



Mobile Security Plan

Bluegreen Media

Danielle Wicklund

INFS3110-B

Dr. Jamie Pinchot

December 3rd, 2020




Table of Contents

Introduction.....	Page 3
Mobile Threats.....	Pages 4 - 6
Phishing.....	Page 4
Out-of-Date Devices.....	Pages 4 - 5
Spyware.....	Page 5
Browser exploits.....	Page 5
Mobile ad fraud.....	Page 5
Poor password hygiene.....	Pages 5 - 6
Vulnerability Analysis Plan.....	Pages 7 - 9
Vulnerability Assessment.....	Pages 7 - 9
Audit Process.....	Page 9
Recommendations.....	Pages 10 - 11
Prioritization of updates.....	Page 10
Strong authentication measures.....	Page 11
Applications that are suspicious or malicious are blocked	Page 11
References.....	Page 12

Introduction

Bluegreen Media is an up-and-coming social media provider. Currently, there are 35 full-time employees working at Bluegreen. Workers collaborate with each another on projects in offices or shared spaces. The company headquarters is located in a three-story building, which used to be an old warehouse and was converted for office use. Inside the building, the two floors encompass employee working spaces while the third floor has vacancy.

A year ago, Bluegreen created a social media Web site for young urban professionals and launched a mobile app to assist in Google Android or Apple iOS device access to the site. This Web Site is successful. In fact, it is becoming more popular each month. Bluegreen's CEO is planning to hire more talented individuals and take the company public in the future. Thus, she is considering BYOD and wants to further secure the company's wireless network infrastructure. In order to make these choices, the CEO needs a current mobile threat analysis report and recommendations for strengthening the mobile security posture at Bluegreen.

As the one of the network professionals on the IT team, it is my job to help the CEO and team by writing a mobile security plan. This report will include the following:

- Mobile Threats section that describes pertinent mobile threats.
- Vulnerability Analysis Plan that details the vulnerabilities, tools, and suggested audit process.
- Recommendations section that entails suggestions for mobile security enhancements.
- References section that includes APA cited sources used throughout this report.

Mobile Threats

As mobile technology evolves, so does the threats. It is imperative to know about these threats, especially since employees might encounter one of them. Subsequently, these are the six mobile security threats that Bluegreen Media and other small companies must be cognizant of:

1. Phishing

1. Phishing is a type of social engineering tactic. Essentially, cyber criminals trick users by impersonating a trusted contact. Then, they may ask the user to click a link, open a file, or provide personal information. "Users are actually three times more likely to respond to a phishing attack on a mobile device than a desktop, according to an IBM study — in part because a phone is where people are most likely to first see a message" (Raphael, 2020). Even more troubling, these threat actors are becoming more clever. For instance, there are now phishing apps that look like the real ones. It is hard to differentiate between the two because of the small font and screen on a mobile device. These fake apps will collect data you input such as passwords (Norton Life Lock, 2020).

2. Out-of-Date Devices

1. Sometimes, certain devices and technology companies do not release regular updates. This is alarming because an outdated mobile devices does not have the necessary patches and software updates installed yet. As a result, this increases vulnerabilities to mobile threats like data breaches In the case of the

Internet of Things (IoT), it would exacerbate this issue since it is the new frontier of technology (Raphael, 2020).

3. Spyware

1. In a mobile device, spyware lingers unnoticed. While the user is going about his/her/their daily lives, Spyware collects data without your permission, which is shared with advertising companies or other third parties. This includes information about your internet usage, location, and contacts. Thus, this becomes an issue for the user, as well as his/her/their family, friends, and mutual connections (Norton Life Lock, 2020).

4. Browser exploits

1. Browser exploits are malicious code. Basically, they manipulate a mobile browsers security flaws and compete against other browser applications. Individuals can spot a browser exploit attack if their homepage or search page has suddenly changed (Norton Life Lock, 2020).

