GROUP 8

Design Security Architecture

ISMAIL MAHAMED 125052191

JASKARAN SOHAL 150343218

RAYYAN KHAN 155534209

EASTON SOARES 108851213

Table of Contents

Business Requirements

List of Requirements

Requirement ID	Requirement description	Test case description	Acceptance criteria
1	Develop a customer-facing website for product purchases, contact with sales representatives, and company information.	Launch a publicly accessible website with e-commerce features and contact options.	Verify the website's functionality; external users can access and use it.
2	Implement network segregation between the Customer network and internal infrastructure.	Establish two distinct security zones: one for internal employee traffic and one for external customer traffic.	Conduct tests to confirm that internal users have access to both zones, while external users can only access the e-commerce section.
3	Ensure that all transactions and privacy practices adhere to Canadian legal requirements.	Deploy the necessary software to safeguard network and public-facing services.	Conduct penetration tests on critical services such as DNS and HTML to verify compliance.
4	Enable employees to access an internal file-sharing website.	Create a file-sharing platform accessible to all employees.	Validate that Samba is integrated with all employee machines for seamless access.

Business Applications

List of Software

Business Software

PHP7
Wordpress
LibreOffice
Github
jQuery

Infrastructure Software

Ubuntu
Linux/Windows
Docker
SMBclient
Apache
PiHole

Role	OS	Software	Version
Private DNS	Ubuntu	PiHole	Latest
DHCP Server	Ubuntu	PiHole	Latest
Active Directory	Windows Server 2019	Windows Server	2019
OSPF (Maybe on Network Services too not sure where)	Ubuntu	Quagga	Latest
Firewall	Ubuntu	Iptables/UFW	Latest
Container Host	Ubuntu	Docker	Latest
User	Ubuntu	Smbclient	Latest
Admin	Ubuntu	Smbclient	Latest
Filesharing	Ubuntu	Samba	Latest
Corp Website	Ubuntu	Apache2	Latest
Internal Website	Ubuntu	Apache2	Latest
Ecommerce Website	Ubuntu	Apache2	Latest
Public DNS	Ubuntu	Pihole	Latest

Security Controls

➢ MA-2 Controlled Maintenance

Control:

a) Schedule, document, and review records of maintenance, repair, and replacement on system components in accordance with manufacturer or vendor specifications and/or organizational requirements;

b) Approve and monitor all maintenance activities, whether performed on site or remotely and whether the system or system components are serviced on site or removed to another location;

c) Require that [Assignment: organization-defined personnel or roles] explicitly approve the removal of the system or system components from organizational facilities for off-site maintenance, repair, or replacement;

d) Sanitize equipment to remove the following information from associated media prior to removal from organizational facilities for off-site maintenance, repair, or replacement: [Assignment: organization-defined information];

e) Check all potentially impacted controls to verify that the controls are still functioning properly following maintenance, repair, or replacement actions; and

Include the following information in organizational maintenance records: [Assignment: organization-defined information]

➢ CM-2 Baseline Configuration

Control:

a) Develop, document, and maintain under configuration control, a current baseline configuration of the system; and

b) Review and update the baseline configuration of the system:
   1. [Assignment: organization-defined frequency];
   2. When required due to [Assignment: organization-defined circumstances]; and
   3. When system components are installed or upgraded.

➢ CA-8 Penetration Testing

Control: Conduct penetration testing [Assignment: organization-defined frequency] on [Assignment: organization-defined systems or system components].

Discussion: Penetration testing is a specialized type of assessment conducted on systems or individual system components to identify vulnerabilities that could be exploited by adversaries.

Penetration testing goes beyond automated vulnerability scanning and is conducted by agents and teams with demonstrable skills and experience that include technical expertise in network, operating system, and/or application level security. Penetration testing can be used to validate vulnerabilities or determine the degree of penetration resistance of systems to adversaries within specified constraints. Such constraints include time, resources, and skills. Penetration testing attempts to duplicate the actions of adversaries and provides a more in-depth analysis of security- and privacy-related weaknesses or deficiencies. Penetration testing is especially important when organizations are transitioning from older technologies to newer technologies (e.g., transitioning from IPv4 to IPv6 network protocols).

➢ AC-2 Account Management

Control:

a) Define and document the types of accounts allowed and specifically prohibited for use within the system;

b) Assign account managers;

c) Require [Assignment: organization-defined prerequisites and criteria] for group and role membership;

d) Specify:
   i) Authorized users of the system;
   ii) Group and role membership; and
   iii) Access authorizations (i.e., privileges) and [Assignment: organization-defined attributes (as required)] for each account;

e) Require approvals by [Assignment: organization-defined personnel or roles] for requests to create accounts;

f) Create, enable, modify, disable, and remove accounts in accordance with [Assignment: organization-defined policy, procedures, prerequisites, and criteria];

➢ AC-17 Remote Access

Control:

a) Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and

b) Authorize each type of remote access to the system prior to allowing such connections.

NIST Compliance with Canadian Cybersecurity Laws

1. **MA-2 Controlled Maintenance**:

   Alignment with Regulations:

   - PIPEDA and the Digital Privacy Act require organizations to implement measures to protect personal information. Controlled maintenance ensures that any system maintenance activities, whether on-site or off-site, are carried out in a way that does not compromise the security and confidentiality of personal data. It helps prevent unauthorized access or disclosure during maintenance.

