Unit Details:

Unit Name: Secure Remote Access Networks
Unit Code: TNE30012
Lab Day and Time: Monday 11:30 AM session
Lecturer Name: Leo Ciavarella
Topic: Assignment - 2 (Security Policy Group Assignment)
Due: 29th Oct 2022 (5:30PM)
Submission: 19th Oct 2022 (8:02 AM)

Student Details:

Name	ID	Email
S M Ragib Rezwan	103172423	103172423@student.swin.edu.au
Jonathan Naumann	101615887	101615887@student.swin.edu.au
Dewmi Kuda Liyana Waduge	103491856	103491856@student.swin.edu.au
Pasan Sanjula Senanayake Senanayake Arachchige	103128866	103128866@student.swin.edu.au

Table of Content:

Introduction

ACME is a private company with two separate multi-tenant datacentres. The primary datacentre contains a series of servers to store data, run enterprise applications and company email while a separate series of public web servers are in a virtual server farm in a DMZ. The secondary datacentre is implemented to provide full redundancy.

The company is having issues in data access between the divisions, property management group and commercial real estate. They are also planning to lease another division for construction and implement wireless access across all the floors. Moreover, they are planning to configure minimal access for external stakeholders and are also concerned about staff using their company email for inappropriate things as well.

This document contains the general security policies that would assist ACME's intentions of being cyber security aware. In the first section of the document key security policies that can be formulated within this company have been identified. From the list, two in-depth security policies have been created for Wireless Communication and Server Security in the next section, followed by some Network Equipment Security Guidelines for the company.

Identification of potential Network Security Policies

ACME is a mid-level business where the staff is accessing service in a remote location (data centre) where many of their services and assets are held. Although ACME has full control over its own devices and infrastructure, there are still security vulnerabilities present in the organization (alongside the fact that their access control is unsupervised). This increases the chance of a security issue occurring in their system, leading to potential future compromises, which in turn can result in damage to the company, both in terms of finance and reputation. So, having a proper policy to dictate and maintain their network security is a must.

Further analysis of the ACME's business environment shows that the implementation of internal policies needs to be done as well, like setting up proper access control for its employees to access the organizational resources (like only letting the commercial real estate group access their own documents and not to other division's documents). Moreover, proper safeguards should also be put in place, in order to limit access to certain resources for external parties (like not letting contractors have full access to all documents in the company's server). After reviewing the business environment and infrastructure, the following network security policies were identified as necessary:

1. **Wireless Communication Policy**
   As many of the employees will use their own devices and will connect to the wireless access networks throughout the site, having proper communication policies in the organization is important. It will reflect on how the media is handled and how the systems are configured with the best practices according to the requirements. Furthermore, it is also in line with the growth objectives of the company and thus

would be extremely beneficial for the company to have, before setting up of the wireless infrastructure for their network

2. **Server Security Policy**

   ACME holds the servers in a separate shared data centre where they have control of their own servers but not the facility itself. Although increases the chance of issues like data breaches occurring (as the data storage facility is not their own), the company does not need to worry about that as it is the duty of the data storage facility's owner to maintain proper policy and security regarding that manner.

   But, it can also be seen that the company currently lacks any policies regarding the use and management of their server and the resources hosted on it, which they are fully responsible for. This can be clearly seen as all the general staff can currently access all the resources on the server without any restriction. Thus the organization must develop this policy.

3. **User Account Policy**

   As each employee needs to access to their own division resources only, they must have separate user accounts (setup using a carefully managed and well-structured Active Directory) in the organization. That's because this is used to determine whether the employee has authority to access a resource, and also what they can do with the resource itself. Furthermore, it can also be used to track the employees on their actions and also allow them to access their resources from any company device. This ensures that employees part if property management group has access to their resources only and not others and also ensures that they don't use company resources for their personal needs.

4. **System Policy**

   ACME has systems in both on-site and remote locations. So considering the possible intrusions and other disasters, having proper system configuration policies is a must. These can be anything like configuration of best practices, proper maintenance policies, etc. which must be followed at all times.