5. Mobile ad fraud

1. Mobile ad fraud has many variations. However, it usually takes the form of malware. On the ad, it appears as a legitimate user, website, and/or application. If the user clicks on it, the ad fraud malware will run and be installed in the background. Then, it damages the mobile user's device. It does this by overheating, draining the battery, slowing it down, or incurring higher data charges (Raphael, 2020).

6. Poor password hygiene

1. Weak passwords pose a significant problem if there are unsecured user accounts. This is especially true if phones have personal and company data and sign-ins on it. "According to a 2018 LastPass analysis, a full half of professionals use the same passwords for both work and personal accounts. And if that isn't enough, an average employee shares about six passwords with a co-worker over the course of his or her employment, the analysis found" (Raphael, 2020).



Image: (Raphael, 2020)

Vulnerability Analysis Plan

It is not enough to know about potentially serious mobile threats. Corporations must mitigate them through various methods. This section includes an outline of suggested tools, an audit process, and a vulnerability assessment.

To start, "Vulnerability assessment is the process of defining, identifying, classifying, and prioritizing vulnerabilities in systems, applications, and networks. It provides an organization with the needed visibility into the risks that exist concerning external threats designed to take advantage of vulnerabilities" (Cavalancia, 2020). In other words, vulnerability assessments are valuable. It gives the business the opportunity to identify unauthorized means of access, create mitigation strategies, and correct any loopholes. Also, it can be used in conjunction with an organization's preferred automated or manual tools (Gonzalez, 2018). These are the four steps in a vulnerability assessment:

1. Conduct an initial assessment.

1. By identifying network devices, organizations better understand the risk associated with them. Client input should be the basis for this assessment like a security assessment vulnerability scanner (Gonzalez, 2018). The level of permissions, Internet accessibility, the device's role, and more should be used when determining the risk (Cavalancia, 2020). In turn, this can be used for the prioritization of tasks and items. Also, it can be utilized to ascertain the risk appetite, countermeasures, risk tolerance level, risk mitigation practices, and risk mitigation policies (Gonzalez, 2018).

2. Define a system baseline.

1. Information about the systems must be gathered. "For each given device to be assessed for vulnerabilities, it's necessary to understand whether its configuration meets basic security best practices" (Cavalancia, 2020). The software, ports, installed services, and operating system should serve as the baseline for the configuration. Additional details should be perused like any installed applications (Cavalancia, 2020).

3. Perform a vulnerability scan

1. There are unauthenticated or authenticated performances for vulnerability scans. It is suggested to use the authenticated means because it is a credentialed scan aimed at finding misconfigurations, missing patches, and technological loopholes. When performing a vulnerability scan, it is important to consider compliance to regulations too. Enterprises may be subject to legalities like the The General Data Protection Regulation (GDPR) (Cavalancia, 2020).
2. These are some recommended tools to render the best results: CMS web scan (Joomla, WordPress, etc.), Most common ports best scan (i.e., 65,535 ports), Firewall scan, Stealth scan, Aggressive scan, Full scan, exploits and distributed denial-of-service (DDoS) attacks, Open Web Application Security Project (OWASP) Top 10 Scan, and OWASP Checks (Gonzalez, 2018).

4. Create a vulnerability assessment report.

1. The importance of reporting can be found in the scan's result and risk of assessed systems. Then, it determines the course of action and next steps an or-

ganization will take. It encompasses pertinent details about vulnerabilities such as the vulnerability discovered, the date of discovery, a list of systems and devices found vulnerable, detailed steps to correct the vulnerability, and mitigation steps (Cavalancia, 2020).

Besides the vulnerability assessment, there should be an audit process as well. External or internal IT auditors can assist in this process by cooperating with various corporate departments, overseeing the mobile app development, and "Implementing a basic robust framework that determines a minimum amount of security controls that allow mobile apps to withstand the risk of operating in a vulnerable mobile environment" (Khan, 2016).

With that being said, ISACA's suggested framework ensures the proper controls for mobile apps. It achieves this by examining the risks to mobile devices, mobile networks, mobile app web serves, and mobile app databases. When these risks are better understood, controls can be used to increase the security of mobile apps. ISACA experts suggest to use penetration testing in conjunction with their framework in order to decrease the likelihood of vulnerabilities, and reduce data leakages (Khan, 2016).

