Ilkogretim Online - Elementary Education Online, 2021; Vol 20 (Issue 4): pp. 3830-3836
http://ilkogretim-online.org
doi: 10.17051/ilkonline.2021.04.419

An Analysis Of The Problems And Issues With Cyber Security

Sanjiv Kumar, Computer Science and Engineering, Graphic Era Deemed to be University, Dehradun, India sanjivdunmca@gmail.com

Harendra Singh Negi, Computer Science and Engineering, Graphic Era Deemed to be University, Dehradun, India, harendrasinghnegi@gmail.com

Kamlesh Purohit, Computer Science and Engineering, Graphic Era Deemed to be University, Dehradun, India, kamleshpurohit80@gmail.com

Sunny Kumar, Department of Computer Application, Graphic Era Deemed to be University, Dehradun, India sunnykumar250198@gmail.com

Aanchal Sharma Lamba, Research Scholar, School of Management, Graphic Era Hill University, Dehradun.

Abstract— Cyber security plays a key role in the realm of information technology. The requirement for extra information is one of the principal problems of the present. When talking about cyber security, the phrase "cyber warfare" immediately comes to mind, and it is getting worse every day. Many governments and companies are waging a determined battle against cybercrime. Despite several efforts, cyber security continues to worry a lot of people. This essay focuses on the vulnerabilities that the most recent technologies have in terms of online security. It also emphasizes ethical issues, contemporary cyber security techniques, and the adaptability of online security.

Keywords—cyber security, phishing, cyber crime, malware.

I. Introduction

Anyone may transmit and receive any kind of data, including audio, video, and email, with the touch of a button, but have you ever been concerned about how securely your data is sent to another party in the event of a data leak? The answer lies in online security. The internet is a component of modern life that is rapidly developing. Today's modern technologies make it possible to change someone's appearance. Given that these new technologies make it difficult for us to adequately protect our personal information, cybercrime is currently on the rise. This industry needs a high level of security for tasks that go above and beyond because more than 60% of all purchases are now made online. Thus, there has recently been anxiety over internet safety. Internet security protects both information access in the IT industry and other domains, such as cyberspace. Even today's most cutting-edge technological advancements, including cloud computing, mobile computing, net banking, e-commerce, etc., require a high level of security. Because these technologies include some crucial information about a person, their safety has become crucial. Improving cyber security and protecting vital information infrastructure are essential for the security and economic success of every country. The creation of new services and governmental initiatives now include provisions for increasing internet security (and safeguarding users of the network). Cybercrime is widely and safely being fought. Given that technology measures alone cannot completely prevent crime, we must create the necessary conditions to effectively investigate and prosecute cybercrime. To prevent the loss of crucial data, many governments and nations today have strong regulations in place for internet statistics. Everyone should learn about cyber security to protect them from the rising tide of online crime. Social media's intrinsic characteristics make users become accessible targets for online crooks. Organizations are expanding their IT budgets in order to protect social networks worldwide. On the social network, members produce and distribute a staggering amount of information. Adopting a new set of tools and procedures is crucial for protecting online data and resources via social networks. As new technologies like IoT and Big Data continue to advance, so do new risks and difficulties. [1] Incidences of spear phishing, which involves installing dangerous malware on the targeted users' computers and obtaining sensitive and important information, are also rising. The virus that has been used can encrypt data on network drives, databases, and backups, which could do catastrophic damage to the target company. Malware may be spread through advertisements on well-known websites. State actors are increasingly using digital means to achieve their strategic goals, as well as to halt or assist wars, as highlighted by intelligence agencies once more. [2] Through cyber theft or cyber espionage, cybercriminals use a person's financial, personal, or private information. Through the use of botnet software, the crooks are seeking to take over certain systems. In actuality, it is true that successful cyber attacks routinely jeopardize the privacy, accessibility, and reliability of Internet-based information systems and their data. [3]

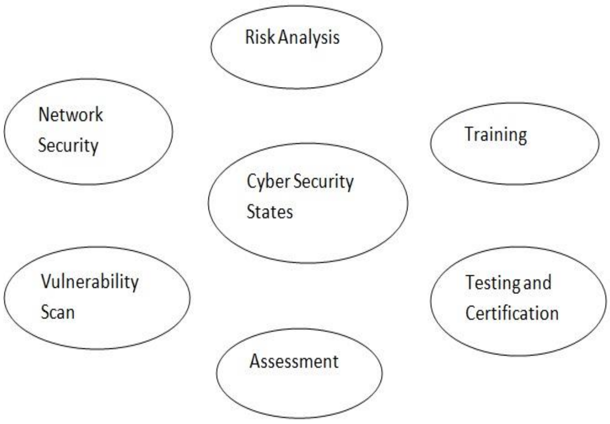

Fig. 1. States of Cyber Security

II. THREAT TYPES IN CYBERSPACE

A cyber attack is a criminal act that targets communications systems, applications, devices such home computers, or datasets like communication networks and data centers [4]. A cyber criminal could be an individual or piece of software that seeks to gain unauthorized access to system data or functionalities with malevolent intent [5]. Here are a few of the most common attack.

