WLAN And Mobile Security Plan

By: Griffin Haas

Alliah company is a new but fast-growing social media provider. Alliah is looking to expand the company and understands that it will need to start looking at expanding its WLAN network while securing it. As well as review their BYOD policy to properly secure the network.

I. WLAN Vulnerabilities and Mitigation

Alliah has five employees who travel 80% of the time. It seems that there may be some network authentication through the firewall, which will help keep company resources from unauthorized users. However, this does not protect the data in transit. Which can be seen if the employee is connecting from an unsecured/public network (Doherty 127). This can lead to attackers, connecting to the network, being able to snoop on traffic, or may use a Man-in-the-middle attack. To mitigate any possible threat, Alliah would need to implement a VPN solution that will create an encrypted tunnel that will encrypt the traffic being sent from the laptop to the company's WLAN. Cisco offers steps to install and use a VPN. The steps are as follows (Cisco):

1. Download all VPN Components (VPN Client, VPN Server, and a VPN Router)
2. Prep Devices (Make sure there is no conflicting ports/services for VPN client/server)
3. Install VPN Clients on the devices
4. Check for a setup Tutorial if the VPN provider does not offer software
5. Log into the VPN
6. Choose what VPN protocols.
7. Troubleshoot any issues
8. Fine-tune Connection.

Alliah should train and educate users on proper remote connectivity practices. Such as, not logging into private accounts on public/unsecured networks, and using a VPN when offsite/out of the office.

In the scenario, it also states that Alliah's internal infrastructure includes a Wi-Fi access point in an open patio area. This can allow a threat actor to place a device called an Evil Twin near the area, which will attempt to steal credentials and other data by acting as a man-in-the-middle between the user and the resources, by posing as a trusted access point. It can also set up fake captive portals that will assist in this campaign. (Doherty 130) To mitigate this kind of attack, Alliah should have users disable auto-connect to Wi-Fi as the Evil Twin attack relies on the victims' computer connecting to a familiar SSID to try and have them connect to the malicious access point. You may do this by going into your Wi-Fi settings and deselecting "Connect automatically" for PCs/Laptops, and similar options for phones. As mentioned before, it would also be good to educate users on proper cyber awareness such as using a VPN and avoiding logging into private accounts on unsecured/public Wi-Fi. (Panda Security)

II. Mobile Device Vulnerabilities and Mitigation

Alliah also deploys a BYOD policy to save money during launch. This can lead to multiple vulnerabilities. One of the vulnerabilities can be theft and/or loss of devices with sensitive information. Having employees travel can allow attackers to steal or find lost devices. If skilled enough, attackers could recover company/sensitive data. (Doherty 128) To mitigate the threat, it would be recommended to put GPS tracking on devices. Which can be used to help track devices if lost. Phones usually have software installed by default such as "Find my iPhone" and similar products for Android. Having the device be fully encrypted or compartmentalize

sensitive information and encrypting that compartment to protect the data from unauthorized access, even if the data was extracted without access to the device interface.

Another mobile device vulnerability is having users introduce malicious software from using their mobile devices. Some users may not be able to tell that they have installed malicious software, and can infect Alliah's network if connected to it, which can then spread the infection to the rest of the network (Doherty 128). To mitigate against this, a Mobile Application Management (MAM) application can be used. This allows the IT team to have control over company applications only. Which will allow the restriction of the use of company applications but not over the employee's device. Another method can be implementing an Anti-Virus solution to scan traffic and devices that are connected to the network.

III. WLAN / Mobile Preventative Measure

There are several options to implement preventive measures for WLAN. For one having device's BIOS configured to automatically terminate WLAN connections if a wired connection is detected. Usually called LAN/WLAN switching.. This helps close off an attack vector from the attacker. The Second is implementing host-based network security tools. Such as Host-based Intrusion Detection and Prevention systems (IDS/IPS). This allows for alerts and defense from multiple network interfaces to be used at once. As well as can stop attackers from entering the network and alert necessary employees to the possible incidents. (NIST SP 800-153, 6)

For mobile devices, preventative measures can be implemented by segmenting organization and personal information. This can be done with a MAM application. However, as the company is growing I would recommend getting rid of the BYOD policy and issuing company-owned devices with a Mobile Device Management (MDM) application as well as

Enterprise Mobility Management (EMM). This would give the IT staff full control over all devices. This will also help prevent or detect malware. As well as authorize users to use company resources. Another recommendation would be to implement a Trusted Execution Environment. Which is defined as "a controlled and separated environment outside the high-level operating system that is designed to allow trusted execution of code and to protect against viruses, Trojans, and rootkits" (NIST SP 1800-22, 16). This allows only trusted applications and code to be executed. Anything that is not explicated allowed.

IV. Federal, State, or Industry Regulations

The EU's General Data Protection Regulation (GDRP) and California Customer Privacy Act (CCPA) all affect Alliah. Focusing on the security aspect, it is expected to have user data adequately protected. To protect user's data from misuse and monetization. (Doherty 149) Alliah being a social media Company will have to worry about these regulations as they collect data from their users. These would be enough to justify the preventative measures above.

V. Recommend BYOD Approach

My first recommendation will go off the assumption that Alliah does not remove the BYOD policy. I would recommend using a MAM to allow segmentation between company resources and personal resources. Then encrypt both partitions to protect company and personal resources. It would also be recommended to use a VPN to connect to company resources and to use strong authentication methods such as MFA to properly authenticate the user. As users connect, they will be separated from the main network by VLAN to access the resources that they need. Having any non-necessary resources only be accessed onsite. I would also recommend adding an IDS/IPS to the access points of the VPN to detect/prevent any unwanted intrusion attempts. (NIST SP 1800-22, 22).

My second recommendation would involve removing BYOD completely and implementing company-issued devices. These will have MDM and EMM installed before handoff with employees. This will allow IT staff to monitor assets as well as track the devices in case of loss or theft. The above connection to remote resources would be the same. (VPN, MFA Authentication, LAN Segmentation). (NIST SP 1800-22, 22-23).

Work Cited

Boeckl, Kaitlin, et al. “Mobile Device Security: Bring Your Own Device (BYOD) Includes Executive Summary (A); Approach, Architecture, and Security Characteristics (B); Example Scenario: Putting Guidance into Practice (Supplement); and How-to Guides (C).” *Mobile Device Security: Bring Your Own Device (BYOD)*, Sept. 2023, nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-22.pdf, https://doi.org/10.6028/NIST.SP.1800-22.

“How to Set up a VPN in 6 Steps.” *Cisco*, www.cisco.com/c/en/us/solutions/small-business/resource-center/security/how-to-setup-a-vpn.html.

Doherty, Jim. Wireless and Mobile Device Security, Jones & Bartlett Learning, LLC, 2021. ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/westerngovernors-ebooks/detail.action?docID=6461875.

Security, Panda. “Evil Twin Attack: Definition and How to Prevent It - Panda Security.” Panda Security Mediacenter, 21 Nov. 2023, www.pandasecurity.com/en/mediacenter/evil-twin-attack/.

Souppaya, Murugiah, and Karen Scarfone. "Guidelines for securing wireless local area networks (WLANs)." NIST Special Publication 800 (2012): 153.