Security Planning and Risk Management for Twitter

**Security Planning and Risk Management for Twitter**

           Corporate organizations are at higher risks of cyber-attacks and hacking activities, where criminals may gain unauthorized access to the organization’s systems and sabotage their profitability and business continuity plan (Mital et al., 2016). These potential vulnerabilities and threats require strategic security and risk management plans by CIOs to ensure that the organizations secure their IT and data systems, and also continue with regular business despite these attacks. This paper highlights potential vulnerabilities of Twitter Social Network Company and how these threats and risks impact the company’s data and network management. It equally addresses the strategic mitigation plans to contain these threats and risks for proper security and safety.

**Potential Vulnerabilities and Threats facing Twitter Social Network Organization**

Recent research has indicated that the most affected on twitter are Android twitter users, and this vulnerability indirectly affects the company’s business strategies as well (Mittal et al., 2016).Some of the leading threats that twitter company is facing include password retention issues, input validation, unencrypted communication, inadequate testing, and exposed debugging information, among others. The question of users not letting people to help is another challenge with twitter users. On unencrypted communication (without SSL), Twitter must provide REST API methods as opposed to SSL. In some cases, there can be codes operating on untrusted network; it is advisable to use SSL for sensitive and authenticated requests.

**Describing the Risks involved with these Vulnerabilities (people, network, data, and reputation)**

These areas of threat/vulnerabilities lead to potential risks that affect twitter users, network, data management, and the general reputation of the company. If the threats are not mitigated in time, they breed risks on users by compromising their data and network access services. That is to say, users, network, and data will all suffer from unauthorized activities. On reputation, it will go a long way to adversely affect the fabric of the company and reduce its profitability in the global market.

**Impacts of the risks to the organization**

In the competitive global markets, users only prefer safer and protected services to assure them of data and network stability.As users get affected by the threats mentioned above, the company stands high chances of collapse due to significantly increased consumer apathy. For example, users only want to subscribe to network companies with tested and proven security systems so that their data and personal information can be safe at all times.

**Mitigation Plans for all the Vulnerabilities**

On threats of passwords,it is advisable for both company workers and users not to retain passwords for a long time. Instead, they must use OAuth tokens in possible cases and put other sensitive data threats under secure encryption. To mitigate input validation issues, Twitter Company must sanitize all data and check for valid file types and sane string lengths and so on (Sauerwein et al., 2018). On threats of inadequate testing, twitter must develop the attackers’ mindset to be ahead of any evil tests. Finally, Twitter must educate its users not to expose sensitive information on debugging logs or screens.

References

Mittal, S., Das, P. K., Mulwad, V., Joshi, A., &Finin, T. (2016, August). Cybertwitter: Using twitter to generate alerts for cybersecurity threats and vulnerabilities. In *2016 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)* (pp. 860-867). IEEE.<https://ieeexplore.ieee.org/abstract/document/7752338/>

Sauerwein, C., Sillaber, C., Huber, M. M., Mussmann, A., &Breu, R. (2018, September). The tweet advantage: An empirical analysis of 0-day vulnerability information shared on twitter. In *IFIP International Conference on ICT Systems Security and Privacy Protection* (pp. 201-215). Springer, Cham.https://link.springer.com/chapter/10.1007/978-3-319-99828-2\_15