THINK INDIA JOURNAL

ISSN:0971-1260

Vol-22-Issue-40-December-2019

Study of Cyber Security in Social Media

Sweta R Kumar[1] and Gulabchand K. Gupta[2]

[1]Research Scholar, Shri Jagdishprasad Jhabarmal Tibrewala University, Jhunjhunu, Rajasthan

[2]Seva Sadan College of Arts, Science & Commerce, Ulhasnagar

Abstract

Social Media are the virtual platform where people share their personal information with their known and unknown friends. Cyber-attacks are a sort of offense that helps the hackers to steal the personal information and can extend from introducing spyware in the network or the nodes. A greater part of current assaults essentially utilizes the social media as a conveyance system that breach users authentication and credentials. This calls for progresses in security conventions to shield against programmers which structure the premise of this examination. In this paper, we will discuss a portion of the threats and security concerns and assaults on Social Media.

Keywords- Social media, security, communication, Cyber attack

Introduction

Social media communication sets up interconnected online networks which is the act of growing potentially social contacts or business by making associations through people, regularly through web-based life, for example, Face book, Twitter, LinkedIn.

Social media is generally two types of network like sociocentric and egocentric. The sociocentric targets on huge gatherings of individuals and evaluates the connections between individuals in a gathering in and considers examples of collaborations and how these examples influence the gathering all in all.

Cyber security is the basic necessity for social networking sites as today the world is totally managing the data and is shared anywhere in various structures. The information in some cases is very delicate and can be abused by anybody. To be sure when organizations and associations share delicate data, they ought to ensure that, it is basic to keep the information safe. Besides when government, military, banking and different associations work with information, it must be taken well consideration. This is the place Cyber security has a spot as a significant factor. Digital security can be basically said as an instrument of securing any data by utilizing most recent advancements so that they can't be utilized by any other individual other than to which individual it belongs to. According to Barnes, the ubiquity of these social media, which are frequently utilized by young people and individuals who don't have protection or security on their psyches, prompts an immense measure of conceivably private data being set on the Internet where others can approach it. It also proceeds to state that connecting with individuals isn't new, however this media for doing it is generally new. The crime on social media is wil increasing very fast.

Security process includes mainly people, technology and processes as it is dynamic and adaptive. People in this process are the users who should be aware of all the risks of cyber threats and must have the proper data backup and other are the security personnel. The process helps people how to react to the threats. Technology are the tools that helps the procedures to work together. [1-3]

Significant Security Area

It tends to stay aware of the changing security dangers. The customary methodology has been to concentrate assets on vital framework segments. Now a day cyber security requires the coordination through a data framework as- Application security which is an unauthorized code which is used to manipulate the content, Network security that detects and responds as per the security policies and tools to the threats, Information security and Operational security.

Security Threats in Social Media

1. Deep Fakes

ISSN:0971-1260

Vol-22-Issue-40-December-2019

Deep fakes are deep learning that is basically machine learning based on artificial neural network. In this procedure the video or image of an existing person is replaced or combines the existing media using machine learning techniques. Generally, there are large number of data like images and videos of celebrities and politician. These data are used to change the faces of personnel and create photo realistic videos and images which are targets of deep fakes.

Deep fakes are threatening to the security of the world that can affect the political tensions, fake speeches, financial market and fool the public. Positive impact can also be there by deep fake in the shooting or recording the voices.

2. Ransom ware

It is a type of malware that blocks the public data and manipulates it without their knowledge and stops accessing the user their data till the ransom amount is arranged. Ransom ware is mainly used for high yield revenue purpose and as per the statistics and as per the statistics of Safeatlast.co [4&5].

3. Social Engineering

The human interaction to unauthorized access to the sensitive information which is protected. Different types of social engineering attacks are baiting, scareware, pretexting, spare phishing.

4. Malware Malwares are the applications which are introduced in the users gadgets without the information and client consent. These spreads very quick and causes security abandons in the product infections, worms, and Trojan steeds are instances of malevolent programming.

5. Phishing Phishing is a sort of social designing normally utilized to take client information, for example, Mastercard numbers and login credentials. It happens when an aggressor, acting like a confided in singular, deceives the injured individual to open an instant message, email, or text. This breach can have grievous outcomes. For an individual, this incorporates data fraud, taking of assets, or unapproved buys.

6. Exploitation of IOT Security The growth of IOT devices implementation is very fast and it takes only five minutes to hack the device as per the NETSCOUT report after connection to internet. As per Kaspersky Labs report there were over 105 million attacks on IOT devices in first six months of 2019 which was nine times the statistics of 2018.

Cyber Attack Anatomy

- The cyber attacker enters into the organizational network or application and inserts the malware. The objective is presently undermined.
- The additional network access is reviewed by the advanced malware to communicates with command and control websites to receive additional malicious code.
- The malware normally sets up extra break focuses to guarantee that the digital assault can proceed in the event that one point is shut.
- When a risk on-screen character has built up arrange get to he/she starts to assemble information, for example, account names and passwords. When the assailant breaks the passwords, he/she would now be able to can recognize and get to information.
- Information is gathered on an arranging server, at that point the information is exfiltrated. An information rupture is presently happening.
- Proof of the digital assault is expelled, however the association is still undermined and the digital criminal can return whenever to proceed with the information rupture.[6]

Conclusion

Social media stores large amount of data around various servers having different layers of security. Hence the significant rise new technology advancement like Internet of Things, cloud computing, Artificial Intelligence and 5G in social networking world will lead vast information to the user on finger tips but at the same time large amount of new security risks. In this paper we discussed about various types of security

ISSN:0971-1260

Vol-22-Issue-40-December-2019

threats and anatomy. It is assumed that many organisations have also started targeting customers through social media and the concern is the user's data security for which different cybersecurity methods need to be improved. It is concluded that we should educate and update the users about the cyber security and mitigate security risk of the present and future.

References

1. https://digitalguardian.com/blog/what-cyber-security
2. Barnes, S. (2006). A privacy paradox: Social networking in the United States. First Monday, 11(9). doi:10.5210/fm.v11i9.1394
3. https://www.techopedia.com/6-cybersecurity-predictions-for-2020/2/34130
4. https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf
5. https://safeatlast.co/blog/ransomware-statistics/#gref
6. Bendovschi, A. (2015). Cyber-Attacks – Trends, Patterns and Security Countermeasures. *Procedia Economics and Finance*, *28*(December 2015), 24–31. https://doi.org/10.1016/s2212-5671(15)01077-1
7. Kumar, A., Gupta, S. K., Rai, A. K., & Sinha, S. (2013). Social Networking Sites and Their Security Issues. *International Journal of Scientific and Research Publications*, *3*(1), 2250–3153. Retrieved from www.ijsrp.org
8. Ghari, W. (2012). Cyber Threats In Social Networking Websites. *International Journal of Distributed and Parallel Systems*, *3*(1), 119–126. https://doi.org/10.5121/ijdps.2012.3109
9. Kumar, A., Gupta, S. K., Rai, A. K., & Sinha, S. (2013). Social Networking Sites and Their Security Issues. *International Journal of Scientific and Research Publications*, *3*(1), 2250–3153. Retrieved from www.ijsrp.org
10. Computer Networks, 5e (5th Edition) by Andrews Tanenbaum,David J.Wetherall by Pearsons Edition.
11. Computer Networking: A Top-Down Approach by Kurose James F. (Author), Ross Keith W. Pearsons Edition.
12. Data Communications and Networking by Forouza Indian Edition.