**Cyber Security Threats, Vulnerabilities and Risk**

Nabin Poudel

1. INTRODUCTION

Nowadays technology has become an indispensable part of our lives. People are relying more on technologies to perform their daily tasks. Every machine has some vulnerabilities, that if, exposed can cause severe consequences. In computers and computer networks an attack can be described as an attempt to expose the vulnerabilities in the network of system or destroy and steal something from the system by gaining unauthorized access. Likewise, cyberattacks can be described as an attempt to target computer information and infrastructure to gain some benefits. The people involved in these attacks are known as attackers. They try to access data, restricted sites or confidential information without authorization. Cyber-attacks can be a part of cyberwarfare or can be very severe that can be described as cyberterrorism and is punishable by law. These attacks can be employed by individual groups, a person, and an organization [1]. Sometimes even the states are involved in cyberattacks as well. Due to the advancements in technologies attackers are also becoming advance making cyberattacks increasingly dangerous and sophisticated. There are several types of cyberattacks but the most prominent attack that came under the spotlight recently is ransomware attack. It is a type of an attack in which attackers target computers that are running Microsoft window operating system. They encrypt the data and demand ransom payments in the form of Bitcoins [4]. Several leading companies were affected by this attack as most of them were not prepared for this attack. This attack causes companies to lose millions of money as they had to pay the attackers. This paper will explain ransomware attacks by utilizing an example of a real-life company that was under the ransomware attack. Furthermore, the paper will discuss potential reasons for an attack, the amount of loss that a company suffered and the countermeasures that were taken to address the attack.

1. CYBERATTACK ON TOYOTA AUSTRALIA

Toyota is a Japanese automotive manufacturer that was founded on 28 August 1973. According to the statistics of 2017, it is one of the largest automotive manufacturers. It is also the world’s first automotive company that manufactured almost 10 million vehicles per year. Specifically discussing hybrid electric vehicles Toyota is considered as a leader of the world’s market sale of these vehicles. Toyota has several branches in many countries such as Australia, USA, Singapore, etc. Also, they have multiple branches in almost every city in each country. As Toyota is considered as one of the leading cars manufactures it therefore automatically became the priority target of the hackers. This is because hackers know that a company with high reputation will pay more to save their reputation. Also, hacking a reputable company and leaking the data can cause severe damage to the Company’s reputation while impacting their business in the global market.

Recently, Toyota Australia has suffered a cyber-attack due to which they faced severe consequences. One day on 21st February 2019 the employees at Toyota Australia complained that they are unable to login their emails. After some time they complained that they cannot even reach their phone as well. This raised concerns as even the company website was unreachable due to which they were unable to do business. The first step the IT department took was to inform all clients that they had some technical issues and they are constantly trying to fix these issues. After this, they start investigating the real cause of the problem. It was later identified that the company has suffered from a cyberattack. The shocking part was that on the same day a non-profitable hospital was also under cyberattack due to which they lost patient’s files that were extremely confidential. Initial reports suggested that the source of these attacks are from Russia or North Korea. Due to several speculations the Carmaker Company released a statement in which they accepted that they have suffered a cyberattack due to which clients’ data was lost however personal details of the clients are still protected. Although this time the company managed to combat the attack but again in May 2019 Company suffered a major data breach in which they lost the personal data of over 3.1 million customers and the only way to recover the data was to use some backup or to pay the money to the attackers.

1. ATTACKERS

Several factors contribute to cyber-attacks such as spectacularity factor, vulnerability factor and fear factor. The spectacularity factor can be described as the attack that causes direct losses while gaining negative publicity. The vulnerability factor can be described as an exploitation of the vulnerability of an organization’s security system. The last factor is the fear factor which involves fear of being hacked by the hackers [5]. While discussing the sources of attacks, an attack can be caused due to human error, system faults and malicious attack. There are several types of attacks such as botnet attack, syntactic attacks, denial of service attack, etc. However, the attack that has gained the spotlight in recent years is ransomware attacks. Ransomware attacks are behind 56% of malware attacks. Due to the raising concerns regarding data privacy and loses that occurred because of ransomware attacks many countries have found ways that can help combat the attack. In Australia, according to the Australian Information Commissioner, there were only two cases of ransomware attacks out of all the cybersecurity attacks that were reported in 2018.

Ransomware attacks can be described as a malware that threatens to leak the victim’s data or block their access to their account unless a ransom is paid in the form of Bitcoin cryptocurrency [4]. Typically, these attacks are carried out by using Trojan that is camouflaged as a legitimate file. Users fell prey to the trap and end up downloading or opening the file containing a virus. WannaCry ransomware attacks also known as high-profile ransom attacks are the cyberattacks in which the attacker target the computer that runs Microsoft windows operating system. The attackers launch the attack by using the WannaCry ransomware crypto-worm to gain access over computers [3]. After accessing the data hackers demands ransom payments in Bitcoins. This type of attack can spread itself in the system. It first checks the “Kill Switch” domain name and f the name is not found then the ransom encrypts computer’s data while attempting to exploit SMB vulnerability. Several companies have become a potential target of this attack that made them lose a massive amount of customers’ data.

