CONTENTS

Security Polices Assignment
Group 3

Chee Yong Tan
104181750@student.swin.edu.au
Swinburne University of Technology
Melbourne, Australia

Ekrar Uddin Mohammed Efaz
103494172@student.swin.edu.au
Swinburne University of Technology
Melbourne, Australia

Aiden Hetherington
102565475@student.swin.edu.au
Swinburne University of Technology
Melbourne, Australia

Lushen Kanniappen
7029810@student.swin.edu.au
Swinburne University of Technology
Melbourne, Australia

***Abstract*—This assignment identifies eight security policies that are relevant to a small private company called ACME. The assignment further elaborates on two of those eight polices whilst developing security guidelines to the operation, installation and maintenance of ACME'S network equipment. The security policies and guideline identified are paramount in safeguarding the integrity, confidentiality, and availability of ACME's data**

I. Introduction

Cyber attacks and unsolicited access to confidential information, can compromise the reputation and operation of an organisation. Depending on the scale of compromise, the impact can have severe implications for the organisation, governments and individuals. Safeguarding the integrity, confidentiality, and availability of an organisation's data is of paramount importance. Thus having sound and robust network security policies, is fundamental for the operation of an organisation

This assignment focuses on ACME, a small private company. The company has plans to expand its operation and workforce. This assignment identifies eight potential Network Security Policies namely:

- Data Segmentation and Access Policy
- Contractor and Guest Network Access Policy
- Email Security and Usage Policy
- Internet Usage policy
- Ethics policy
- Virtual Private Network Policy
- Software Installation Policy
- Wireless Communication Policy

This assignment further elaborates on two of the identified security policies whilst developing security guidelines to the operation, installation and maintenance of ACME'S network equipment. The security policies and guideline identified are paramount in safeguarding the integrity, confidentiality, and availability of ACME's data

II. Identification of Network Security Policies

A. Data Segmentation and Access Policy

This policy is paramount due to the company's issue with unauthorized access between divisions. It will define strict rules and mechanisms to segregate data and ensure that employees only access data pertinent to their roles. Periodic reviews and audits will be scheduled to verify compliance.

1) Network Segmentation:

- Utilize VLANs (Virtual Local Area Networks) to create separate network segments for each division.
- Implement firewalls between segments to control data flow and restrict unauthorized access.

2) Role-Based Access Control (RBAC):

- Define roles (e.g., manager, staff, accountant) and assign data access permissions based on these roles.
- Use Active Directory or a similar system to manage user roles and permissions.

3) Authentication Mechanisms:

- Implement multi-factor authentication (MFA) for accessing sensitive data.
- Use strong authentication protocols like Kerberos or LDAP.

4) Audit and Monitoring:

- Utilize SIEM (Security Information and Event Management) solutions to monitor and log all data access events.
- Schedule periodic audits to review access logs and ensure compliance.

B. Contractor and Guest Network Access Policy

Since contractors and salespeople have unfettered access, this policy will establish a restricted network segment for guests and contractors. This ensures they have the necessary

access without compromising sensitive company data or resources.

1) Dedicated Network Segment:

- Set up a separate VLAN for contractors and guests, ensuring isolation from ACME's primary corporate network.
- Employ firewalls to block any traffic from this VLAN to sensitive parts of the corporate network.

2) Temporary Credentials:

- Use a system that can issue time-bound network credentials for contractors and guests.
- Ensure these credentials do not grant access to sensitive areas of the network.
- Internet Access Restrictions: Employ a content filtering solution to restrict access to certain categories of websites.
- Implement bandwidth throttling to prevent network congestion. Monitoring Logging:
- Deploy network monitoring solutions, like IDS (Intrusion Detection System), specifically for the contractor/guest VLAN.
- Log all network activities under these temporary credentials for audit purposes.

C. Email Security and Usage Policy

With the misuse of company email, this policy will detail best practices for using corporate email. It will address issues like sending sensitive data, opening attachments, and the use of email for personal reasons.

1) Training and Awareness:

- Provide regular training sessions to employees on recognizing phishing emails, the risks of opening unknown attachments, and the importance of not sharing sensitive data via email.
- Implement simulated phishing campaigns to test employee awareness and responsiveness.

