C844 – EMERGING TECHNOLOGIES IN CYBERSECURITY

TASK 2: WLAN AND MOBILE SECURITY PLAN

By Kershia Mukoro Shin

SCENARIO SUMMARY

Alliah Company is a fast-growing social media provider for young professionals. One year ago, they launched a website and mobile app, funding it mainly through crowdfunding. The team operates from a three-story, 10,000-square-foot converted warehouse, with 35 employees using two floors and a third available for expansion.

The network includes a gigabit managed switch, a wireless LAN controller, seven well-placed wireless access points (APs), one covering an outdoor patio, and firewall protection. The LAN controller is the single management point for the wireless LAN deployment.

Five account representatives travel frequently, using company-issued laptops, tablets, and smartphones. They work from a shared office when onsite. To cut launch costs, Alliah implemented a bring-your-own-device (BYOD) policy. The IT team, consisting of five members, splits their time between website maintenance and network management. The growing success of their website has driven CEO Jennifer to prepare for rapid expansion. She wants to understand the security risks better, secure the network, consider the BYOD policy's impact, and explore whether to restrict access to company-owned devices or adopt a balanced approach.

1. WLAN Vulnerabilities

1. **Centralized Management Vulnerability:** A single wireless LAN controller manages the entire network, and Alliah's network faces a potential single point of failure. If the controller is compromised, it could disable access to or allow unauthorized control over all connected access points (APs), posing a significant security risk.

2. **Insufficient Security for Outdoor Access Point:** The outdoor access point, intended for employee use on the patio, could expose the network to unauthorized access outside the building's controlled environment. This vulnerability becomes more significant without network segmentation or additional access restrictions for areas outside the physical office.

2. Mobile Vulnerabilities

1. **Device Security in Transit:** The frequent travel of account representatives increases the risk of device theft or loss, which could lead to the exposure of corporate data stored on company-issued laptops, tablets, or smartphones. Without robust device security protocols, including encryption and remote wipe capabilities, any compromised device could provide an entry point into the company network.

2. **BYOD Policy Risks:** The existing BYOD policy increases the network's vulnerability to malware or unauthorized access, especially if employees' personal devices are not consistently monitored or updated. Open access to the network from unmanaged devices heightens the risk of data breaches because personal devices may lack the level of security of company-issued equipment.

3. Mitigation Steps for Identified Vulnerabilities

WLAN

1. Centralized Management Vulnerability Mitigation

Implement Redundancy for the WLAN Controller: Add a secondary wireless LAN controller to provide failover support, ensuring the network remains operational if the primary controller fails or is compromised. (Cisco. 2021)

- The Federal Information Security Modernization Act (FISMA) requires federal agencies to implement information security programs, including ensuring the availability of systems (NIST, 2020).

Enable Access Control and Monitoring: Use access control lists (ACLs) and logging to limit who can access the WLAN controller and monitor for unusual activities.

- The Sarbanes-Oxley Act (SOX) Section 404 requires public companies to establish internal controls for financial reporting, which includes IT systems access controls (SEC, 2002).

Tools/Documentation: Document redundancy and access control policies and implement monitoring tools for continuous visibility into the controller's status and access points.

2. Insufficient Security for Outdoor Access Point Mitigation

Limit Access Point Signal Range: Configure the outdoor access point to minimize its range beyond the building perimeter, reducing the potential for external unauthorized access.

- The California Consumer Privacy Act (CCPA) requires businesses to implement reasonable security procedures to protect consumer data, which includes securing wireless networks (State of California, 2018).

Set Up Network Segmentation: Create a separate guest network or segmented area specifically for the outdoor access point, isolating it from the main corporate network to contain any potential security breach.

- The Health Insurance Portability and Accountability Act (HIPAA) Security Rule requires covered entities to implement technical safeguards, including network segmentation, to protect electronic protected health information (HHS, 2013).

Tools/Documentation: Access control software, segmentation configuration guides, and guidelines for users to follow when connecting to the outdoor network.

MOBILE

1. DEVICE SECURITY IN TRANSIT MITIGATION

Enforce Full-Disk Encryption and Remote Wipe: All company-issued mobile devices must have full-disk encryption and enable remote wipe features, protecting data in case of loss or theft.

