities, and permissions.

**Auditing -** Documenting occurrences pertaining to configuration modifications, user access, and security incidents.

**Router Password Protection -** Keeping router passwords strong, distinct, and up to date in order to thwart unwanted access.

**NIDS**

**LAN IDS -** Keeps track on network traffic inside a particular LAN segment in order to identify potentially harmful or suspicious behavior.

**External IDS -** Keeps track on network traffic from external source in order to identify potentially harmful or suspicious behavior.

**Signature and Anomaly Based Detection -** Predetermined signatures, which are patterns of known attacks, or anomaly detection, which finds departures from typical activity.

**Switches, VLANs**

**Physical Switches and wiring –** Devices in a local network are connected by physical network switches through electrical wires.

**VLAN and VLAN1-** The logical division of a physical network into several virtual networks. Performance, manageability, and security are all improved.

**VLAN Trunking –** Availability of multiple VLANs among single physical connection within switches.

**VLAN Port Security –** Port restriction of non-used or non-authorized services or protocols.

**VLAN 802.1x and Management Policy Server –** Network device policy ensuring access authentication mechanisms.

**VPN**

**Gateway-to-Gateway –** Network to network connection over the internet with security measures.

**Host-to-Gateway –** Host device connection to the external network for securely communicating over the internet.

**Network Topology of Ayurhealthybaby**

A diagram of a 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. Moreover, VPN is established to provide encryption, authentication, and encapsulation for the communications.

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

**Ports, Protocols, and Services  
  
Service Hardening** – Periodically updates and patches of the network services to prevent any potential threats due to existing vulnerabilities.

**Secure Protocols** – Use HTTPS instead of HTTP, SFTP instead of FTP and more.

**Firewall** – Implement firewalls to restrict access to the services and port to only required purposes. Also, helps in preventing DoS/DDoS attacks.

**Protocols and Traffic Filtering** – Filter IPv4 and IPv6 along with the incoming traffic to reduce potential security risk and misconfigurations.

**Device Management**

**In-Band Management –** In-band management refers to using the same network for organization devices like router, switches etc.

**Out-Band Management -** Out-band management refers to using the different or multiple external network for organization devices like router, switches etc. providing isolation and grouping mechanisms according to the nature of tasks.

**Regular Updates –** Timely and periodic upgrades of versions, firmware, and configurations to patch vulnerabilities and improve performance.

**Device Monitoring**

**SNMP -** A protocol for managing and keeping an eye on network devices.

**Network Management Station -** Using SNMP or other management protocols, this central system is in charge of controlling and keeping an eye on network devices.

**Network Authentication, Authorization, and Accounting (Auditing)**

**Access Control -** The method of limiting user access to resources on the network according to their roles, identities, and permissions.

**Auditing -** Documenting occurrences pertaining to configuration modifications, user access, and security incidents.

**Router Password Protection -** Keeping router passwords strong, distinct, and up to date in order to thwart unwanted access.

**NIDS**

**External IDS -** Keeps track on network traffic from external source in order to identify potentially harmful or suspicious behavior.

**Signature and Anomaly Based Detection -** Predetermined signatures, which are patterns of known attacks, or anomaly detection, which finds departures from typical activity.

**Switches, VLANs**

**Physical Switches and wiring –** Devices in a local network are connected by physical network switches through electrical wires.

**VLAN and VLAN1-** The logical division of a physical network into several virtual networks. Performance, manageability, and security are all improved.

**VLAN Port Security –** Port restriction of non-used or non-authorized services or protocols.

**VPN**

**Host-to-Gateway –** Host device connection to the external network for securely communicating over the internet.

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

|  |  |
| --- | --- |
| **Control** | **Status** |
| **Ports, Protocols, and Services** | |
| Service Hardening | Present |
| Secure Protocols | Present |
| Firewall | Present |
| Protocols and Traffic Filtering | Present |
| Unicast Reverse Path Forwading | Absent |
| **Device Management** | |
| VMS | Absent |
| In-Band Management | Present |
| Out-Band Management | Present |
| Regular Updates | Present |
| **Device Monitoring** | |
| SNMP | Present |
| Network Management Station | Present |
| SIEM | Absent |
| **Network Authentication, Authorization, and Accounting (Auditing)** | |
| Access Control | Present |
| Auditing | Present |
| Router Password Protection | Present |
| **NIDS** | |
| External IDS | Present |
| Signature and Anomaly Based Detection | Present |
| LAN IDS | Absent |
| **Switches, VLANS** | |
| Physical Switches and wiring | Present |
| VLAN and VLAN1 | Present |
| VLAN Port Security | Present |
| VLAN Trunking | Absent |
| VLAN 802.1x and Management Policy Server | Absent |
| **VPN** | |
| Host-to-Gateway | Present |
| Gateway-to-Gateway | Absent |