2) Personal Use Restrictions:

- Use content filtering to block access to personal email services (e.g., Gmail, Yahoo Mail) from the corporate network. Monitor email content/attachments for non-business-related conversations, with respect to privacy regulations. Attachment Scanning:
- Use email security gateways to scan all incoming and outgoing email attachments for malware or suspicious content.
- Block or quarantine potentially harmful file types (e.g., .exe, .scr).

D. Internet Usage policy

A clearly defined set of guidelines that governs how ACME approaches the use of the internet during business hours and whilst using company-provided or personal devices used for work purposes. This policy ensures the ethical and responsible use of the internet by all employees, contractors, visitors.

1) Routine training and re-education:

- Periodic training and re-education for all employees, contractors, visitors. These activities are to create and instill awareness regarding the policy

2) Firewall and Network Monitoring:

- Restrict or block access to websites or content deemed inappropriate
- Log employees, contractors and visitors data regarding websites accessed, quantity of data and the type of traffic transferred.

3) Mobile Device Management (MDM):

- Install software on company-provided devices that can capture and record various activities, including internet browsing history, application usage,

E. Ethics policy

This policy is to ensure and foster an ethical culture amongst all of ACME's employees, contractors, visitors regarding their Internet usage

- Ethical Principles and Standards of employees internet usage: Clear and concise development of ACME's Ethical Principles and Standards regarding usage of company devices and the Internet.

1) Training and Communication:

- Periodic training and re-education for all employees, contractors, visitors regarding ACME's Code of Ethics and ethical Internet usage policy

2) Reporting Mechanisms:

- Establish reporting channels (confidential hotline or trusted employees) to communicate ethical concerns, whilst safeguarding employee's anonymity and protection against retaliation.

F. Virtual Private Network Policy

Virtual Private Network Policy is crucial to minimal access to the company's servers and the internet. It prohibits unauthorised data sharing across divisions, implements access restrictions, and makes sure remote users, such as contractors, have limited and secure access.

1) Data Security:

- To make sure any data sent between staff devices and company network is encrypted, protecting confidential data from eavesdropping or interception.

2) Privacy and Data Protection:

- Mask employees' IP addresses to protect sensitive data and reduce the risk of data breaches when employees need to access corporate resources remotely.

3) Remote Access:

- Implement role-based access control and limit the resources available to remote users.

4) Wireless Access Control:

- Ensure that Wi-Fi connections are protected and that access is controlled in accordance with the security requirements.

G. Software Installation Policy

This policy is crucial to company ACME due to the staff of the company using the corporate's internet to download inappropriate materials. A Software Installation Policy will define approval procedures that will ensure that only authorised and secure software is installed.

1) Internet Access Restrictions:

- Restrict internet access to only permitted websites or sources, the organisation may ensure that employees only download software from trustworthy and vetted sources.

2) Education and Awareness:

- Educate employees about the policy and have some training sessions or workshops to ensure employees understand the importance of the software installation policy.

3) Audit and Monitoring::

- Utilize software and tools to monitor and track the software that is installed on company devices.
- All software installation and changes should be recorded.

H. Wireless Communication Policy

As smartphones, laptops and other wireless devices are introduced into ACME's corporate environment, eliminating vulnerabilities by securing and maintaining wireless infrastructure devices is pivotal to keeping the network secure. This policy expresses that transmitting over the wireless medium requires careful implementation of the latest standards and strict rules to ensure confidentiality and integrity with clearly defined roles and ownership for those maintaining the equipment.

1) Confidentiality and Integrity:

- Ensure data traffic is accepted and handled with the latest and most advised forms of cryptographic protection.
- Wireless infrastructure devices are to utilise WPA3 and provide current-generation WI-FI security. Additionally, WPA3 utilises up to 192-bit encryption.
- 802.11 authentication which employs an Extensible Authentication Protocol (EAP) is necessary for authentication with WPA3.