- The General Data Protection Regulation (GDPR) requires organizations to implement appropriate technical measures to ensure data security, including encryption (European Parliament and Council, 2016).

Implement Mobile Device Management (MDM) Policies: Use MDM software to monitor and manage devices, enforcing policies like password requirements and auto-lock to secure access.

- The Payment Card Industry Data Security Standard (PCI DSS) requires organizations to protect cardholder data, including on mobile devices (PCI Security Standards Council, 2018).

Tools/Documentation: Deploy MDM software and provide employees with a security protocol handbook outlining device handling procedures and promptly reporting lost devices.

2. BYOD POLICY MITIGATION

Require MDM Enrollment for BYOD: Make MDM enrollment mandatory for personal devices accessing the network, ensuring consistent security measures like encryption, remote wipe, and malware protection.

- The Gramm-Leach-Bliley Act (GLBA) requires financial institutions to implement information security programs, which include managing risks associated with BYOD (FTC, 2002).

Restrict Network Access for Unmanaged Devices: Limit access for non-enrolled devices to a segmented guest network, isolating them from sensitive internal resources.

- The Federal Information Security Modernization Act (FISMA) requires federal agencies to implement access controls, which includes managing access for BYOD devices (NIST, 2020).

Tools/Documentation: MDM software, network access control tools, and a BYOD policy document detailing access restrictions, device management requirements, and employee responsibilities.

4. Preventive Measures for Small Business WLAN and Mobile Environments

Preventive Measures for WLAN

1. Access Control Management

   Implement robust access control measures based on user roles and device types to limit network access.

   For Alliah, this would mean restricting network access based on employee roles and ensuring that only authorized devices connect to sensitive areas of the WLAN. By applying role-based access control, Alliah can reduce the risk of unauthorized access. Limiting access to sensitive data and resources helps ensure that employees only interact with necessary network segments, reducing the chance of data breaches or unauthorized entry. According to the Federal Information Security Management Act (FISMA), federal agencies and contractors must protect network access and control access levels (NIST, 2020), providing a strong basis for implementing access control at Alliah.

2. Regular Security Patching and Updates

   Ensure all WLAN devices, including access points, switches, and firewalls, are updated regularly to protect against known vulnerabilities.

   Regularly updating firmware and security patches helps safeguard Alliah's network from exploit vulnerabilities, particularly those targeting outdated or unpatched systems. The Gramm-Leach-Bliley Act (GLBA) mandates that companies handling sensitive customer information must implement measures to protect against potential risks, including keeping systems up to date (FTC, 2002). Alliah's regular patching schedule would demonstrate compliance with similar data protection best practices.

3. Intrusion Prevention System (IPS)

   Deploy an Intrusion Prevention System (IPS) to continuously monitor the WLAN for unauthorized access points or suspicious activities.

   An IPS provides active monitoring and alerts the IT team to unusual activity. Early detection capability enables Alliah to respond quickly to security threats, minimizing potential damage. IPS use aligns with Health Insurance Portability and Accountability Act (HIPAA) guidelines, which require active monitoring for unauthorized access in health-related organizations (HHS, 2013). For Alliah, implementing an IPS supports proactive security management across the network.

PREVENTIVE MEASURES FOR MOBILE ENVIRONMENT

1. MULTI-FACTOR AUTHENTICATION (MFA)

   Implement Multi-Factor Authentication (MFA) for all remote and mobile access, requiring users to verify identity through multiple authentication methods.

   MFA adds an additional layer of security for remote access. Even if a device is lost or stolen, MFA reduces the likelihood of unauthorized access. The Federal Trade Commission (FTC) Safeguards Rule under the GLBA requires businesses to use access control measures, such as MFA, to secure sensitive data (FTC, 2021). By implementing MFA, Alliah strengthens the security of its mobile environment and complies with data protection regulations.

2. DEVICE ENCRYPTION AND REMOTE WIPE CAPABILITIES

   Enforce full-device encryption and enable remote wipe on all mobile devices to secure data in case of device loss or theft.

