A logo of a university

Description automatically generated

**Western Governor’s University**

Emerging Technologies in Cybersecurity

C844

Joshua Lee

GRP1 Task 2: WLAN and Mobile Security Plan

1. **Vulnerabilities to the WLAN**

One of the vulnerabilities that is plausible for Alliah’s WLAN would be that it is very possible to plant an evil twin access point. There are seven access points that service the wireless LAN’s coverage for the company. It would be easy to add an evil twin access point with same SSID to get users to connect to it instead of the actual network. They could attach it to the network around the back patio area or if they gained access to the building, out of sight on the vacant third floor. This would allow the threat actor to gain access to various hosts that connect to the evil twin and be able to carry out attacks against those hosts.

Another vulnerability that the WLAN would be susceptible to is war driving. One of the areas that has an access point is the back patio area used by employees. Depending on the signal strength, a threat actor could search for an exploit in the WLAN to gain access to the network for internet access, all the way to gaining access to the network to steal data from the company (WLAN Security, n.d.).

1. **Mobile Device Vulnerabilities**

One mobile vulnerability that is apparent is malware. Being that there is no mention of any management of the mobile devices connecting to the network, this shows a vulnerability that can make many threats in. Malware can do anything from stealing confidential data to manipulating information and location data to perform blackmailing activities on the user of the device. Being as there is a BYOD program also in effect, this makes the attack surface bigger. BYOD devices are not as monitored usually as company-provided devices, which makes the probability of this happening greater.

Another vulnerability is the device stealing or loss for those who are traveling. The attack surface of this happening is increased as the five account representatives have 3 company issued devices each. It also doesn’t mention if others travel as well, just not as much. This would make the attack service bigger. Not to mention if they user BYOD devices on the network and store data on there and lose those.

1. **Mitigation of the Vulnerabilities**

To mitigate the impact if an evil twin access point was placed. First would be education to the employees on how to notice if they might have been compromised by connecting to an evil twin. Have them look for things such as a captive portal asking for login details that normally doesn’t show up or checking their connection if they are getting disconnected a multitude of times out of the norm (*Evil Twin Attack*, 2023). For the IT side of things, if something like this gets reported you would monitor the network to see if users who are in building are showing up on the network or not. Another mitigation tactic is to have a list of MAC addresses of the existing access points and verify those of which users are connecting to and root out the evil twin. Check areas (such as the vacant third floor or patio) for devices and if not found that way, use a spectrum analyzer to find them (Piccininni, n.d.). If anyone is has connected to an evil twin, the mitigation plan would be to remove the device from the evil twin, change all passwords, make sure 2FA is enabled, run a full system scan, and contact the authorities.

To mitigate war driving there would be a couple options that would fit for Alliah. If the offices are closed at a certain time and no one is allowed in after office hours, you could have the AP devices on a timer to not broadcast during off hours. Making sure all APs have had their default credentials changed is a huge blow to war driving, as they cannot get into the settings and manipulate them to their advantage. Also, to make sure that you are using the strongest encryption that your APs provide in order to allow getting into the devices harder to do so (*Wardriving*, n.d.).

To mitigate malware on mobile devices. First you would set forth a policy that devices (both company-provided and BYOD) would need an antivirus on them in order to prevent and also mitigate if malware were to affect them. Employee education is also a big factor here for mitigation. This would teach the users on how to be wary of signs of malware infection and teach them ways to encrypt their data when not in use, so that if they do get compromised, it reduces the probability of data being stolen or used (Zamora, 2016).

For lost or stolen devices, mitigating this would be partially the user being always aware of their devices, but also a process if this occurs. Report to the company immediately if the device is missing or stolen. If missing, notify all the locations you think it may have been lost to either find or have them on the look out for it. If stolen, users should file a police report immediately. If any thing such as remote lock or find my device is possible to be activated, the user should do so. Changing passwords would be smart just in case a non-authorized individual gains access and can look through your passwords saved on the device. Service providers should also be notified in order for them to disable the device or if they have alternate tracking methods (*6 Steps Organizations Can Take to Minimize the Impact of Lost/Stolen Devices*, 2018).