Specifically discussing Toyota Australia, the company was targeted not once but twice in the same year. Initially, the company linked the attack to the Russian or North Korean hackers yet later it was identified that a group known as ATP 32 is involved in cyberattacks. The ATP 32 is a Vietnamese hacking group that is also known as Ocean Lotus group. This group is known for its sophisticated attacks on several private national and international companies, government agencies and journalists. This group started hacking Chinese entities in 2012 and then expanded across Asia and other continents. This group targets the most confidential information of the people and clients associated with specific organizations. As companies will do anything to keep their clients' information anonymous and will pay a huge ransom to get back the stolen data.

ATP 32 group was also behind the attack on Toyota Australia. The company was attacked not once but twice. The second attack was after a few weeks of the first attack. It was estimated that that almost 3.1 million customers data have been leaked due to the security breach. Previously, the breach occurred in Toyota Company Australia branch but the second attack occurred in the company’s head office that is in Japan. This was alarming as even the head office was not safe. The attack that occurred in the Australian branch was very severe and disruptive. As due to the attack Toyota Australia Company was unable to handle sales and delivery of the vehicles to the client. After several investigations, it was revealed that a notorious group known as ATP 32 was behind these security breaches. They used a combination of both open-source tools and some custom-build tools to breach the company. Following the breach, the company released a press statement that only the client’s personal information was stolen and their credit card details are still secure. Specifically, the Lexus car owners are more at risk as most of the information was stolen. After the Australian branch attack, the company is focused more on doing an internal audit of the IT department. Also, they are trying to build firewalls strong enough to combat cyberattacks.

1. SECURITY RESOLUTIONS

Toyota Company has suffered data breach twice which is alarming. It also highlights that the company lags at security and major interventions are needed to ensure the security of the data. The first thing the company should do is to accept the problem as most leading companies remain in denial that their security system has vulnerabilities. It is, therefore, necessary that cybersecurity training is conducted regularly so that every employee must be aware of the potential threats. Secondly, internal auditing and documentation are important this will ensure systems security. Additionally, the company should review their security policy by including a NIST framework. According to this framework, it is necessary to first identify a threat then protect system using several counter mechanisms. The next function is to detect in which an organization must identify the threats by monitoring the solutions that detect anomalous activity. The fourth function is responding which imply that an organization must create a response plan in case of an attack. The last function is recovered according to which the company must have a recovery plan to restore all the material that was exposed to the threat or attack [6]. Another model that help mitigate the attack is a SAFE model that comprises of three phases. The first phase is the capability phase in which security capabilities based on potential threats are analysed and applied to address attacks. The second phase is an architectural phase in which a security architecture is defined utilizing security capabilities. While the third phase is the design phase in which using security architecture a design consisting of cost, configuration and product list is created. All these security resolutions can help in combating any future attacks [7].

1. CONCLUSION

Due to the rise in technologies cyberattacks are prevailing widely. Therefore, there is an immense need to have strategies and policies that can mitigate the attacks. Cyber-attacks can be a part of cyberwarfare or can be very severe that can be described as cyberterrorism and is punishable by law. These attacks can be employed by individual groups, a person, and an organization. Recently, Toyota Australia suffered a major data breach due to which almost 3.1 million customer’s data was hacked. This raised several questions on the security system and policies of the company. However, after suffering from immense loss company also made several interventions not only in their security policy but in their security system as well. This will ensure the company’s data security and help in combating several security attacks. By looking at the case of Toyota Australia, every company must be prepared for cyberattacks by making new strategies and educate its employees regarding the importance of cybersecurity.

1. REFERENCES

[1] K. N. Sevis and E. Seker, "Cyber warfare: terms, issues, laws and controversies," *2016 International Conference On Cyber Security And Protection Of Digital Services (Cyber Security)*, London, 2016, pp. 1-9.  
URL: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7502348&isnumber=7502334>

[2] A. Alzahrani, A. Alshehri, R. Alharthi, H. Alshahrani and H. Fu, "An Overview of Ransomware in the Windows Platform," *2017 International Conference on Computational Science and Computational Intelligence (CSCI)*, Las Vegas, NV, 2017, pp. 612-617.  
URL: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8560864&isnumber=8560703>

[3] A. Chuquilla, T. Guarda and G. Ninahualpa Quiña, "Ransomware - WannaCry Security is everyone's," *2019 14th Iberian Conference on Information Systems and Technologies (CISTI)*, Coimbra, Portugal, 2019, pp. 1-4.  
URL: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8760749&isnumber=8760589>

[4] S. R. Kumar, S. A. Yadav, S. Sharma and A. Singh, "Recommendations for effective cyber security execution," *2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH)*, Noida, 2016, pp. 342-346.  
URL: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7542327&isnumber=7542293>

[5] A. Ferreira, "Why Ransomware Needs A Human Touch," *2018 International Carnahan Conference on Security Technology (ICCST)*, Montreal, QC, 2018, pp. 1-5.  
URL: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8585650&isnumber=8585426>

[6] N. Teodoro, L. Gonçalves and C. Serrão, "NIST CyberSecurity Framework Compliance: A Generic Model for Dynamic Assessment and Predictive Requirements," *2015 IEEE Trustcom/BigDataSE/ISPA*, Helsinki, 2015, pp. 418-425.  
URL: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7345310&isnumber=7345233>

[7] “SAFE Overview Guide: Threats, Capabilities, and the Security Reference Architecture,” http://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/designzone-security/safe-overview-guide.pdf