   Encryption protects stored data by rendering it inaccessible to unauthorized users, while remote wipe ensures data can be erased if a device is lost. The California Consumer Privacy Act (CCPA) requires businesses to implement reasonable security procedures to protect consumer data, which includes encrypting sensitive information (State of California, 2018). For Alliah, implementing device encryption aligns with CCPA's data protection standards, securing data stored on mobile devices.

3. MOBILE DEVICE MANAGEMENT (MDM) SYSTEM

   Utilize a Mobile Device Management (MDM) system to enforce security policies, monitor devices, manage apps, and control access to corporate resources.

   An MDM provides centralized control over mobile devices and helps ensure that only compliant devices have network access. Alliah's IT team can monitor device compliance, push security updates, and enforce policies remotely. The GLBA also mandates that organizations handling sensitive information must have information security programs, which include managing mobile devices that access sensitive information (FTC, 2002).

REFERENCES

Aruba Networks. (2021). *Network Access Control: Secure Network Access in a Mobile World*. Retrieved October 29, 2024, from https://www.arubanetworks.com/assets/wp/WP_NAC.pdf

California Consumer Privacy Act (CCPA). State of California. (2018). *California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 et seq.* Retrieved October 30, 2024, from https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

Cisco. (2021). *High availability (SSO) deployment guide*. Retrieved October 31, 2024, from https://www.cisco.com/c/en/us/td/docs/wireless/controller/9-9/config-guide/b_cg99/high_availability.html

CISA. (2021). *Cybersecurity Best Practices*. Retrieved November 1, 2024, from https://www.cisa.gov/cybersecurity-best-practices

Federal Information Security Modernization Act (FISMA). U.S. Congress. (2014). *Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073*. Retrieved October 28, 2024, from https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf

Federal Trade Commission (FTC) Safeguards Rule. Federal Trade Commission. (2021). *Standards for Safeguarding Customer Information (Amended), 16 CFR Part 314*. Retrieved November 2, 2024, from https://www.ftc.gov/legal-library/browse/federal-register-notices/16-cfr-part-314-standards-safeguarding-customer-information

Forrester Research. (2021). *The Forrester Wave™: Unified Endpoint Management, Q4 2021*. Retrieved November 3, 2024, from https://www.forrester.com/report/the-forrester-wave-unified-endpoint-management-q4-2021/RES176043

Gartner. (2021). *Magic Quadrant for Unified Endpoint Management Tools*. Retrieved November 4, 2024, from https://www.gartner.com/en/documents/4003126

General Data Protection Regulation (GDPR). European Parliament and Council. (2016). *Regulation (EU) 2016/679*. Official Journal of the European Union, L 119/1. Retrieved October 29, 2024, from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Gramm-Leach-Bliley Act (GLBA). Federal Trade Commission. (2002). *Standards for Safeguarding Customer Information, 16 CFR Part 314*. Retrieved October 30, 2024, from https://www.ftc.gov/legal-library/browse/rules/safeguards-rule

Health Insurance Portability and Accountability Act (HIPAA). U.S. Department of Health and Human Services. (2013). *HIPAA Security Rule, 45 CFR Part 160 and Subparts A and C of Part 164*. Retrieved October 31, 2024, from https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

NIST. (2020). *SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations*. Retrieved November 1, 2024, from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

NIST. (2020). *SP 800-63B: Digital Identity Guidelines*. Retrieved November 2, 2024, from https://pages.nist.gov/800-63-3/sp800-63b.html

NIST. (2021). *SP 800-124 Rev. 2: Guidelines for Managing the Security of Mobile Devices in the Enterprise*. Retrieved November 3, 2024, from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r2.pdf

NIST. (2021). *SP 800-207: Zero Trust Architecture*. Retrieved October 28, 2024, from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

Palo Alto Networks. (2021). *What is an Intrusion Prevention System?* Retrieved November 4, 2024, from https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips

Payment Card Industry Data Security Standard (PCI DSS). PCI Security Standards Council. (2018). *Payment Card Industry (PCI) Data Security Standard: Requirements and Security Assessment Procedures, Version 3.2.1*. Retrieved October 29, 2024, from https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf

Sarbanes-Oxley Act (SOX). U.S. Congress. (2002). *Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745*. Retrieved October 30, 2024, from https://www.congress.gov/107/plaws/publ204/PLAW-107publ204.pdf