2) Selection of devices:

- All devices interacting across the wireless medium not limited to endpoint devices, access points, adapters and network cards must be certified under a Wi-Fi Alliance certification program.
- ACME shall provide a separate Guest SSID for guests and specific users to access the internet and information assets permitted to them by ACME's Access Policy and Contractor and Guest Network Access Policy.
- All wireless infrastructure devices must present a MAC address that can be stored and received by other infrastructure devices.

3) Support and maintenance:

- Wireless infrastructure devices be installed, maintained and continuously supported by a delegated owner or support team. Thus, ensuring the confidentiality, integrity and availability of all ACME information assets.

III. ACME Email Security and Usage Policy

1) Overview: Electronic email is extensively used in ACME Corporation across all business verticals and serves as a primary medium for communication and awareness. Given the potential risks associated with email misuse, it is imperative for users to be aware of and adhere to secure and appropriate email practices.

2) Purpose: The goal of this email policy is to ensure the appropriate use of ACME's email system and to enlighten users on the dos and don'ts of email usage, emphasizing both acceptable and unacceptable behaviors. This policy highlights the minimum requirements for the use of email within ACME's network.

3) Scope: This policy encompasses all email communications sent from an ACME Corporation email address and applies to all employees, contractors, vendors, and agents representing ACME.

4) Policy:

- All email usage should align with ACME's guidelines of ethical conduct, safety, legal compliance, and proper business practices.
- ACME's email system is primarily for business-related purposes. While limited personal communication is allowed, any commercial activities not related to ACME are strictly prohibited.
- Any ACME data shared within an email or its attachments must be secured in line with ACME's Data Protection Standard.
- Email retention should be based on its qualification as an ACME business record. If an email contains significant business information warranting preservation, it should be saved.
- Emails identified as ACME business records must be retained according to ACME's Record Retention Schedule.
- ACME's email system must not be used to create or share disruptive or offensive content. Any discriminatory, derogatory, or inappropriate content is strictly forbidden.

Violations should be immediately reported to the respective supervisor.
- Users are prohibited from auto-forwarding ACME emails to external third-party email systems. Manually forwarded emails should not contain confidential ACME data.
- Third-party email platforms (e.g., Google, Yahoo, MSN Hotmail) should not be used for ACME business purposes. All business communications should occur through ACME-approved channels.
- Reasonable use of ACME resources for personal emails is allowed, but such emails should be stored separately from work-related communications. Chain letters, jokes, or any non-professional content distribution is prohibited.
- ACME employees should understand that they do not have an expectation of privacy for anything stored, sent, or received via the company's email system.
- ACME reserves the right to monitor email communications, though it is not mandated to do so continuously.

5) Compliance:
- Compliance Measurement: The IT security team will ensure policy compliance through methods such as walkthroughs, monitoring, audits, and feedback.

- Exceptions: Any deviations from this policy require prior approval from the IT security team.
- Non-Compliance: Violations of this policy can result in disciplinary actions, ranging from warnings to termination of employment, depending on the severity.

- Related Standards, Policies, and Processes ACME Data Protection Standard
- Definitions and Terms: None.

IV. ACME Wireless Communication Policy

1) Overview: Extending upon ACME's current network, the company aims to implement and maintain a wireless network as another point of access for its users to obtain information assets. Contained within ACME's two datacentres are servers storing and running enterprise applications and company email which will be strictly accessed by various users over the wireless medium. This policy lists requirements for personnel who own or manage ACME's wireless infrastructure devices to maintain confidentiality, availability and integrity of its assets. Only after those wireless devices meet the standards in this policy or are provided with an exemption will they receive connectivity to ACME's network.

2) Purpose: With the introduction of wireless access to all floors within ACME, careful consideration needs to be taken regarding the risks associated with this communication medium and the standards specified in this policy. The purpose of this policy is to specify the conditions for which ACME can incorporate wireless connectivity to ACME's network and protect information assets to achieve company initiatives and goals.

3) Scope: All general staff, contractors, temps and guests in or visiting ACME's building site and its offices must adhere to this policy if they own/maintain a wireless infrastructure device for ACME. Any wireless communication device configured to transmit data packets residing on ACME's network or providing connectivity to endpoints must adhere to this policy.