Malware: Threat to Microsoft systems is malware. This abbreviation stands for harmful software. Malware is created with the intention of harming a server, network, or PC with Microsoft software installed on it. Malware comes in several forms, including viruses, worms, and malware. The spread of a computer worm involves reproduction. A virus is a piece of code that infects another program's code and drives it to carry out malicious actions and spread itself. A Trojan, which is unable to reproduce itself, impersonates a desired item and lures the user into activating it. Then it can spread and cause damage.

Phishing: Phishing is the practice of sending customers fraudulent emails to induce them to divulge personal information such as bank usernames, OTP, credit card numbers, etc.

Denial of Service: A brute-force assault known as a Denial of Service denies users access to an online service. For instance, cybercriminals could overwhelm a system's functionality by sending a website or database a lot of requests, keeping it busy and unavailable to visitors. In a distributed denial of service attack, the targets' traffic is hijacked using a large number of machines, typically infected with malware and under the control of cybercriminals.

Cryptojacking: An attack known as "cryptojacking" uses the victim's computer to produce cryptocurrency. To complete their transactions, the attackers frequently install malware in the target's PC.

Ransomware: A type of malware called ransomware encrypts the files on the target system. The target is then asked to pay the attacker a ransom in order to recover access to the data. The payment instructions for receiving the decryption key will be issued to the victims. Costs range from a few hundred to thousands of dollars, and fraudsters typically demand payment in bitcoin.

III. REASONS FOR VULNERABILITY

Basic cyber security issues, such as out-of-date software, might be more serious than other issues, such as a lack of management team support. Cross-site scripting, outdated software, insecure protocols, weak passwords, and missing system patches are the top five most common enterprise vulnerabilities. The entry point for attackers to more deeply infiltrate a corporation, on the other hand, has been characterized as phishing attempts. Here are a few additional problems that put a company at risk [6]. The top security measures that a corporation cares about are data privacy and security. All information in the world we currently live in is stored digitally or online. On social networking sites, users can interact with friends and family in a secure setting. Cybercriminals that use social networking sites to steal personal information will continue to target domestic consumers. When using social media and doing bank transactions, one must take all necessary security steps. 98% of businesses retain or improve their internet security measures, and of those, 50% increase the services they offer to protect against cyber attacks. Cyber attacks were identified as the fifth most significant global danger in the World Economic Forum's report on Global Security Risks in 2020 [7], [8]. According to a 2019 FBI report [9], cybercrime costs the United States more than $350 million. Cyber attacks have impacted almost every industry. The most severely impacted industry is finance, with yearly expenditures exceeding $1.2 billion in 2018 [8]. In order to determine the expenses and industry-specific makeup of the approximately 10000 cybercrime that occurred between 2004 and 2015, Romanosky et al. conducted an analysis [10].

IV. TROUBLES WITH CYBER SECURITY

In a ransomware assault, a malicious program infiltrates our system and encrypts all of our data. The system then locks all of its files. Only once a ransom has been paid will the decryption key be sent. [11]. General Data Protection Regulation regulation protects the personal information of EU people. All businesses who handle consumer data, process data for other EU businesses, or have offices in an EU nation are impacted by its implementation. Because the costs outweigh the risks, many businesses will not attempt to comply with the requirements. [12]. A network-connected collection of electronic gadgets is known as the "internet of things." This offers users access to the majority of linked devices from a single point of control, which could increase the danger of an attack. Botnets, DDoS assaults, and ransomware attacks are a few issues with IoT [13]. Sensitive data is stored in large quantities on cloud platforms. Cloud misconfigurations, specter and meltdown vulnerabilities, the use of less secure APIs, and data loss are a few of the difficulties [14]. Artificial intelligence and machine learning may be used to carry out a variety of assaults, including password guessing and the usage of chatbots to deliver more spam messages [15]. Since cryptocurrency technology is still in its infancy, many businesses cut corners on security measures. Strikes in this category include the Sybil, Eclipse, and DDoS attacks [16].