Recommendations

Finally, Bluegreen must take action when it comes to strengthening the security of the company's mobile environment and mobile security posture. Although the enterprise has taken the liberty of increasing cybersecurity with methods such as a network firewall, threat actors are coming up with newer and better techniques. Hence, it is better to be proactive rather than reactive. In order to safeguard the company's and users' data, Bluegreen must decide on which next steps to take. Based on the company's profile, these are the top three recommendations:

1. Prioritization of updates

1. When it comes to business, updates are essential. Updates have security patches that protect against mobile security threats. If these are not installed immediately, the business's data, security, and solutions may be in jeopardy (Hein, 2019).
2. This is especially true when it comes to Bring Your Own Device (BYOD). Since Bluegreen has a BYOD policy to control costs, there must be some considerations. According to Schick (2019), "In BYOD environments, it's critical to set minimum requirements for the devices that are allowed to access corporate systems and apps. Beyond three years from initial release, many devices stop receiving regular OS updates and security patches, making them more vulnerable to new exploits. If you're dealing with constrained IT resources, you have to determine the tradeoff between trying to figure out a mobile security strategy on your own and simply making use of what is already market-ready and available to businesses" (pg. 1).

2. Strong authentication measures

1. In terms of mobile cybersecurity, this is a company's first line of defense. Authentication provides assurance that rogue third parties have reduced access to an enterprises's mobile devices. Instead, only authorized users can obtain access (Hein, 2019). Short and easily forgotten passwords weaken authentication. Therefore, experts recommend the implementation of two-factor authentication. This installation can aid in a businesses developing a layered mobile security strategy (Schick, 2019).

3. Applications that are suspicious or malicious are blocked

1. Wary applications installed on the mobile device can damage the associated systems and networks. For instance, corporate data could be stolen (Schick, 2019). So, it is imperative for users to understand that they only install business-verified apps. If worst case scenario happens, enterprise management solutions block suspicious or malicious apps using security policies and permissions as guidelines (Hein, 2019). Some of the suggested tools include whitelisting and blocklisting applications. They inform employees and employers on the safety of specific apps and devices. To demonstrate, IT departments can leverage blocklists to their advantage because they block access to apps and notify personnel of any attempts. On the contrary, whitelists help employees choose work, corporate mobile tools, over play, games and social media, with special highlighting features (Schick, 2019).

References

- Cavalancia, N. (2020, July 8). *Vulnerability assessment steps, process explained*. AT&T Cybersecurity. Retrieved from <https://cybersecurity.att.com/blogs/security-essentials/vulnerability-assessment-explained>
- Gonzalez, K. (2018, June 8). *A step-by-step guide to vulnerability assessment*. SecurityIntelligence. Retrieved from <https://securityintelligence.com/a-step-by-step-guide-to-vulnerability-assessment/>
- Hein, D. (2019, October 25). *7 essential mobile security best practices for businesses*. Solutions Review. Retrieved from <https://solutionsreview.com/mobile-device-management/7-essential-mobile-security-best-practices-for-businesses/>
- Khan, M. (2016, July 1). *Mobile app security—audit framework*. ISACA Journal. Retrieved from <https://www.isaca.org/resources/isaca-journal/issues/2016/volume-4/mobile-app-securityaudit-framework>
- Norton Life Lock. (2020). *5 mobile security threats you can protect yourself from*. Norton. Retrieved from <https://us.norton.com/internetsecurity-mobile-types-of-common-mobile-threats-and-what-they-can-do-to-your-phone.html>
- Raphael, JR. (2020, February 25). *8 mobile security threats you should take seriously in 2020*. SSO. Retrieved from <https://www.csoonline.com/article/3241727/8-mobile-security-threats-you-should-take-seriously-in-2020.html>
- Schick, S. (2019, August 21). *10 mobile security best practices to keep your business safe*. Insights. Retrieved from <https://insights.samsung.com/2019/08/21/10-mobile-security-best-practices-to-keep-your-business-safe/>