   Specifics:

   - Subpoint (a) emphasizes the importance of scheduling and documenting maintenance activities according to manufacturer or organizational specifications. This aligns with PIPEDA's requirement for organizations to implement security safeguards, including measures to protect personal information during maintenance.
   - Subpoint (d) stresses the need to sanitize equipment before removal from organizational facilities for off-site maintenance. This is essential for compliance with data security and privacy regulations like PIPEDA, which require organizations to protect personal data from unauthorized access.

2. **CM-2 Baseline Configuration**:

   Alignment with Regulations:

   - Maintaining a current baseline configuration is crucial for ensuring the integrity and security of personal information, as required by PIPEDA and PHIPA. Unauthorized changes to configurations can lead to data breaches or unauthorized access to sensitive information.

   Specifics:

   - Subpoint (a) emphasizes the need to document and maintain a current baseline configuration. This aligns with PIPEDA's requirement for organizations to implement safeguards to protect personal information and regularly review and update their security practices.
   - Subpoint (b) specifies circumstances under which the baseline configuration should be reviewed and updated. This aligns with regulatory requirements to adapt security measures as needed to protect personal information effectively.

3. **CA-8 Penetration Testing**:

Alignment with Regulations:

- PIPEDA, CASL, and other Canadian privacy and security regulations require organizations to assess and identify vulnerabilities in their systems to protect personal information and prevent data breaches.

Specifics:

- Penetration testing (as described in the control) helps identify vulnerabilities and weaknesses that could be exploited by adversaries, aligning with PIPEDA's requirement for organizations to take steps to protect personal information from unauthorized access or disclosure.
- The control also mentions the importance of penetration testing during technology transitions (e.g., IPv4 to IPv6), which can be relevant to PIPEDA's requirement for organizations to adapt their security measures to evolving technology.

4. **AC-2 Account Management**:

Alignment with Regulations:

- PIPEDA and other privacy regulations necessitate proper user access controls to protect personal information. Unauthorized access to personal data is a significant concern addressed by these regulations.

Specifics:

- Subpoint (a) aligns with PIPEDA's requirement for organizations to define and document types of accounts allowed and prohibited. This helps control access to personal information.
- Subpoint (f) emphasizes the need to create, enable, modify, disable, and remove accounts in accordance with established policies. This aligns with regulatory requirements for organizations to manage user access and privileges to protect personal data.

5. **AC-17 Remote Access**:

Alignment with Regulations:

- PIPEDA and other privacy regulations require organizations to secure remote access to protect personal information, especially in scenarios where remote work or access to systems from external locations is involved.

Specifics:

- Subpoint (a) emphasizes the need to establish and document usage restrictions and configuration/connection requirements for remote access. This aligns with the need to secure remote access to personal information as required by privacy regulations.
  - Subpoint (b) underscores the importance of authorizing each type of remote access to the system before allowing connections, which is essential for ensuring the security and confidentiality of personal data.

Infrastructure Services

Infrastructure	Role	Software	Software Version
External Router	External Router for providing a gateway to internal router	Ubuntu	Latest
Core Router	DHCP server Firewall	Iptables Isc-dhcp-server	Latest
Private DNS	Private DNS server	Pihole	Latest
Public DNS	Public DNS server	Pihole	Latest
Docker Host	Docker machine hosting containers	Docker Wordpress Apache2 Samba	Latest

Security Zones and Firewalls

Security Zones
DMZ
Management Zone
Internal zone
External Zone

DNS	
Public DNS	**External Zone, Management Zone**
Private DNS	**DMZ, Internal Zone**

Firewalls

DMZ

DMZ zone is going to be a zone that hosts services that are accessible from both internal and external networks.

Allow Inbound Web Traffic: Allow incoming traffic on port 80 (HTTP) and 443 (HTTPS) to your web server:

- Source: Any
- Destination: Webservers
- Port: 80, 443
- Action: Allow

DNS

Allow incoming DNS traffic (port 53) for DNS servers in the DMZ.

- Source: Any
- Destination: DNS Servers
- Port: 53
- Action: Allow

Management Zone

SSH

Allow SSH (port 22) access for administrators to manage network devices.

- Source: Admin IP
- Destination: Devices in Management Zone
- Port: 22
- Action: Allow

SNMP Access: Allow SNMP traffic for network monitoring:

- Source: Monitoring Server
- Destination: Devices in Management Zone
- Port: 161, 162
- Action: Allow

➢ Internal Zone

internal zone contains trusted resources and internal servers. It's important to limit access to only what's necessary.

Internal Server Access: Allow communication between internal servers.

- Source: Internal Ip Devices
- Destination: Internal Server Ip
- Port: Specific to your application
- Action: Allow

➢ External Zone

The external zone includes untrusted networks and the internet. You should have rules to protect your internal network from external threats.

Inbound Firewall Rules:
Webserver

- Source: Any
- Destination: DMZ Web Server
- Port: 80, 443
- Action: Allow

Outbound Firewall Rules:

In configuring outbound rules, the team's collective goal is to manage the traffic leaving their network. To enhance network security, we collaborate to restrict various forms of outbound traffic, ensuring that only essential communication is authorized.