Case Study on the Target Data Breach

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

The hackers started off their invasion from Fazio Mechanical Services as a third part of Target. And then attackers utilized verification information from Fazio to move into the Target’s payment system since there were not segments between vendor systems and core systems. Why could hackers get the username and password so easy? This is because 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 attack was indeed not on them. So as the victim, Target should require third even fourth party to improve security protection level. Let them know this is also what they should take responsibility. Second, there is only one wall to isolate internal and external. Once someone breaks into internal network, he can get everything.

Known vulnerabilities will continue to dominate (John Pescatore, 2017). It seems that the same thing is still happening all the time no matter before or after. 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 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 could receive a bunch of warnings daily. So security officials won’t address every issue in time because of limited cost and people will get bored if they think such jobs like bug fixed are useless since a vast majority of vulnerabilities would not be exploited by attackers. Even more disappointing is a system function that could prevent attacking was turned off and no one knew the reason. I mentioned above 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 system since machine would not feel bored and tired when they do such job. Due to the classification of warning levels by the system, human can focus on some serious issues. Therefore new technology such as machine learning, big data analysis can help security team exclude large amounts of low level risks.

Reference

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