Case Study on the Target Data Breach

At the age of information, the security of data is the foundation of a modern organization. Companies cannot guarantee they will not be attacked, so the more important thing is how to decline the number of attacks and average loss. Analyzing the typical examples are very helpful to improve the cybersecurity mechanism. In 2013, the retail giant Target occurred a serious security incident of more than 100 million personal data breach that led to massive loss of profit and reputation. I will analyze why it happened and how to deal with such issues.

The hackers started their invasion from Fazio Mechanical Services as the third part of Target. And then attackers utilized verification information from Fazio to move into the Target’s payment system since there were no segments between vendor systems and core systems. Why could hackers get the username and password so easy? Fazio used a free version of antivirus software. The cause of core problem was where the party who is in a position to protect a system is not the party who would suffer the results of security failure, then problems may be expected (R Anderson, 2001). As a heating and ventilation provider, Fazio did not think they could be the target of attack. Moreover, as a result of this incident, the focus of the offense was indeed not on them. So as the victim, Target should require third even fourth parties to improve security protection level. Let them know that they should take responsibility for the client’s security. Second, there is only one firewall to isolate internal and external. Once someone breaks into the internal network, he can get everything.

Known vulnerabilities will continue to dominate (John Pescatore, 2017). The same thing is still happening all the time no matter before or after. The target was not immune. At least seven months before the attacks, in April and again in August 2013, Visa had published alerts to retailers detailing security vulnerabilities to the RAM scraper malware (D. filed Aug. 25, 2014). The top management ignored this issue. It is an easy way to find out defects and how to void errors occurred if you know the aftermath. But before the data breach, the security team may receive a bunch of warnings daily. It was reasonable that security officials wouldn’t address every issue in time because of limited cost. Also, people will get bored if they think such jobs like the bug fixed are useless since attackers would not exploit a vast majority of vulnerabilities successfully. Subsequent investigation even found that there was a system function that could prevent attacking but was turned off, and no one knew the reason. Such issues illustrated that security management in the company was not robust. They did not pay attention to the role of the protection system. Many repeated and checking jobs of data could be done by the system since the machine would not feel bored and tired when they do these jobs. The system can handle many problems automatically if the company makes the best of the protection system. Also due to the classification of warning levels by the system, the staff can focus on some serious issues. Therefore new technology such as machine learning, big data analysis can help the security team exclude large amounts of low-level risks.

In this case, Target didn’t have a sound emergency response mechanism. The company got information about the data breach was December 12. However, they started to remove the malware on December 15. These two or three days had more customers’ information leakage. More important, they were not planning to inform customers about this issue at the first time. Many people found their credit cards fraud. In general, there is no way to void attackers all the time. So companies should have a comprehensive security process plan to address the problem quickly and efficiently and reduce data loss. When some problems occurred, the company should put customer’s interests on the top to let them know the seriousness and help them prevent damage as soon as possible.

In conclusion, a successful attack needs to meet many conditions. Maybe in this incident, attackers sent tons of emails to different companies. Several letters were clicked by workers. Few companies could not detect the malware so that the hacker got username and password. Then hackers tried every username and password to find that Target was their target. According to the small probability of event occurred, many companies think they are safe enough. However, with the advent of autonomous hacking machines, every company could become a victim. The company should build a comprehensive solution for cybersecurity including from management to ethic, from human beings to AI.

References

Ross Anderson, Why Information Security is Hard – An Economic Perspective,(2001) **ISBN:** 0-7695-1405-7

John Pescatore, 2017,Cyber Security Trends: Aiming Ahead of the Target to Increase Security in 2017

In re: Target Group. Customer Data Security Breach Litigation, No 0:14-md-02522, Complaint (D. filed Aug. 25, 2014)