Quinton Green

Emerging Technologies in Cybersecurity - C844

GRP1 TASK 2: WLAN AND MOBILE SECURITY PLAN

A WLAN vulnerability that presents a risk for Alliah is a rogue access point. The company headquarters has a vacant third floor that can be used to set up a rogue access point by an attacker who gains access to the building. The rogue access would go unnoticed because no one goes to that floor. Another WLAN vulnerability is an evil twin access point. Alliah has 7 wireless access points around the facility and 1 on the back patio. An attacker can create an SSID to appear like one of the authorized SSID’s to trick employees to connect to them and give them access to the network to launch attacks (Doherty, 2021).

A lost or stolen device presents mobile security risks for Alliah. Since five employees are account representatives who are on the road at least 80 percent of the time, and each rep has a company-issued laptop, tablet, and smartphone, any of those 15 devices are at risk. If those representatives saved or store their passwords or VPN information on the devices an attacker can gain access to the company network through the employees’ credentials or find ways to crack their passwords (Doherty, 2021). Another mobile security vulnerability is browser exploits on the BYOD environment. Due to their effort to save costs and based off the scenario information there does not seem to be mobile device management set up for those devices which means patches and updates will be behind and not up to date with the company-owned devices (Doherty, 2021). The BYOD devices will be open to malicious malware (Doherty, 2021).

These vulnerabilities need to be mitigated. To mitigate the rogue access points, the IT team can conduct regular site surveys sweeps to monitor authorized access point and discover rogue access points (Doherty, 2021). For the evil twin access points have IT conduct SSID site surveys to find any suspicious, duplicate, or misspelled SSID’S (Ledesma 2023). The lost or stolen mobile devices can be mitigated by remote locking and data wiping to cut off access to sensitive data and business account information, use strong encryption on stored information, and use mobile GPS and tracking to try to find the devices before an attacker gets the chance to access them. If the device is simply lost it can be found by the GPS tracking and a remote wipe would not be needed, a remote lock can always be removed. (Doherty, 2021). BYOD devices can be mitigated by employing mobile device management so that all devices receive updates, and patches, and mobile application management or having all devices become COPE or CYOD approved devices.

There are several preventive measures I recommend for Alliah to maintain the security posture of the WLAN and mobile environments. The first major preventive measure to protect the WLAN and mobile environments are user training and education. Regularly educating employees on being aware of suspicious emails that could be used for phishing, accessing, and downloading applications or links from insecure sites, strange text messages used for smishing in the mobile environment, misspellings or errors in emails and websites all the way down to physical access to the building. They need to be aware of the suspicious SSIDs and how to spot them, so they don’t connect to rogue access points or evil twin access points. Employees need to be aware of tailgating, clean desk policies, locking screens on mobile devices, and having strong passwords for every device and not storing password information in a place that is accessible (Doherty, 2021).

Implementing logical/technical controls are another preventive measure to protect the network. Install network intrusion protection, antimalware software, host intrusion detection and protection, and firewalls (Doherty, 2021). The technical controls will prevent evil twin access points and rogue access points from being undetected. To prevent rogue access points from being set up in the facility, physical controls should be in place. These controls would be smart badges, man traps, cameras, door locks, and a security guard especially for the vacant third floor to prevent attackers from accessing the building (Doherty, 2021). Establishing strong encryption standards will also protect both the WLAN and mobile environments.

Ideally for the BYOD devices vulnerabilities you can employ mobile device management (MDM) and mobile application management (MAM). They can be used to update and download antimalware software, enforce company regulations and security policies, and configure the devices to the company’s security standards, restrict access of sensitive company information, protect the devices from lost or theft by remote lock and remote wiping, provide encryption, and secure applications and the network (Doherty, 2021). On the administrative control side, I would have the employees sign acceptable use and BYOD policies, so they understand procedures and processes (Doherty, 2021). Since Alliah is a small business and may not be able to afford MAM or MDM, making all the device COPE devices is an option or choose your own device CYOD from a list of approved and tested devices. Desktop virtualization is another option because it bypasses many remote access security issues and having employees access company resources through a secure VPN (Doherty, 2021).

Regulations that justify these measures can be supported by the PCI DSS standard which requires that organizations build and maintain a secure network, maintain a vulnerability management programs, implement strong access control measures, maintain an information security policy, and regularly test and monitor networks (Doherty, 2021). As more people visit and join the social media website their personal information needs to be protected. The General Data Protection Regulation (GDPR) and California Customer Privacy Act CCPA gives people control over their personal information and protects their rights, collect the minimum amount of date required for the purpose of using their social media website and platforms, and under lawfulness, fairness, transparency, misuse, and monetization Doherty, 2021). When the CEO decides to take the company public, she will have to initiate SOX regulations for corporate governance and financial reporting for public companies (Doherty, 2021).

**References**

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.= pages 127, 128, 130

Ledesma, Josue (2023 June 16) [Evil Twin Attack: What it is, How to Detect & Prevent it (varonis.com)](https://www.varonis.com/blog/evil-twin-attack)