5. **Remote access Policies**

   ACME employees must have access to their remote servers (as it contains all the resources they need for their work), which can lead to vulnerabilities and threats if proper policies are not in use. Proper implementation of policies will ensure the best practices are followed.

6. **Credential Management Policy**

   Having proper passwords in user accounts is a must, especially in a company like ACME which has many remote connections (i.e. to their leased server racks). This not only ensures that the minimal characteristics are present in a given password (i. e: minimum length, use of upper and lower case, symbols and digits, etc.) and but also ensures proper expiration dates are set and followed, forcing the user to change their passwords in a timely manner.

7. **Data Retention Policy**

   The data retention policy outlines the kinds of data the company must keep and how long it must keep it. The policy specifies how the data is going to be kept and how it will be disposed of. By removing redundant and out-of-date data (like documents, customer records, transactional data, email messages, contracts, etc.), this policy will free up more storage space for the company.

   Furthermore, it will not only ensure that the company focuses on the confidentiality and integrity of the data stored by it but will also assist it in future data organization aspects. So, for a company like ACME which contains business sensitive information (like details of customers seeking property and real estate), this policy is absolutely crucial. Hence the organizations' requirements for data retention should be based on regulatory standards.

8. **Incident Response Policy**

   The business continuity plan of an organization includes the incident response policy. It describes a company's response to a data security incident. Given that it focuses on procedures to be followed in the event of any security incident (like a data breach, loss of access, etc.), the incident response policy should be documented properly and kept separate from the disaster recovery plan. ACME holds information not only about itself but also about various third parties (like vendors, contractors, etc.) associated with it. Hence, having proper incident response policy will ensure all the proper procedures are followed during an incident.

9. **Security Awareness and Training Policy**

   All employees should receive security awareness training so that they can effectively carry out their duties and properly protect the corporate information of the company (like know what to and not to access when browsing online). When they have finished the training, the employees must be required to sign a confidentiality agreement and present proof of its completion. The training program should be created by the management group in the company with the goal of educating users about the company's security policy.

10. **Acceptable Use Policy**

    The acceptable use of computer equipment is described in the Acceptable Use Policy (AUP). In the normal course of business, it is used to serve the interests of the organization, clients, and customers. The inappropriate use of information systems and the risk it poses are both defined in the AUP. The network system could be compromised by improper behavior, which could also have legal repercussions. For instance, an employee using the company’s computer to access information for any purpose other than performing his or her duties is an example of inappropriate use. The AUP covers acceptable behavior both in handling confidential or proprietary information and also in general use and hence is a must have for the company.

Detailed Security Policy:
Part A: Wireless Communication Policy:

Here a detailed Network Security Policy regarding Wireless Communication Policy has been produced using the Free to Use SANS Template **[1]** as a basis (alongside the wireless communication policies of "College of Saint Mary" **[2]** and "William and Mary" **[3]**), in order to craft a suitable and robust policy for ACME.

1. Overview

Nowadays, there has been a huge increase in the number of smartphones and tablets used by people, leading to almost all companies allowing their employees to access company resources on their own device via BYOD (Bring your own device). This in turn has led to an increase in work efficiency and effectiveness as now employees had flexibility in the way they could access company resources (i.e. they can move around the building and still access resources from anywhere without losing connection to company network).

Thus, ACME deciding to provide wireless access is quite a good initiative in terms of future growth. But considering the dangers that insecure wireless configurations provide (alongside the fact that this is the company's first setup of wireless access), the desire and necessity for a strong and effective wireless communication policy for the company is also quite high.

2. Purpose

This policy has been made to secure and protect the information assets owned by ACME by establishing rules and procedures regarding wireless access to company resources. This ensures that personnel can only gain access to those resources if either:

1. Their wireless communication devices satisfy the specified standards and protocols,

2. They have been granted an exception by the Information Security Department

Furthermore, it also ensures that the Confidentiality, Integrity and Availability (CIA) of the informational assets in the organization are properly maintained.

