Research on Security Systems Used by Target

Student Name

Institution Affiliation

Research on Security Systems Used by Target

Up to date, the Target company has not yet disclosed how the attack on the company's network system took place. However, through other credible sources, we can understand how the firm got attacked and the vulnerabilities that existed initially. These vulnerabilities enabled the phishing of critical data from the central servers of the firm. According to Hoffman & Gold (2015), the breach was initiated at a third-party Vendor called Fazio Mechanical service. The breach was a procedural attempt that the hackers did with utmost patience as discussed below.

The hackers first compromised the security systems of the Fazio mechanical service. This phase was vital as it gave them access to the domain network of the Target Corporation. According to Nolen (2018), the penetration was through Fazio Mechanical Service that deals with heating systems. However, it is unclear if Fazio was still a target or not.

Consequently, the hackers got access to the network through the vendor. They investigated the system to find any vulnerabilities within it. Two vulnerabilities gave them an entrance to the company’s database. According to Hoffman & Gold (2015), the point of sale security was so simple that it would allow unauthorised access to any software. The other one was that the segmentation of the network. The network was so basic and general that it failed to separate the sensitive domains to the less sensitive ones. For example, the domain that contained the consumer credit card information was supposed to be secured with more complex data security measures than any other Target firm branch.

The hackers used a Citadel Trojan virus to be able to mine data from the firm. The virus gave the hacker full range power to take over the network making the phishing process way more comfortable. Moreover, poor network segmentation was an additional advantage for the easy penetration of the Trojan virus. According to Heagney (2018), a specific Trojan virus was

required to attack the business section. This section was vital as it contained the data that the hackers were after and intended to use to cause mass destruction.

Once the Trojan got installed in the servers, it started to send the data to an unspecified server whose location piggybacked to Russia after investigations. The data that was being sent got encrypted after being extracted from the point of sale. According to Nolen (2018), the hackers used a backdoor username and password. The data encryption was vital as it protected the hackers from being noticed by a traditional windows security feature.

There are weaknesses that the hackers exploited to take over the firm's network system. The first one is that the firm did not apply proper access controls to the network system. According to Pigni et al. (2016), it was possible for the third-party personnel to access vital information that was supposed to be limited to the top management of the frim. It, therefore, came as an advantage to the hackers making it easier for them to infiltrate the system from the outside.

As stated earlier on, the point of sale allowed unauthorised access to software. The point of sale terminal allowed hackers to read sensitive information from debit and credit cards. The software, therefore, understands this data, encrypted it from the source and sent it to the hackers. According to Pigni et al. (2017), the Trojan virus Black POS encrypted the information that was collected from the credit cards and stored them in the file destination "C:nWINDOWSnsystem32nwinxml.dll". It should be noted that all of this happened without recognition by the internal Information Technology experts.

The experts ignored vital alerts on security. It is a weakness that was caused solely by the ignorance of the monitoring team. According to Pigni et al. (2016), the monitoring team even went as far as switching off the functionality of the Fire eye software that would have detected

and eliminated malware. They switched off the feature probably because it gave a lot of alerts that the team did not take into serious consideration.

The last weakness is related to the segmentation of the network. The initial design of the system was basic. The firm applied a VLAN approach which is so easy to bypass. It failed to isolate sensible systems from easily accessed ones. The hackers used the easy access section to be able to take control of the net. They used the vendor credentials to access the business section since the network boundaries were not clearly defined. To be able to secure a network, the border must be clearly defined.

The target suffered a catastrophic loss of both data and money after the hack. Revenues were lost, and trust from the firm by consumers dwindled. However, the firm has since recovered from the loss and has put strategies to secure their data. From the above analysis, there are few recommendations that the firm should consider while setting up the security systems.

The firm should establish an integrity payment system. A system that would not allow the access of credit card information by a third party while reading the credit card information in the point of sale terminals. Since the data is stored in a network server, the flow of data within the network system should be monitored closely and continuously to know what kind of data is getting into the system and what type of information is flowing out.

The security personnel put in place should be able to carry out around the clock surveillance of the system. The staff should be qualified enough to know that any alerts made by the system are vital and should be checked out. The firm should also develop effective security alert system that would seek attention and revoke other activities until the problem is solved.

In conclusion, data security for the Target requires close attention on the segmentation of the network, the point of sale access and the focus to security alerts. Without implementing such

security measures, the company's servers will continue to remain vulnerable to any hacker with the knowledge on how to bypass its current security system.

References

Heagney, G. (2018). *Target Corporate*. A Bullseye Views. Retrieved 8 October 2018, from https://corporate.target.com/about.

Hoffman, A., & Gold, N. (2015). Target Corp's Tarnished Reputation: Failure in Canada and a Massive Data Breach. doi:10.4135/9781526429308

Nolen, J. (2018). *Target Corporation | American corporation*. *Encyclopedia Britannica*. Retrieved 8 October 2018, from https://www.britannica.com/topic/Target-Corporation

Pigni, F., Bartosiak, M., Piccoli, G., & Ives, B. (2017). Targeting Target with a 100-million-dollar data breach. *Journal of Information Technology Teaching Cases*, *8*(1), 9-23. doi: 10.1057/s41266-017-0028-0