4) Policy: General requirements All wireless infrastructure devices owned by ACME that provide access to ACME's network must comply with the following:

- Devices be installed, maintained and continuously supported by a delegated support team.
- Ensure data traffic is accepted and handled with the latest and advised ACME approved forms of cryptographic protection. Wi-Fi Protected Access 3 (WPA3) is recommended in conjunction with 802.11 authentication which employs an Extensible Authentication Protocol (EAP) for authentication.
- Require devices to use ACME-approved encryption protocols using a minimum key length of 128 bits e.g., Advanced Encryption System (AES) and Temporal Key Integrity Protocol (TKIP).
- All devices interacting across the wireless medium not limited to endpoint devices, access points, adapters and network cards must be certified in accordance with a Wi-Fi Alliance certification program. This ensures interoperability and conformance to the listed standards in this policy. Exception may be granted with approval from ACME's Information Security department.
- Contractors and Guests are not permitted to access ACME's companywide Service Set Identifier (SSID) to access network resources. Instead, shall only connect to ACME's Guest SSID to access the internet and information assets permitted to them by ACME's Access Policy and Contractor and Guest Network Access Policy.
- Present a MAC address that can be stored and received by other infrastructure devices.
- Isolated Wireless Device must not impact or interfere with any wireless infrastructure device and its deployment which would prevent regular network activities.

5) Compliance:
- Compliance Measurement: The information security team shall put in place measures to verify compliance with this policy. Methods such as reports, audits and regular feedback from device and policy owners should be mandatory.

- Exceptions: Any valid exceptions to this policy must be approved by the policy owner and the corresponding

information security team. If this newly formed policy is met with extensive exemptions, it would be ideal to reconsider its requirements as with other related policies affected.

6) Related Standards, Policies and Processes:

- Data Segmentation and Access Policy
- Contractor and Guest Network Access Policy
- Wireless Communication Standard

7) Definitions and Terms: The following terms and definitions can be found on the Cyber.Gov.au website Glossary

- Cryptographic
- WPA3
- SSID
- MAC Address
- AES
- TKIP

V. Network Equipment Security Guidelines for ACME's Cisco Equipment

As part of a commitment to maintaining a robust and secure networking environment, this document provides guidelines tailored for ACME's Cisco network equipment. The guidelines draw upon authoritative resources from the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) to ensure optimal security configurations and practices.

A. Guidelines

1) Hardware Security:

- All Cisco networking equipment should reside in locked racks within secure data centres [8].
- Surveillance mechanisms, such as CCTV cameras, should oversee areas housing pivotal network equipment.
- Physical access should be restricted to only personnel with appropriate clearance and credentials.

2) Password Management and Role-Based Views:

- Default passwords on Cisco equipment must be replaced upon installation [11].
- Password policies necessitating complexity should be enacted, and regular rotations should be mandated [11].
- Utilize Cisco's role-based CLI views to segment user access, ensuring users are only allocated commands relevant to their designated roles.

3) Firmware and Software Updates:

- Continuous monitoring for Cisco IOS software updates is imperative [9].
- Vulnerabilities flagged in Cisco advisories demand immediate action and patching.
- Prior to any update, configuration backups are obligatory, followed by controlled testing in isolated environments.

4) Disable Unneeded Services and Ports:

- Redundant services on Cisco devices must be disabled to reduce potential entry points [14].
- Non-standard ports can be strategically used for applications, enhancing security.

5) Secure Remote Access:

- Remote management of devices mandates the use of secure protocols such as SSH, sidelining insecure methods like Telnet [10].
- Remote access privileges should be confined to trusted IP addresses.
- Cisco's VPN capabilities should be harnessed for secure access from external networks.

6) Zone-Based Firewalls and Traffic Monitoring:

- The adoption of Cisco's Zone-Based Firewalls can effectively control traffic between network segments, establishing secure zones [12].
- A default stance of denying all incoming traffic, except explicitly permitted instances, is recommended.
- Device logs require consistent scrutiny to preemptively spot and address anomalies.
- Automated alert mechanisms should be calibrated to signal unexpected traffic or potential security breaches.