**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 |
| **Ports, Protocols, and Services** | |
| Unicast Reverse Path Forwarding | IP address spoofing |
| **Device Management** | |
| VMS | Unpatched versions, Lack of vulnerability assessment and tracking |
| **Device Monitoring** | |
| SIEM | Lack of monitoring and logging, Weak Network Security, Inadequate security policies and compliance |
| **NIDS** | |
| LAN IDS | Inadequate security policies, Lack of internal traffic monitoring |
| **Switches, VLANS** | |
| VLAN Trunking Protection | Inadequate VLAN segmentation, VLAN hopping |
| VLAN 802.1x and Management Policy Server | Lack of authentication, Inadequate access-control, Lack of cryptography implementation |
| **VPN** | |
| Gateway-to-Gateway | Lack of cryptography implementation, Lack of authentication |

**List of Potential Vulnerabilities:**

1. Unauthenticated/Unauthorized Access
2. Weak network security
3. Poor security policies and compliance
4. Lack of cryptography implementation
5. Inadequate access-control
6. Inadequate VLAN segmentation
7. VLAN hopping
8. Lack of monitoring and logging
9. Unpatched versions
10. IP address spoofing
11. Lack of vulnerability assessment and tracking

**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 |
| **Ports, Protocols, and Services** | |
| Unicast Reverse Path Forwarding | Interruption of operations |
| **Device Management** | |
| VMS | Compromise of network |
| **Device Monitoring** | |
| SIEM | Unauthorized access to the network infrastructure, Information Disclosure and data breach, Interruption of operations |
| **NIDS** | |
| LAN IDS | Malicious traffic, Interruption of Operations |
| **Switches, VLANS** | |
| VLAN Trunking | Interruption of operations, Compromise of network, Disgruntled employee |
| VLAN 802.1x and Management Policy Server | Unauthorized access to the network infrastructure, Information Disclosure and data breach |
| **VPN** | |
| Gateway-to-Gateway | Unauthorized access to the network infrastructure, Information Disclosure and data breach |

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

1. Unauthorized access to the network infrastructure.
2. Prone to malware and virus attacks.
3. Interruption in operations.
4. Information Disclosure and data breach.
5. Compromise of network.
6. Disgruntled employee.

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

**Port, Protocol, Service:**

* Only use authorized and required ports, protocols, and services.
* Restrict or block all non-essential and not used ports
* Conduct periodic risk assessments and update the services as per the current security regulations and compliance.

**Device Management:**

* Use strong and unique passwords for the devices.
* Implement regular vulnerability assessments and patches along with regular updates.
* Establish access controls.
* Implement principle of least privilege to restrict unauthorized access.
* Implement measures such as endpoint protection, encryption, and secure device configurations.

**Device Monitoring:**

* Formulate incident response plan and execute few drills.
* Implement IDS and IPS systems for network monitoring.
* Use logging and alerting triggering mechanisms.

**Network Authentication, Authorization, and Accounting (Auditing):**

* Implement authentication and authorization.
* Regularly review and update access permissions based on job roles and responsibilities.
* Implement continuous monitoring for unauthorized access attempts.
* Conduct regular audits of user accounts, permissions, and network configurations.
* Implement corrective actions based on audit findings to mitigate identified risks.

**NIDS:**

* Define policies for the deployment and operation of NIDS.
* Regularly update intrusion detection signatures and configurations based on the latest threat intelligence.
* Conduct regular risk assessments to ensure NIDS effectiveness aligns with evolving threats.

**Switches, VLANs:**

* Develop policies for network segmentation using switches and VLANs.
* Regularly assess and adjust segmentation to limit lateral movement in case of a security breach.
* Implement secure VLAN configurations and regularly audit switch configurations for compliance.

**VPN:**

* Establish policies for secure VPN usage, including encryption and authentication.
* Assess VPN configurations for vulnerabilities.
* Monitor and detect anomalies in VPN traffic.

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

**Port, Protocol, Service:**

* Implement enhanced firewall rules and execute stealth mode.
* Establish secure protocols like HTTPS and SSH for communication

**Device Management:**

* Implement encryption and hashing channels for communication.
* Establish configuration change management system to approve and track desired configurations.

**Device Monitoring:**

* Execute SIEM alert and monitoring modes along with incident response mechanisms.
* Monitor network activity and act vigorously on the malicious activity.

**Network Authentication, Authorization, and Accounting (Auditing):**

* Make and implement guidelines for continuous monitoring of network traffic and activities.
* Establish log retention periods and procedures for analyzing logs.
* Ensure compliance with current standards and frameworks.

**NIDS:**

* Patch and update IDS/IPS systems for monitoring and detection eliminating any potential current vulnerabilities.

**Switches, VLANs:**

* Configure network segmentation to avoid VLAN hopping and misconfigurations.
* Check whether single VLAN switch isn’t exposed to the ports for heavy incoming traffic.
* Ensure port and services security.

**VPN:**

* Implement gateway-gateway VPN for central communications encryption and encapsulation.
* Keep the VPN version updated and patched to avoid vulnerabilities.