1. **Preventive Measures for the Wireless and Mobile Environments**

There are multiple preventive measures that can be applied to Alliah’s WLAN. One of the most important would be having a system can monitor and even repel or prevent attacks to the network (Souppaya & Scarfone, 2012). Having a NIDS (Network Intrusion Detection System) and/or a NIPS (Network Intrusion Prevention System) would be a way of achieving this. Not only can they detect and/or protect the network, but they also have tools that analyze and connect to databases to identify the attacks that possible or occurring (*20 Ways to Monitor Network Traffic | Teramind Blog*, 2022).

The same could be said for the mobile environment and the multitude of measures that could be applied. The biggest one that I believe would have a great effect on Alliah’s mobile environment would be an MDM (Mobile Device Management) solution. By having an MDM solution, this could be installed on both BYOD and corporate-provided mobile devices. This would let the user know or also prevent them from being non-compliant with whatever policy is created by Alliah (Boeckl et al., 2022). This can range from not allowing a list of applications to be installed on devices if they are to interact with the network to wiping parts of data that could cause troubles if the device was lost and compromised.

The regulations that would justify these measures taking place would be both the European Union’s General Data Protection Regulation and the California Customer Privacy Act. Since this is a website aimed young professionals, this would be able to be accessed anywhere on the planet. Europe and California definitely would be a probable part of the demographic to be accessing this site. By employing a NIDS/NIPS to the WLAN and an MDM to the mobile environment, this would allow the Alliah to keep the data confidential, allow greater integrity by protecting the data, and show accountability on the way the data is handled.

1. **Solutions to BYOD Approach**

The first recommended solution would be for users who are traveling or not on the actual network to use a VPN. This can be a solution for corporate-provided devices but would be even more so for BYOD due to less control over the personal devices. It would protect data in-transit and protect from an array of different attacks such as eavesdropping and data interception. This would maintain the confidentiality and integrity of data when interacting with corporate data or applications (Boeckl et al., 2022).

Another strong solution would be to access content through a Virtual Desktop Infrastructure/Remote Desktop. This would prevent data being stored on the local device and is managed still within network on the Virtual Desktop, be it a physical workstation being remoted into or a virtual machine. The company would also have more control over the infrastructure to do things such as add additional authentication or have total control over what applications or settings get made to the environment (*Bring Your Own Device (BYOD)*, n.d.). This would provide a great amount of security to the confidentiality, integrity, and availability of corporate resources.

**References**

Boeckl, K., Grayson, N., Howell, G., Lefkovitz, N., Ajmo, J., McGinnis, M., Sandlin, K., Slivina, O., Snyder, J., & Ward, P. (2022). *Mobile Device Security: Bring Your Own Device (BYOD)* (NIST Special Publication (SP) 1800-22 (Withdrawn)). National Institute of Standards and Technology. <https://csrc.nist.gov/pubs/sp/1800/22/2pd>

Piccininni, J. (n.d.). *Detecting & Locating Rogue Access Points—Inpixon*. Retrieved November 12, 2023, from <https://www.inpixon.com/blog/detecting-locating-rogue-access-points>

Souppaya, M., & Scarfone, K. (2012). *Guidelines for Securing Wireless Local Area Networks (WLANs)* (NIST Special Publication (SP) 800-153). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-153>

Zamora, W. (2016, September 20). Top 10 ways to secure your mobile phone | Malwarebytes Labs. *Malwarebytes*. <https://www.malwarebytes.com/blog/news/2016/09/top-10-ways-to-secure-your-mobile-phone/>

*Bring your own device (BYOD)*. (n.d.). Retrieved November 13, 2023, from <https://www.ncsc.gov.uk/collection/device-security-guidance/bring-your-own-device>

*Wardriving: What it is and how to help protect your network*. (n.d.). Retrieved November 12, 2023, from <https://us.norton.com/blog/id-theft/wardriving-what-it-is-and-how-to-help-protect-your-network>

*WLAN security: Best practices for wireless network security | TechTarget*. (n.d.). Security. Retrieved November 5, 2023, from <https://www.techtarget.com/searchsecurity/WLAN-security-Best-practices-for-wireless-network-security>

*6 Steps Organizations Can Take to Minimize the Impact of Lost/Stolen Devices*. (2018, May 1). Vaporstream. <https://www.vaporstream.com/blog/6-steps-lost-stolen-devices/>

*20 Ways to Monitor Network Traffic | Teramind Blog*. (2022, June 15). <https://www.teramind.co/blog/ways-to-monitor-network-traffic/>

*Evil twin attack: What it is and how to prevent it | NordVPN*. (2023, September 12). <https://nordvpn.com/blog/evil-twin-attack/>