Data Security Threat

Student’s Name

Institutional Affiliation

Professor’s Name

Course

Date

Data Security Threat

**Introduction**

Technology development has been a major milestone achieved by human beings. Through technology, people can improve the accuracy of a task, reduce operating costs and the time taken for any project. These factors are achieved through data collection. Data ensures that society is well informed and can use different lenses to study the past and predict the future through continuous trends or data analytics. However, data security threat has been classified as unintended consequences. Any data breach that affects a company has a major impact on the company's reputation, customer loyalty, market share, and financial statement. One of the greatest data breaches in history was experienced by Yahoo, where 3 billion user accounts were affected. The previous assignment focused on the shift in data security threats in social media platforms. The paper focused on the Twitter breach that occurred on 15th July 2020. This paper will evaluate how the research on data breaches and the writing has changed my understanding of the event.

**Changes that occurred**

The research on the event and the topic helped to increase my understanding. Previously, I only had a general idea of the attack and its sequence. The research on the event indicates that there were three phases of the attack. The first phase is stealing credentials and the administration log-in key through social engineering. The second phase involves accessing high-profile Twitter accounts, and the third phase is the high-profile bitcoin scam. The research also indicates the hackers accessed 130 accounts but only used 45 accounts for the scam. Previously, I thought that only the high-profile names were compromised since the headlines from different bulleting news indicated the six high profile members Barack Obama, Kim Kardashian, Jeff Bezos, Apple, Elon Musk, and Joe Biden (Hutchinson, 2020). Previously, I thought that the attackers used malware, phishing email, exploits, or backdoor to access the accounts. The research on the event helped me in identifying the real cause of vulnerability. The main issue was based on Twitter's Virtual Private Network, as employees worked remotely during the pandemic. The VPN had a problem, and hackers used the vulnerability to call and claim they were responding to the problem. There was also the use of phishing websites where employees were required to enter the details, and lastly, there was the generation of a false log-in generated MFA notification.

The research helped in creating a different perspective on data protection. There is a need for integrating different techniques in ensuring maximum protection of the system. I believe that there is a need to educate employees on data security and how to identify an authentic call from the head office. Provision of such education is important in ensuring that employees are well aware of the procedure to be followed in case of an attack. Network forensic shows that the first account that was compromised did not have access to the internal tools. The hackers we able to access the internal tool on 15th July (Twitter Inc. 2020). Therefore, educating employees about the process would have helped to identify the risk earlier. Some of the employees agreed to authenticate themselves through the use of MFA notification. This shows that most employees were not aware of the official number of communications. The company has various tools and techniques, such as two-factor authentication and data access control. These factors are considered effective in data protection. Therefore, employees should be considered in data protection, and companies should educate employees to address the vulnerability.

**Reconsidering my opinion**

Before the research, I believed that historical lenses are effective enough to identify possible channels that hackers can use. However, the research on the event indicates the need to conduct a simulation when there is an organizational change. The pandemic ensured that the government implements different policies that limited interaction between people. This also forced companies to implement policies that encourage telecommuting. Twitter was one of the companies that implemented this policy. The company was implementing a new culture in the shortest time possible hence the presence of vulnerabilities. Therefore, conducting a simulation will help a company to consider future occurrences and any vulnerability created while shifting the organization's culture (Twitter, 2020). The company could have realized that hackers can contact employees and request log-in credentials by simulating business operations. The department analysis indicated that there was no evidence the Twitter employees knowingly aided the Hackers. Rather, the Hackers used personal information about the employees to convince them that the Hackers were legitimate and could, therefore, be trusted.

**How the changes occurred**

The NBC news source had a major effect on my understanding. The article titled; *Twitter breach exposes one of tech's biggest threats: Its own employees* indicates how employees play a major role in a data breach (Chapman, 2020). Another supporting article indicates that social media data breach accounts for 56% of data breaches. This indicates that there is a need to analyze the issues in social media and identify the main issue. The research by Stanford University indicated that employees cause approximately 88% of data breaches. The statistical data provided by the two studies helped me to identify the issue. There is also a provision of a case study on how social media has affected company performance. An example is Alan Craig, who used Twitter to affect the stock of Audience Inc. and Sarepta Therapeutics. The policy violated by Alan is Section 10(b) of the Securities Exchange Act of 1934 and Rule 10b-5. There is a need to implement other policies that are in line with the current technological advancement. Another resourceful source is on network forensic of the company. The article provides details on the step-by-step process followed by hackers in acquiring the administrative tool. The details provided are critical in the implementation of better techniques to prevent future breaches.

By writing about the details of the event, I was able to understand the response approach from a Twitter perspective. Most news outlets indicate that there was a slow response from Twitter. The network forensic indicate that the response team was already investigating the incident after the calls and the takeover. Later, Twitter tweeted a statement saying it was "aware of a security incident impacting accounts on Twitter" and was "taking steps to fix it."(Twitter. (2020)) The step taken included preventing verified users from changing their passwords or tweeting. There was also a lockdown on accounts that had their password changed within the 30 days of the incident. One of the accounts affected through the process is the National Weather Service which failed to tweet a tornado advisory. The data access control strategy was improved as employees were denied access to the internal system and an aggressive verification process, including changing passwords. The company had restored most of the accounts within three hours.

**Conclusion**

The research on the Twitter data breach had a major impact on my understanding. The research included creating a synopsis from different sources. The approach helped identify what went wrong, how the hackers accessed the log-in credentials, the responses, the outcome, and possible regulation violation fines. Therefore, the research helped increase my knowledge of the event, the vulnerability present in two-factor authentication, and the need to conduct simulations in the diagnosis process. Therefore, the research helped me gain new perspectives on the research and reconsider some of my assumptions.

References

Chapman, G. (2020). Twitter breach exposes one of tech’s biggest threats: Its own employees. Retrieved 7 July 2021, from [https://www.nbcnews.com/tech/security/twitter-breach- exposes-one-tech-s-biggest-threats-its-own-n1234076](https://www.nbcnews.com/tech/security/twitter-breach-%20exposes-one-tech-s-biggest-threats-its-own-n1234076)

Hutchinson, A. (2020). Several High-Profile Twitter Accounts Hacked in Massive Security Breach. Retrieved 7 July 2021, from [https://www.socialmediatoday.com/news/several- high-profile-twitter-accounts-hacked-in-massive-security-breach/581705/](https://www.socialmediatoday.com/news/several-%20high-profile-twitter-accounts-hacked-in-massive-security-breach/581705/)

Twitter Inc. (2020). An update on our security incident. Retrieved 7 July 2021, from <https://blog.twitter.com/en_us/topics/company/2020/an-update-on-our-security-incident>

Twitter. (2020). *Twitter Investigation Report*. Department of Financial Services. Retrieved 5 August 2021, from <https://www.dfs.ny.gov/Twitter_Report>.