What Alliah ShouldDo to Best Mitigate Their Risks Concerning Network Security

Student’s Name

Institutional Affiliation

What Alliah Should do to Best Mitigate Their Risks Concerning Network Security

**Two LAN Vulnerabilities that Present Risk to Alliah**

The organization has several employees who use a WLAN gigabit connection that can be subject to several risks or vulnerabilities. WLAN risks that would affect Alliah are modern because the organization is a social media provider for young professionals. Professional information is critical; hence, it is likely the company may be subject to listing and measurement. The exercise involves the sensitivity of social media data that Alliah is privy to, connoting that it can be a target of surveillance. The second LAN vulnerability to the growing company is cross-site scripting, also known as XSS, because the product is provided as a web application. An AXSS worm that steals cookies, key logs, or port scanningcan attack Alliah’s network (Almarabeh, & Sulieman, 2019). The issues cannot be ignored and are equally devastating to any technology organization.

**Two Mobile Vulnerabilities**

The social media platform for young professionals that Alliah provides is linked to a mobile app that can be vulnerable to security vulnerabilities. One of them may be based on the design of the social media app, whereby professional users face privacy issues because the app is developed on their willingness to share personal details. The vulnerability may also be in the form of the inability of a user to delete messages from Alliah’s systems. The second mobile vulnerability is information disclosure because the app is designed as a social community that may lead to the reveal of location dataor an insecure framework that might allow SQL injections into Alliah’s systems via the app (Wüest, 2010). Nonetheless, the two issues are threats that the organization can combat successfully.

**Mitigation for the Identified Vulnerabilities**

Alliah can observe several measures that can help it to counter the vulnerabilities listed above. Firstly, it should combat listing and measurement. While it is a small organization with 35 workers, it can develop a social media policy backed up by enterprise-level security tools. Such a measure can protect its systems from surveillance by intruders that use personal information to develop profiles that can be used to cause harm. Alliah can also rectify cross-site scripting*.* The company must ensure that its web applications and WLAN environment is developed by leveraging the security development lifecycle. The exercise should involve a secure network to ensure that all data received by the organization is from a trusted source. The system should also be used for data, cookies, files and emails, to mention a few. Moreover, the organization can manage privacy and willingness to share personal data**.**Alliah’s mobile app can, by design, task people to share private data for their professional profiles, which might be a threat to the safety of their information (Neisse et al, 2016). The organizationmust secure the best encryption solutions in the industry to safeguard data entrusted to it. Lastly, the firm can control information disclosure*.* Alliah must deploy a mobile application firewall to protect users from sensitive information disclosure that, if leaked, could lead to disastrous outcomes such as fraud or identity theft. Alliah’s IT team must detect, block, or rewrite information before it can be inadvertently disclosed. The implementation of the steps above would be crucial in preventing the occurrence of the riks or mitigating their severity.

**Preventive Measures**

Several security options for small businesses such as Alliah can be employed in this scenario. Firstly, the 35 employees must be trained vigorously on security principles such as using strong passwords and other guidelines, and violation must be accompanied by penalties (FCC, n.d.). Robust security policies must be outsourced from industry-leading vendors, and the internal IT team must ensure that workers abide by them and are aware of elements such as password policies and incident response procedures. OS level security must also be examined in terms of deployment of patches, applications and services, as well as privileges. Ultimately, such measures can help prevent cases of attacks.

**Solutions for the Company’s BYOD Approach**

BYOD is encouraged in growing companies such as Alliah that do not have sufficient funds to cater for every device their workers use. In cases where employees bring their own devices, the company must enforce the following guidelines: use password-protected access control, manageWLAN and service connectivity, and monitor application access and permissions (Bello Garba et al., 2015). The company can, therefore, save money by not buying computer hardware for employees while keeping the work environment secure.

References

Almarabeh, H., & Sulieman, A. (2019). The impact of cyber threats on social networking site. *International Journal of Advanced Research in Computer Science*, *10*(2).

Bello Garba, A., Jocelyn Armarego, and David Murray. "Bring your own device organizational information security and privacy." *ARPN Journal of Engineering and Applied Sciences* 10, no. 3 (2015): 1279-1287.

Neisse, R., Geneiatakis, D., Steri, G., Kambourakis, G., Fovino, I. N., & Satta, R. (2016). Dealing with User Privacy in Mobile Apps: Issues and Mitigation. In *Protecting Mobile Networks and Devices* (pp. 81-106). Auerbach Publications.

Wüest, C. (2010). The risks of social networking. *Symantec Corporation*.