**Remote Access Tools Policy**

# **Overview**

Remote desktop software, also known as remote access tools, provide a way for computer users and support staff alike to share screens, access work computer systems from home, and vice versa. Examples of such software include LogMeIn, GoToMyPC, VNC (Virtual Network Computing), and Windows Remote Desktop (RDP).  While these tools can save significant time and money by eliminating travel and enabling collaboration, they also provide a back door into the Ayurhealthybaby network that can be used for theft of, unauthorized access to, or destruction of assets. As a result, only approved, monitored, and properly controlled remote access tools may be used on Ayurhealthybaby computer systems.

# **Purpose**

This policy defines the requirements for remote access tools used at Ayurhealthybaby

# **Scope**

This policy applies to all remote access where either end of the communication terminates at a Ayurhealthybaby computer asset

# **Policy**

All remote access tools used to communicate between Ayurhealthybaby assets and other systems must comply with the following policy requirements.

**4.1 Remote Access Tools**

Ayurhealthybaby provides mechanisms to collaborate between internal users, with external partners, and from non-Ayurhealthybaby systems. The approved software list can be obtained from <link-to-approved-remote-access-software-list>. Because proper configuration is important for secure use of these tools, mandatory configuration procedures are provided for each of the approved tools.

The approved software list may change at any time, but the following requirements will be used for selecting approved products:

1. All remote access tools or systems that allow communication to Ayurhealthybaby resources from the Internet or external partner systems must require multi-factor authentication. Examples include authentication tokens and smart cards that require an additional PIN or password.
2. The authentication database source must be Active Directory or LDAP, and the authentication protocol must involve a challenge-response protocol that is not susceptible to replay attacks. The remote access tool must mutually authenticate both ends of the session.
3. Remote access tools must support the Ayurhealthybaby application layer proxy rather than direct connections through the perimeter firewall(s).
4. Remote access tools must support strong, end-to-end encryption of the remote access communication channels as specified in the Ayurhealthybaby network encryption protocols policy.
5. All Ayurhealthybaby antivirus, data loss prevention, and other security systems must not be disabled, interfered with, or circumvented in any way.

All remote access tools must be purchased through the standard Ayurhealthybaby procurement process, and the information technology group must approve the purchase.

# **Policy Compliance**

Compliance Measurement

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

Exceptions

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

Non-Compliance

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

# **Related Standards, Policies and Processes**

None.

# **Definitions and Terms**

The following definition and terms can be found in the SANS Glossary located at:

https://www.sans.org/security-resources/glossary-of-terms/

* Application layer proxy

# **Revision History**

|  |  |  |
| --- | --- | --- |
| Date of Change | Responsible | Summary of Change |
| Aug 2023 | Kalp Shah | Implementation of MFA before accessing remote services. |

**Virtual Private Network Policy**

**1.0 Purpose**

The purpose of this policy is to provide guidelines for Remote Access IPSec or L2TP Virtual Private Network (VPN) connections to the Ayurhealthybaby corporate network.

**2.0 Scope**

This policy applies to all Ayurhealthybaby employees, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties utilizing VPNs to access the Ayurhealthybaby network. This policy applies to implementations of VPN that are directed through an IPSec Concentrator.

**3.0 Policy**

Approved Ayurhealthybaby employees and authorized third parties (customers, vendors, etc.) may utilize the benefits of VPNs, which are a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees. Further details may be found in the *Remote Access Policy*.

Additionally,

1. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to Ayurhealthybaby internal networks.
2. VPN use is to be controlled using either a one-time password authentication such as a token device or a public/private key system with a strong passphrase.
3. When actively connected to the corporate network, VPNs will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.
4. Dual (split) tunneling is NOT permitted; only one network connection is allowed.
5. VPN gateways will be set up and managed by Ayurhealthybaby network operational groups.
6. All computers connected to Ayurhealthybaby internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the corporate standard (provide URL to this software); this includes personal computers.
7. VPN users will be automatically disconnected from Ayurhealthybaby's network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.
8. The VPN concentrator is limited to an absolute connection time of 24 hours.
9. Users of computers that are not Ayurhealthybaby-owned equipment must configure the equipment to comply with Ayurhealthybaby's VPN and Network policies.
10. Only InfoSec-approved VPN clients may be used.
11. By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of Ayurhealthybaby's network, and as such are subject to the same rules and regulations that apply to Ayurhealthybaby-owned equipment, i.e., their machines must be configured to comply with InfoSec's Security Policies.

**4.0 Enforcement**

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

**5.0 Definitions**

**Term Definition**

IPSec Concentrator A device in which VPN connections are terminated.

**6.0 Revision History**

|  |  |  |
| --- | --- | --- |
| Date of Change | Responsible | Summary of Change |
| Feb 2022 | Kalp Shah | Updated policy on usage of Info-Sec VPNs only. |