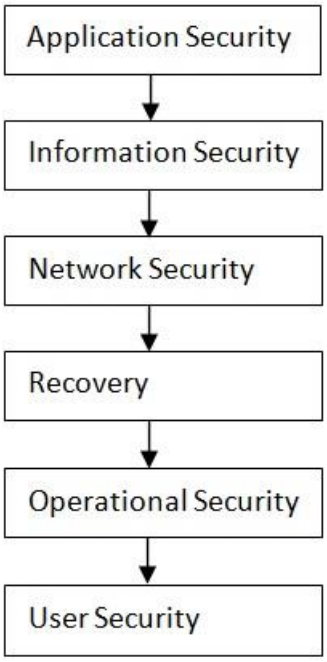

Fig. 2. Elements of Cyber Security

V. ROLE OF SOCIAL MEDIA IN CYBER SECURITY

Businesses must come up with creative solutions to protect client information in an increasingly social and connected world. Social media has a big role in cyber security and will have a big impact on individual cyber risks. Both the use of social media by people and the threat of attack are rising quickly. Social media and social networking sites have become a key platform for hackers to access personal data and steal crucial information because the bulk of them are used almost daily. [17] In a society where we're willing to give our personal information, businesses must be similarly quick to recognise dangers, respond in real-time, and stop any kind of breach. Hackers use these social media platforms as bait because people are drawn there by nature, giving them access to the information and data they need. Users must take the necessary precautions, especially when using social media, to avoid losing personal information. The ability of people to share knowledge with an audience of millions of people is at the core of the specific conundrum that social media presents to corporations. In addition to enabling anybody to communicate information that is commercially important, social media also gives everyone the ability to disseminate incorrect information, which might be just as harmful. [18] The report Worldwide Threats 2013 lists the rapid dissemination of false information via social media as one of the brand-new issues. Cybercriminals can benefit from social media, but businesses cannot afford to cease exploiting it because it is crucial for boosting brand recognition. They require solutions that will bring the problem to their attention, so they may address it before any actual harm is done. In order to reduce risks, businesses should be aware of this, understand the significance of information analysis, particularly in social interactions, and offer workable solutions. Social media management requires the use of the proper tools and techniques.

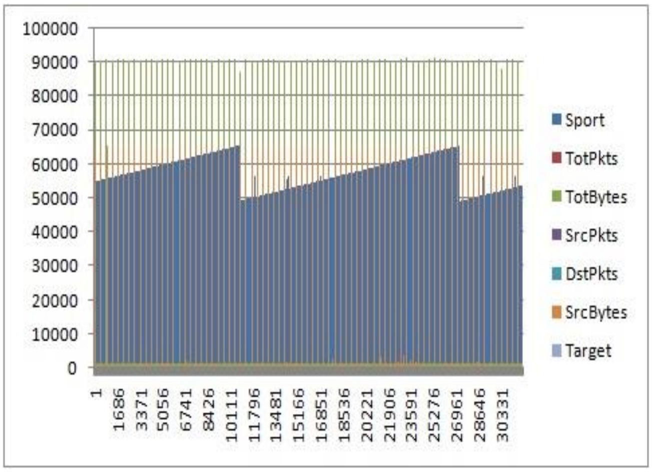

FIG. 3. CLASSIFICATION

Social media platforms are now widely used for communication and sentiment sharing. The number of users worldwide is consistently rising day by day. According to predictions, there will be more than three times as many social network users in 2021 as there were in 2010. [19] Users' security objectives, such as confidentiality, integrity, and privacy, are severely impacted by the dramatic increase in security issues that has been brought on by the surge in social network users. The biggest challenge in maintaining cyber security in social media is the vulnerability of social network security solutions. [20] Facebook applications' flaws could make it possible for hackers to attack users' personal information. These attacks often fall under the CSRF or XSS categories and may result in data breaches. Social media platforms frequently permit other programs to access user data via a variety of interfaces, which is risky. Due to the contradictory needs of social media users, challenges arise. They like to connect with as many friends as they can and share more information, but they also want to maintain their privacy. By posting a variety of personal or other sensitive information on their social media profiles, frequently about their passions and interests that may be readily available to cybercriminals, people run the risk of endangering themselves and those linked to their social network. This information can be used by spammers, stalkers, and hackers for their own gain. [21] Information securities are more at risk from an organizational standpoint due to issues brought on by employees' social media behavior. Employees commonly mix up their official and personal obligations when cooperating and communicating with clients and coworkers on social media, which also poses a security risk. When a person is in a more senior position within the company, these dangers increase. Employees frequently communicate on social media, which may not always be under the organization's control. Information security may have a problem as a result of this.