3. Scope

All personnel affiliated with ACME (like employees from property management, commercial group or future construction group, contractors, consultants, etc.) and any third party or vendors related to ACME using any wireless communication device

(like mobile phones, computers, PDA, etc.) must adhere to this policy. This includes any wireless communication device that is capable of transmitting data and is either connected to or resides on the companies' wireless network.

4. Policy

All personnel using wireless devices that are either located at ACME, connecting to ACME network, or accessing resources over the company's network must:

- Follow the standards specified in wireless communication Standard,
- Use company approved authentication (Radius, Tacacs+, etc.) and encryption protocol (SHA, MD5, etc.),
- Use company approved infrastructure that are installed, supported and maintained by an approved support team,
- Maintain hardware access (MAC address) that can be tracked,
- Not interfere with other Organizations' wireless infrastructure,
- Not access or download harmful or suspicious websites or content from the internet whilst using the company network,
- Not share their access with any other personnel within or outside their company,
- Not impact the CIA of the information assets of the company they are accessing in any way.

Furthermore, ACME's extremely sensitive and confidential information that is not necessary for daily business activity (like DMZ or virtual server setup) must be isolated from the corporate network and comply with *Lab Security Policy*.

Moreover, the SSID set for the network must not have any information of the company in it (like name, division, id, etc.) and must use proper, complex passwords (like combination of uppercase and lowercase letters, numbers, symbols, etc.)

5. Policy Compliance

Authorized personnel from the ACME Company (members of their Information Security Team) will periodically verify that compliance to the policy has been maintained via video monitoring, reports, audits, etc. Any employee found to have violated this policy at any time, without having explicit approval from the authorized personnel for the exception, will be subject to serious disciplinary actions, up to and including termination of employment.

6 Related Standards, Policies and Processes

- Lab Security Policy
- Wireless Communication Standard

7 Definitions and Terms

Term	Definition
BYOD	It is the practice of allowing the employees of an organization to use their own devices for work purposes
CIA	It is a model designed to guide policies for information security within an organization, ensuring that the Confidentiality, Integrity and Availability of the information asset is maintained
PDA	It is a type of mobile device also known as a handheld PC
Radius	It is a client-server protocol that enables remote access servers, used to authenticate users
Tacacs+	It is a remote authentication protocol developed by Cisco
SHA	It is an algorithm used to create hashes files
MD5	It is a message digest algorithm that had been initially used to create hashes of files
MAC Address	It is a unique hardware identifier that helps identify any device on a network
DMZ	It is called as demilitarized zone and is basically a sub network that is used to protect an organizations' exposed outwards facing service
SSID	It is called Service Set IDentifier and is basically the name of the network

8 Revision History

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Updated and converted to

		new format
October 2022	S M Ragib Rezwan	Updated and modified the format to be more applicable/ suitable to ACME

Part B: Server Security Policy:

Here, detailed Network Security Policy regarding Server Security for ACME has been built using the Free to Use SANS Template **[4]** and Tarala **[5]** as reference.

1. Overview

At present, there are numerous cyber-attacks designed to target the servers on the internet, leading to vulnerable servers becoming a major entry point for almost all malicious threats. Therefore, protecting data and resources stored in servers is an important aspect that must be prioritized by every organization.

ACME uses servers to store data, run enterprise applications and organization email and also a series of public web servers in a virtual server farm in a DMZ along with redundant servers. Moreover, ACME servers can be considered as highly vulnerable to attacks due to poor access control to the servers. Hence, establishing a server security policy is worthwhile.

2. Purpose

The purpose of Server Security Policy is to outline control standards that ACME will follow regarding server access and data protection. These standards are intended to establish minimal access to the company servers, restrict unauthorized access to confidential and sensitive data (in order to protect them from being compromised) and ensure that the staff can access data as required for them to work efficiently.

