**Alexis Tostado**

**C844 Task 2**

1. **WLAN Vulnerabilities**

* The first WLAN vulnerability in this scenario is the access point that is located outside in the patio. This presents a lot of leakage from the network, meaning that anyone on the outside of the building can perform a passive or active attack on the network.
* Secondly, with the setup in this scenario, there is a chance of a rogue access point being installed by a malicious or even non malicious actor that can compromise the network.

1. **Mobile Vulnerabilities**

* One mobile vulnerability in this scenario would be the fact that a Bring Your Own Device (BYOD) policy is still in place. This poses a vulnerability as these mobile devices are not managed or encrypted and can be used by attackers to gain access to the greater network.
* Second, would be the fact that employees are travelling 80% of the time with three company devices. Which without proper management these devices can be stolen or lost and potentially picked up by someone with malicious intent for the device.

1. **Mitigation Steps**

* To mitigate the RF leakage from the AP that is outside in the patio, the IT technicians should adjust the signal power, so it does not go past the boundaries. Furthermore, assuming the access point is using omnidirectional signaling, the device antenna could be swapped out for a semi - directional antenna set up in a horizontal slice to provide service inward of the building and not all around.
* To prevent a rogue access point from being installed in the network, the company should implement a form of network inventory system and auditing to ensure only company approved devices are installed and nothing else is added on. Using commercial rogue AP detection hardware would be a useful product in this scenario as the IT team is small and this device can help detect and prevent rogue AP from working.
* To prevent the employees’ devices from being the source of malicious attacks to the company a policy change would be required. To ensure proper use of network resources and network security from mobile devices a Mobile Device Management (MDM) and Mobile Application Management (MAM) systems should be implemented. With these systems in place the IT team can easily push security updates onto these devices and set policies and firewalls for intranet and internet surfing. Furthermore, MAM would ensure only approved applications are installed on the phone with proper credentials.
* A way to mitigate the risk from a device being stolen or lost would be to have the ability to remote wipe devices (NIST SP 800-88). With this ability the device regardless of its location can be wiped of all its sensitive data before the data becomes compromised. (Akella)

1. **Preventative Measures**

* A preventative measure that would reduce the risk of unauthorized access to company resources would be to implement Multifactor Authentication (MFA) for all employees. MFA would require employees to have 2 or more factors in which they can log in to a workstation for example, pin and facial scan. This policy can eliminate the risk of possible unauthorized access to the company resources. Furthermore, implementing a strong access control measures can further prevent unauthorized access. These measures are backed by the PCI DSS compliance standards and Alliah should follow their checklist to not only follow regulatory guidelines, but also benefit her company. (PCI Security Standards Council)
* Secondly, the PCI compliance standards list the use and regular update of an anti-virus software. (PCI Security Standards Council) Alliah having an anti-virus software or device installed in their internal server will help in preventing the intrusion of unwanted traffic. Furthermore, it can be used to manage network ports and software management.

1. **BYOD Solution**

* Having a Bring Your Own Device (BYOD) policy can save the company money however, it must come with detailed and strict policies that are enforced. The company must set clear standards for acceptable device allowed for use and proper control for what apps are downloaded. Furthermore, using the MDA and MAM software can be used to enforce and ensure that these policies are being enforced.
* Since employees are travelling 80% of the time also, devices must also be secured because these devices become a logical extension of the network and thus can pose a risk to the data in the device and the network back at HQ. Furthermore, employees have access to the company network remotely and policies should be implemented and enforced to use a Virtual Private Network (VPN) when accessing the company network. The VPN will provide a secure and encrypted way of communication with the company’s network safely. (Souppaya and Scarfone)

**References**

Team, Blog. “WIFI Antenna Types.” *WiFi Antenna Types*, www.accessagility.com/blog/wifi-antenna-types. Accessed 19 Aug. 2023.

93digital. “What Is NIST 800-88, and What Does ‘Media Sanitization’ Really Mean?” *Blancco*, 18 May 2023, www.blancco.com/resources/blog-what-is-nist-800-88-media-sanitization/#:~:text=NIST%20Special%20Publication%20800%2D88,data%20from%20electronic%20storage%20media.

Akella, Prasanthi. “BYOD in the Workforce: MDM and MAM With Microsoft Intune.” *Application Security Blog*, May 2022, www.synopsys.com/blogs/software-security/byod-workforce-mdm-mam-microsoft-intune.

Wilson, Mark G., and Joan Hash. *Building an Information Technology Security Awareness and Training Program*. 1 Jan. 2003, https://doi.org/10.6028/nist.sp.800-50.

Grassi, Paul, et al. *Digital Identity Guidelines: Revision 3*. 22 June 2017, https://doi.org/10.6028/nist.sp.800-63-3.

Souppaya, Murugiah, and Karen Scarfone. *User’s Guide to Telework and Bring Your Own Device (BYOD) Security*. 1 July 2016, https://doi.org/10.6028/nist.sp.800-114r1.

PCI Security Standards Council. “Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security and Credit Card Security Standards.” *PCI Security Standards Council*, 8 Aug. 2023, www.pcisecuritystandards.org/document\_library.