Kiarah Pettaway
[redacted]
C844: Emerging Technologies in Cybersecurity

Task 2: WLAN AND Mobile Security Plan

A. WLAN Issues

Insufficient Network Security Measures: Alliah's WLAN is protected by a firewall, but there is no mention of other security measures such as encryption protocols (e.g., WPA2, WPA3) or network segmentation. Without these measures, the WLAN is more susceptible to unauthorized access, eavesdropping, and data breaches.

Limited Coverage and Capacity Planning: While Alliah has strategically located access points, the coverage and capacity of the WLAN may become inadequate as the company grows and more employees join. This could lead to network congestion, slow performance, and potential security vulnerabilities if employees resort to using insecure networks to work around connectivity issues.

B. Mobile Device Issues

Unsecured Devices: The account representatives, who are on the road 80% of the time, use company-issued laptops, tablets, and smartphones. If these devices are not properly secured with updated antivirus software, encryption, and strong passwords, they are vulnerable to malware, data breaches, and unauthorized access.

BYOD Policy: Alliah allows a bring your own device (BYOD) policy, which can introduce additional security risks. Personal devices may not have the same level of security as company-issued devices, potentially leading to data leaks, unauthorized access to company resources, and compliance issues if personal devices are lost or stolen.

C. Mitigation

To mitigate the identified WLAN and mobile vulnerabilities at Alliah, the following steps can be taken:

1. **WLAN Vulnerabilities:**

a. Insufficient Network Security Measures:

- Enable WPA2 or WPA3 encryption on the WLAN to protect data in transit.
- Implement network segmentation to isolate sensitive data and devices from the rest of the network.
- Regularly update firewall rules and IDS signatures to protect against emerging threats.

b. Limited Coverage and Capacity Planning:

- Conduct a wireless site survey to identify areas with weak coverage or potential interference.
- Add additional access points or upgrade existing ones to improve coverage and capacity.
- Implement Quality of Service (QoS) policies to prioritize traffic and improve performance.

2. **Mobile Vulnerabilities**:

a. Unsecured Devices:
- Ensure that all company-issued mobile devices have updated antivirus software, encryption, and strong passwords.
- Implement Mobile Device Management (MDM) software to remotely monitor and manage devices, enforce security policies, and perform remote wipes if necessary.

b. BYOD Policy:
- Implement a comprehensive BYOD policy that outlines security requirements for personal devices, including the use of antivirus software, encryption, and strong passwords.
- Require employees to install security apps approved by the company, such as mobile antivirus software and VPN clients.

Tools and documentation needed for mitigation:
- Wireless site survey tools (e.g., Ekahau, NetSpot) for assessing WLAN coverage and performance.
- Firewall and IDS management software for updating rules and signatures.
- MDM software for managing and securing mobile devices.
- BYOD policy documentation outlining security requirements and procedures for personal device use.

D. Preventative Measures (w/ Regulations)

Regular Security Audits and Vulnerability Assessments:
- Conduct regular security audits and vulnerability assessments of the WLAN and mobile devices to identify and address potential security weaknesses (Scarfone, 2008).

Implement Strong Authentication and Encryption:
- Use strong authentication mechanisms (e.g., WPA2-Enterprise) for WLAN access to prevent unauthorized access (Frankel, 2007).
- Encrypt data in transit and at rest on mobile devices using industry-standard encryption protocols (e.g., AES) (Frankel, 2007).

Enforce BYOD Security Policies:
- Implement and enforce BYOD security policies that include requirements for antivirus software, encryption, and strong passwords on personal devices (Souppaya, 2016).

Employee Training and Awareness:
- Provide regular training to employees on mobile security best practices, including recognizing phishing attempts and securing devices (Wilson, 2003).

Mobile Device Management (MDM):
- Use MDM software to manage and secure mobile devices, enforce security policies, and remotely wipe devices if lost or stolen (Howell, 2023).

Monitor and Log Network Activity:
- Implement network monitoring and logging to detect and respond to suspicious activity on the WLAN and mobile devices (Kent, 2006).

Regular Software Updates and Patch Management:

- Regularly update WLAN access points, mobile devices, and software applications to patch known vulnerabilities (Barker, 2020).

E. BYOD

Alliah's BYOD approach can be effectively secured by implementing an MDM system. MDM solutions provide a centralized platform to manage, monitor, and secure mobile devices used in the organization, enabling the enforcement of security policies such as encryption, password protection, and remote data wipe. With robust security features such as encryption, remote wipe, and device tracking, MDM systems ensure the protection of sensitive company data from unauthorized access or loss. They also facilitate compliance with regulations such as GDPR and HIPAA by enforcing security policies. Furthermore, MDM systems streamline device management tasks, saving time and resources for IT staff, while enabling secure access to corporate resources from personal devices, thereby improving the overall user experience.

F. Resources

Scarfone, Karen, et al. “Technical Guide to Information Security Testing and Assessment.” CSRC, 30 Sept. 2008, csrc.nist.gov/pubs/sp/800/115/final.

Barker, Elaine. “Recommendation for Key Management: Part 1 – General.” CSRC, 4 May 2020, csrc.nist.gov/pubs/sp/800/57/pt1/r5/final.

Frankel, Sheila, et al. “Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i.” CSRC, 7 Feb. 2007, csrc.nist.gov/pubs/sp/800/97/final.

Howell, Gema, et al. “Guidelines for Managing the Security of Mobile Devices in the Enterprise.” CSRC, 17 May 2023, csrc.nist.gov/pubs/sp/800/124/r2/final.

Kent, Karen, and Murugiah Souppaya. “Guide to Computer Security Log Management.” CSRC, 13 Sept. 2006, csrc.nist.gov/pubs/sp/800/92/final.

Souppaya, Murugiah, and Karen Scarfone. “Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology.” CSRC, 6 Apr. 2022, csrc.nist.gov/pubs/sp/800/40/r4/final.

Souppaya, Murugiah, and Karen Scarfone. “Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security.” CSRC, 29 July 2016, csrc.nist.gov/pubs/sp/800/46/r2/final.

Wilson, Mark, and Joan Hash. “Building an Information Technology Security Awareness and Training Program.” CSRC, 1 Oct. 2003, csrc.nist.gov/pubs/sp/800/50/final.