VI. CONCLUSION

Computer security is a vast subject that is becoming more and more crucial due to the fact that significant transactions are made across networks. As each year comes to a conclusion, cybercrime and information security continue to move in opposite directions. Businesses are being tested by the newest and most sophisticated technology in terms of how they protect their infrastructure and how they do so by leveraging cutting-edge platforms and intelligence, in addition to the new cyber tools and threats that surface every day. If we wish to have a safe and secure future in cyberspace, cybercrimes can't be totally avoided, but we should endeavor to limit them to a minimum.

REFERENCES

[1] S. D. Pawlowski and Y. Jung, "Social representations of cybersecurity by university students and implications for instructional design,"J. Inf. Syst. Educ., vol. 26, no. 4, p. 281, 2015.

[2] W. Oosterbaan, Eur. Cyber Secur. Perspectives, 2017. [Online]. Available: https://www.tno.nl/media/9401/european cyber security perspectives 2017.pdf

[3] N. Rao, "GSM-R global system for mobile communication-railway," CSI Commun., p. 13, 2012

[4] E. P. Dalziell, "Understanding the vulnerability of organisations," 2005.

[5] M. Taddeo, "Is cybersecurity a public good?" Minds and Machines, vol. 29, 10 2019.

[6] "Wthe global risks report 2020." [Online]. Available: https://www.weforum.org/reports/the-global-risks-report-2020

[7] T. R. Soomro and M. Hussain, "Social media-related cybercrimes and techniques for their prevention." Appl. Comput. Syst., vol. 24, no. 1, pp. 9–17, 2019.

[8] S. Romanosky, "Examining the costs and causes of cyber incidents," Journal of Cybersecurity, vol. 2, no. 2, pp. 121–135, 2016.

[9] R. Richardson and M. M. North, "Ransomware: Evolution, mitigation and prevention," International Management Review, vol. 13, no. 1, p. 10, 2017.

[10] P. Voigt and A. Von dem Bussche, "The eu general data protection regulation (gdpr)," A Practical Guide, 1st Ed., Cham: Springer International Publishing, vol. 10, p. 3152676, 2017.

[11] M. Nawir, A. Amir, N. Yaakob, and O. B. Lynn, "Internet of things (iot): Taxonomy of security attacks," in 2016 3rd International Conference on Electronic Design (ICED). IEEE, 2016, pp. 321–326.

[12] A. Singh and K. Chatterjee, "Cloud security issues and challenges: A survey," Journal of Network and Computer Applications, vol. 79, pp.88–115, 2017.

[13] N. Kaloudi and J. Li, “The ai-based cyber threat landscape: A survey,” ACM Computing Surveys (CSUR), vol. 53, no. 1, pp. 1–34, 2020.

[14] [P. J. Taylor, T. Dargahi, A. Dehghantanha, R. M. Parizi, and K.-K. R. Choo, “A systematic literature review of blockchain cyber security,”

[15] Digital Communications and Networks, vol. 6, no. 2, pp. 147–156, 2020.

[16] S. Kunwar and P. Sharma, "Social media: A new vector for cyber attack," 2016 International Conference on Advances in Computing, Communication, & Automation (ICACCA) (Spring), 2016, pp. 1-5, doi: 10.1109/ICACCA.2016.7578896.

[17] D. Herrick, "The social side of ‘cyber power’? Social media and cyber operations," 2016 8th International Conference on Cyber Conflict (CyCon), 2016, pp. 99-111, doi: 10.1109/CYCON.2016.7529429.

[18] Statista. “Number of social media users worldwide from 2010 to 2021 (in billions),” 2017. [Online]. Available: https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/.

[19] C. Wuest, “The Risks of Social Networking,” Symantec Corporation, Mountain View, CA, USA, 2010.

[20] P. Gundecha and H. Liu, “Mining social media: A brief introduction,” New Directions in Informatics, Optimization, Logistics, and Production (Informs, 2012), pp. 1–17.

[21] R. Hekkala, K. Va€yrynen, and T. Wiander, “Information security challenges of social media for companies,” ECIS, p. 56, 2012.