3. Scope

All ACME employees from the property management group, commercial real estate group, contractors, salespeople and other workers at ACME and its subsidiaries must adhere to this policy. This policy applies to server equipment that is owned, operated or leased by ACME or registered under the ACME owned internal network domain.

4. Policy

General requirements

- Server information must be registered with ACME enterprise management system and should be on up to date in order to positively identify as a point of contact such as,
    - Server contacts, location and backup contact,
    - Hardware and Operating System Version,
    - Main functions and applications.
- For security, compliance and maintenance purposes, authorized personnel should monitor and audit systems and processes,
- Organization's computer users shall be educated on data and system risks,
- Backup of each system shall be performed on a daily basis,
- A detailed disaster recovery plan should be implemented, tested and maintained.

Configuration requirements

- Each of these servers shall have appropriate file and network-based access control lists configured and server access attempts should be logged,
- Applications and services that will not be used should be disabled where appropriate,
- User access shall be granted based on the principle of least privilege only on authorized user accounts,
- Inactive user accounts shall be removed,
- Only authorized running services and listening network posts will be inventoried,
- Remote server administration and access shall be performed over encrypted channels,
- Recent security patches must be installed,

Monitoring

- Access control methods such as an application firewall will be installed in front of all critical servers for monitoring and logging critical events and to generate alerts,
- All security-related events on all critical or sensitive systems shall be logged, audit trials shall be saved and backup of logs will be retained for a minimum of 2 years,
- Vulnerability scans shall be performed on a regular basis and corrective measures will be prescribed as needed.

5. Policy Compliance:

Authorized personnel from ACME will verify compliance to this policy not being limited to internal and external audits, periodic walk-throughs, business tool reports and video monitoring. Any personnel under ACME violating this policy shall be subjected to disciplinary action and even may cause termination of employment.

6. Related Standards, Policies and Processes:

- Audit Policy
- DMZ Equipment Policy

7. Definitions and Terms:

Term	Definition
DMZ	Demilitarized Zone, which separated a network from other untrusted networks

8. Revision History:

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Updated and converted to new format
October 2022	Dewmi Kuda Liyana Waduge	Updated to suit ACME

Network Equipment Security Guidelines

Network equipment is basically anything that can be used to combine, split, switch, boost, or direct packets of information along a computer or telecommunications network **[6]**. This can be anything like hubs and switches, routers and gateways, multiplexers, etc. So, any guidelines referring to the proper and secure use of that equipment (like "good practices") are known as Network Equipment Security Guidelines.

In ACME, this is extremely important! This is because it has both remote and local networks directly linked together; with various equipment (like switches, routers, etc.) and services (like ftp, web, etc.) present in it. Therefore, it should follow the Network Equipment Security Guidelines in order to ensure that the configuration and management of the equipment are done while following both these best practices and also the corporation's policies.

The following are best practice guidelines that are suggested for the network equipment used by ACME:

[Note: *Here information from National Security Agency**[7]**, Netwrix **[8]** and NIST**[9]** have been utilized in order to note down the best practices that are most suitable for the ACME* **]**

- The physical security of all devices should be maintained, and only authorized personnel should have physical access to them. Keeping routers switches and other devices in a secure room is advised to achieve this physical security,

- Maintaining the most current stable version of all network device operating systems is critical to ensure the latest updates are being used. Before implementing an update, it should be tested in a simulated environment to ensure stability,

- Hardening of each network device can greatly increase the security, prioritizing the disabling of unused interfaces, and ports. Port security should be enabled and any unused interfaces, routing protocols, and ports should be disabled/shutdown. Any IP directed-broadcast and IP proxy-arp should be disabled as well,

- Continuing with hardening, default services can be exploited by attackers and should be managed. Research should be done on the specific devices' default services and decisions should be made on whether they should be disabled

or not. For instance, NSA **[7]** recommend the following should be considered to harden the device to service threats:

- **Services to Enable**
  - SSHv3 or TLS: secure communication to remote devices is done through these protocols,
- **Services to Disable**
  - Echo Protocol: this protocol measures a packet's round-trip time, this is a legacy service,
  - Chargen Protocol: this service tests, debugs, and measures the connection, this is a legacy service,
  - Discard Protocol: this protocol discards packets, this is a legacy service,
  - Daytime Protocols: this protocol displays the current date and time,
  - FTP Protocol: this allows the copying of files between systems in the network,
  - Telnet: this is a clear text protocol; it is used to communicate with other devices in the network,
  - BootP Service: this service assigns IP addresses to devices, this is a legacy service,
  - HTTP Server: this web service is generally enabled on network devices,
  - SNMP Protocol: this protocol manages network devices,
  - Discovery Protocols: this service shares information with other devices,
  - IP Source Routing: this gives the sender control of the route of information,
  - IP Unreachable: this can allow the network to be mapped by ICMP (Internet Control Message Protocol) messages,

    - IP Mask Reply: This responds to ICMP mask requests with network information,
    - Zero Touch Provisioning: this allows devices to download firmware and configurations on their own,

- The configuration files of all devices should be backed up and securely stored offline (air gapped). These files should never be shared by any unsecured means, as access to these files could help attacker find vulnerability,
- Ensure that power supplies to devices are protected. Using uninterruptible power supplies can ensure that your devices cope better with power disruptions, and backup generators can provide better coverage. These devices should be checked and replaced following the manufacturers recommendations,
- Starting at a personal device level, software-based firewalls should be installed on any device that will connect to the network. Personal firewalls protect from internal attacks, these can be configured and exported to each device.

Conclusion

In this document, we have identified the potential Network Security Policies by taking the organizational assets and their implementation into consideration. As wireless communication and servers were recognized as important areas where policies needed to be formulated, detailed security policies have been developed for Wireless Communication and Server Security. By implementing these formulated network security policies and following the suggested network equipment guidelines, ACME will be able to better protect themselves from the current cyber threats.

Reference

[1] SANS Consensus Policy Resource Community, "*Wireless Communication Policy.*" SANS Institute 2014. https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blte0e352dc1934ea5f/5e9dfb76d5a1cb709eee4a6e/wireless_communication_policy.pdf (accessed Oct 3rd, 2022).

[2] College of Saint Mary, "*CSM Wireless Policy*." College of Saint Mary. https://www.csm.edu/sites/default/files/Wireless%20Policy.pdf (accessed Oct 3rd, 2022).

[3] William and Mary, "*Wireless Communications Policy and Procedures*." William and Mary. https://www.wm.edu/offices/compliance/policies/wireless_communications/index.php (accessed Oct 3rd, 2022).

[4] SANS Consensus Policy Resource Community, "*Server Security Policy.*" SANS Institute 2014. https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt50e440e7b0db16c9/5e9dfee150e659126c8d77d5/server_security_policy.pdf (accessed Oct 3rd, 2022).

[5] Kelli K. Tarala, "*Server Security Policy.*" AuditScripts. https://www.auditscripts.com/samples/server-security-policy.pdf (accessed Oct 3rd, 2022).

[6] Global Spec Engineering 360, "*Learn More About Network Equipment.*" Global Spec. https://www.globalspec.com/learnmore/networking_communication_equipment/networking_equipment/networking_equipment (accessed Oct 15th, 2022)

[7] National Security Agency, "*Hardening Network Devices.*" National Security Agency Defence. https://media.defense.gov/2020/Aug/18/2002479461/-1/-1/0/HARDENING_NETWORK_DEVICES.PDF (accessed 12th Oct)

[8] Netwrix, "*Network Security Best Practices.*" Netwrix. https://www.netwrix.com/network_security_best_practices.html (accessed Oct 12th, 2022)

[9] Traci Spencer, "*How to Protect Your Business from Cyber Attacks.*" NIST. https://www.nist.gov/blogs/manufacturing-innovation-blog/how-protect-your-business-cyber-attacks (accessed Oct 12th, 2022)