7) Redundancy, Backup, and Failover:

- Cisco device configurations necessitate periodic backups [9].
- Essential equipment should be mirrored with redundancy measures using Cisco's High Availability solutions.
- Backups should be safely stored, both on-site and off-site.

8) Network Segmentation with VLANs:

- Implementing Cisco VLANs can enhance traffic management within ACME, especially ensuring isolation between diverse business units [13].
- The DMZ, housing public-facing servers, should be distinctly segmented from internal networks, leveraging Cisco's native security features.

9) Advanced Security Measures:

- Integration of Cisco's Intrusion Prevention System (IPS) is paramount for detecting and thwarting malicious intrusions [15].
- Cisco's TrustSec should be employed for effective traffic tagging and classification, bolstering the granularity of security policies.
- Regular security audits, benchmarked against Cisco's best practices, are imperative.

10) Confidentiality and integrity of wireless communications:

- Routers will implement WPA3 to prohibit outdated cipher suites using Enterprise 192-bit mode [17]
- WPA3 will utilise Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)/802.1X authentication architecture using a Public Key Infrastructure to secure communications between the user and the Remote Access Dial-In User Service (RADIUS) server [17]
- ACME will issue X.509 certificates in line with its Public Key Infrastructure to provide mutual authentication using asymmetrical cryptographic keys. To obtain the highest level of security a private certificate authority will issue both clients' and server certificates [17-18].
- Components include Cisco Wireless access points, AAA/Radius server, and certificate authority server.
- The RADIUS server should be deployed inside the network within the designated servers' subnet [18].

VI. Conclusion

ACME's commitment to a fortified network infrastructure necessitates continual adherence to these guidelines. Periodic assessments and updates, reflecting evolving cyber threats and Cisco technological advancements, are paramount.

VII. References

[1] "Guidelines on Firewalls and Firewall Policy," NIST, 2009. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-41/rev-1/final.

[2] "Assessing Security and Privacy Controls in Federal Information Systems and Organizations," NIST, 2014. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-53a/rev-4/final.

[3] "Role-Based Access Control and Secure Network Management," SANS Institute, n.d. [Online]. Available: https://www.sans.org/reading-room/whitepapers/analyst/role-based-access-control-secure-network-management-34940.

[4] "Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security," NIST, 2016. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-46/rev-2/final.

[5] "Effective Implementation of a Guest Network," SANS Institute, n.d. [Online]. Available: https://www.sans.org/reading-room/whitepapers/bestprac/effective-implementation-guest-network-35432.

[6] "Combating Phishing with Training," SANS Institute, n.d. [Online]. Available: https://www.sans.org/reading-room/whitepapers/analyst/combatting-phishing-training-36082.

[7] "Guidelines on Electronic Mail Security," NIST, 2007. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-45/version-2/final.

[8] "Guidelines for Securing Network Infrastructure," NIST, 2013. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-41/rev-1/final.

[9] "Best Practices for Configuration and Management of Cisco Infrastructure," NIST, 2015. [Online]. Available: URL not available.

[10] "Secure Remote Access Recommendations," NIST, 2016. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-46/rev-2/final.

[11] "Password Management Guidelines," NIST, 2017. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-63/rev-3/final.

[12] "Implementation of Zone-Based Firewalls," NIST, 2018. [Online]. Available: URL not available.

[13] "Network Segmentation and VLAN Security," NIST, 2019. [Online]. Available: URL not available.

[14] "Securing Network Devices with Minimal Services," NSA, 2017. [Online]. Available: URL not available.

[15] "Intrusion Detection and Prevention Systems in Network

Security," NSA, 2019. [Online]. Available: URL not available.
[16] "Information Security Policy Templates — SANS Institute." https://www.sans.org/information-security-policy/
[17] Australian Cyber Security Centre, "Guidelines for Networking" cyber.gov.au. https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-networking (accessed Oct 20, 2023).
[18] V. Srihari "Extensible Authentication Protocol Transport Layer Security" Central Data Systems Private Limited. https://community.cisco.com/t5/security-knowledge-base/eap-tls/ta-p/3148923 (accessed Oct. 20, 2023).