WLAN Vulnerabilities

Access Point servicing an outside location

The WLAN is accessible from outside and poses a security risk. Someone could come within range of the signal and try to gain unauthorized access to the network. Alternatively someone could attempt to broadcast a stronger signal to get local hosts to connect to their signal instead. Typically we want wireless access to only be inside the building. Doherty (2021).

Empty Third Floor

An attacker could gain entry to the building. The empty third floor would be a prime place to attempt setting up a rogue access point. Empty spaces that are not often checked are security risks that need to be addressed. Doherty (2021).

Mobile Vulnerabilities

Devices are traveling outside the office often with no MDM enabled

If mobile devices are being used by the company they need to be managed in case of lost or stolen phones. This will ensure that the phone can be remotely wiped if it is lost or stolen ensuring confidentiality of company resources. Doherty (2021).

MAM software is not implemented

Software that determines if an application adheres to the BYOD and acceptable use policy should be implemented. User's may unknowingly install malicious apps that could compromise the confidentiality of your network environment. Doherty (2021).

Mitigation

Limit power output of wireless signal / Remove access point

Limiting the amount of power that your wifi signal puts out is an essential part of containing your signal to the building only. Complete removal of the access point servicing the outside area is recommended. If however the company chooses to reduce antenna power output accessing the router either through webportal or secure connection and lowering the Effective Radiated Power will limit the signal to only the back patio area.

Site Surveys

Enabling regular site survey's and security checks to prevent unwanted access to the building. This will ensure that rogue access points will not go unnoticed for a long period of time. Doherty (2021). Network Teams are able to utilize many free applications to conduct site surveys. Jacobs (2022). Further research needs to be done to determine the exact needs of Alliah as there are many options but a general list of the most popular tools includes Wifi Analyzer, and Ekahau. Ciarlone (2023).

WiFi Analyzer: https://www.wifianalyzer.info/

Ekahau: https://www.ekahau.com/

Mobile Device Management Software

Setting up and enabling MDM software will ensure confidentiality of data when traveling outside the office**.** Doherty (2021). Choosing an MDM software requires some research for the businesses exact needs as many solutions exist. IBM offers a 30 day free trial to their MaaS360 MDM solution. MDM software is an essential part of enforcing the BYOD policy set by Alliah. IBM. (n.d.).

MaaS360: https://www.ibm.com/products/maas360/mobile-device-management

Mobile Application Management Software

With MAM an IT department can verify and authorize the downloading and installation of applications. This ensures that user's are not downloading malicious applications. Doherty (2021). MAM software is often bundled with MDM software.

Here are some available options:

Microsoft Enterprise and Mobile Security Management: https://www.microsoft.com/en-us/licensing/product-licensing/enterprise-mobility-security

MaaS360: https://www.ibm.com/products/maas360

Citrix Secure Hub: https://docs.citrix.com/en-us/citrix-secure-hub/overview.html

Preventative Measures

Standardize, Automate, and centralize WLAN security

This would allow the organization to quickly detect changes in network configuration that are unauthorized. Newly identified vulnerabilities will be much more easily identified and mitigated. This improves our network security by creating a way for us to quickly detect if a rogue access point has been set up on the network. NIST (2012).

Enterprise Mobility Management

Organizations should use EMM solutions to secure mobile devices of user's that are authorized access to the organizations resources. The EMM solution can perform the essential MDM functions that we need on our network at Alliah. NIST (2023).

GDPR

The GDPR regulation states that user data needs to be adequately protected and that businesses need to be accountable for the way they handle user information. Standardizing the security practices of the organization supports this regulation by protecting the network that accesses the user information. If someone could gain access to our network at Alliah they could then foreseeably gain access to our website servers and the data stored within. Enacting an enterprise mobility management solution protects the company in a similar way. This measure will ensure that access to company resources will be restricted to only those whon are allowed. This will mitigate the risk of data being stolen or accessed from a stolen device therefore protecting the confidential data. Doherty (2021).

Recommended BYOD Approach

Desktop Virtualization

Alliah could implement desktop virtualization allowing employees to bring their own devices and connect to the corporate network through a virtual desktop ran on the company network. Employees would connect to the network and control the virtual desktop with their own device. Doherty (2021).

VPN

The use of a VPN can increase security in connections established by authorized mobile devices. This technology applies an additional layer of encryption and also allows a company to set what devices can connect to the network. Enforcing access controls is a great way to ensure only authorized devices can connect. Furthermore a VPN can be used in tandem with the MDM software by restricting access based on MDM compliance. NIST (2023).

References

Ciarlone, J. (2023, May 4). 8 of the Best Wireless Site Survey Tools in the market. 8 Of The Best Wireless Site Survey Tools In The Market. https://services.hummingbirdnetworks.com/blog/the-8-best-wireless-site-survey-tools-for-your-business

Doherty, J. (2021). Security Threats Overview: Wired, Wireless, and Mobile. essay, Jones & Bartlett Learning, LLC.

What is Mobile Device Management (MDM)?. IBM. (n.d.). https://www.ibm.com/topics/mobile-device-management

Jacobs, D. (2022, November 16). 3 types of wireless site surveys and how to conduct them. Networking. https://www.techtarget.com/searchnetworking/tip/3-types-of-wireless-site-surveys-and-how-to-conduct-them

NIST. (2012, February 21). Guidelines for securing wireless local area networks (wlans). https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-153.pdf

NIST. (2023, September 28). NIST Special Publication 1800-22 - Mobile device security. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-22.pdf