RESEARCH ON COMPUTER NETWORK SECURITY BASED ON THE ERA OF BIG DATA

Mr. Gunda Sai Krishna[*1]

[*1] Final Year Student, Department of Computer Science and Engineering ,Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi, Chennai, India.

ABSTRACT

The progress of the times and the development of technology have greatly liberated our productivity, but at the same time, it has also brought certain security risks, especially the problem of computer network security in the era of big data. Important issues that require everyone of us to pay attention to. This article focuses on the current computer network security issues, and puts forward corresponding preventive measures. It is recommended to hire a professional team to check in time, popularize security knowledge, change passwords, download and purchase network firewalls Software, timely discovery of security vulnerabilities, and the government's introduction of cybersecurity laws.

KEYWORDS: Computer; Security; Virus; Network ; Big data; Cyber security.

I.   INTRODUCTION

The information age has come quietly, even affecting everyone around us. For the coming of the information age, our most intuitive feeling is the popularity of computers and the Internet. Nowadays, computer network security issues have endangered each of us. Not only makes us face a more insecure network environment, but also causes certain lines to our own information. Whether it is today's network viruses or system vulnerabilities, it is a manifestation of computer network security, but it is also a big In the era of data, we are an inevitable problem. Therefore, at this stage, we must actively explore how to use scientific methods to beleaguer the problem of computer network security, making the cyberspace more reliable and secure.

II.   ANALYSIS OF COMPUTER NETWORK SECURITY IN THE ERA OF BIG DATA

The popularity of the Internet has made our work more and more efficient, and it also facilitates our daily life needs. However, in the context of the era of big data, we cannot ignore computer network security issues, especially those that may affect our own information. Cause leakage, or even a fatal crisis on the system. Generally speaking, our common computer network security problem is the Trojan horse virus. For criminals, the spread of network viruses is simpler and accountability is more complicated. At the same time, viruses have the characteristics of being reproducible. When a virus has entered After our computer system, it will reproduce again at a rapid reproduction speed and quickly occupy our entire system, and it will lead to the paralysis of the computer network. If the computer is connected to multiple computers in the form of a local area network, it will even cause most computers in this area are paralytic.

In addition, there is a more common network security threat that is a man-made hacker attack. Because some criminals have mastered advanced computer technology, they may be tempted by interests, supplying data for large companies or groups, resulting in all networks in the group. The paralysis of the system and the stealing of relevant data will not only endanger the company's operation and development, but also cause large-scale leakage of employee information, customer information and project information within the company.

III.   COMPUTER NETWORK SECURITY PRECAUTIONS

3.1 Hire A Professional Team To Check In Time

For large enterprises and groups, they are the most vulnerable to computer network virus attacks. At the same time, once this part of the enterprise is threatened by computer network security, it will not only cause information leakage, but also may suffer economic losses. Seriously going to bankruptcy, so we say that for large companies, enterprises and groups, professional computing should be hired in a timely manner. Computer

network security protection team, to achieve real-time inspection and maintenance. First, companies should strengthen the recruitment of talents in this area. When recruiting externally, it is not only possible to recruit management talent, but also needs to focus on computer network security protection positions. To put forward the corresponding recruitment requirements, you need to ensure that the talents you hire have professional academic qualifications and qualifications, and you also need to have corresponding work experience. In addition, after forming a professional team, you also need to make corresponding requirements for the team's work. Not only do you need to regularly and regularly conduct security inspections of your company's local area network, but you also need to build a more secure network platform around the company's actual needs and network characteristics to set a key for the company's internal LAN security. Some smaller companies with less human resources cost budgets can also use third-party outsourcing, and a three-party professional computer network security team will regularly check the company's network status.

3.2 Popularize Common Sense And Change The Password Regularly

At present, although computer network security problems occur frequently, the reason is not always because of hacker attacks and virus intrusions, but more importantly because the computer network users themselves lack common sense of security and have not attacked viruses, Trojans, and hackers. There is a correct understanding. For example, some users often browse some web pages involving obscene violence when using computer networks, and these web pages often contain some hidden viruses. Computers are attacked, even lurking in computer systems. Once some payment passwords are entered, the funds in them will be stolen. Therefore, mainstream media should actively play their social responsibilities and publicize some common sense of computer network security in public places as much as possible. .Including, but not limited to encouraging people to frequently change login passwords and account information, and promote some common network virus methods, such as e-mail transmission virus, QQ group WeChat group picture download transmission virus, etc. Of course, in this regard At present, domestic well-known browsing systems have been able to prevent accidents.

For example, for some unsafe interfaces, Few of systems have been able to make corresponding prompts on the page. When the user clicks on this interface At the time, the prompt message that comes with the browser will appear first. This is a warning for users, and at the same time, Alipay, there are currently requirements and requirements for passwords, login passwords-that is not Less than how many characters, not repeatable characters, etc.

3.3 Download And Buy Network Firewall Softwares

If you really want to prevent computer network security issues from the root cause, then, First of all, you need to set up a powerful network firewall on the computer equipment. In this regard, everyone is encouraged to download some well-known firewall software.

For example, Tencent and other companies have developed anti-virus software for technical clearance.

In fact, some common viruses can be prevented by the firewall to reduce the threat to computer users. But we need to pay attention to downloading firewall software to prevent the occurrence of computer network security problems is not a remedy. You need to take precautions, and you cannot download after the occurrence and discovery of viruses, but you need to download these firewalls and anti-virus software before logging in to the network or spending on computer equipment. For example, at present The well-known 360 security guard software can check and kill the Trojan virus present in the computer, and can automatically repair the vulnerability when the computer is shut down, so as to ensure the safety of the user's network information.

3.4 Find Security Vulnerabilities And Fix Them In Time To Time

For enterprises and companies, they need to connect various computer devices in the local area network and form a total network system, so the risk factor is greater. This is because after any computer device in the system is attacked by a virus, it will It has a negative impact on the entire system, so it is necessary to establish a corresponding risk early warning mechanism. The author recommends that in the mechanism, first of all, the specific functions of each computer device should be established. Once a cross-functional request occurs, early

warning is required to keep this warning information timely Is uploaded to the professional maintenance team of computer network security and the equipment of company leaders. For example, if the computer network equipment that should be used by the sales department suddenly sends a request to enter the financial department system. Then, computer network management the email addresses of the financial department, the sales department and the main leaders of the company will be promptly received an email. At the same time, in order to avoid the untimely situation of email viewing, there will also be a timely notification in the form of a telephone network administrator member. In addition, the maintenance team of computer network security not only needs to carry out timely inspections of computer network equipment, but also has prepared for a rainy day. At the same time, in the face of some security vulnerabilities that have been checked and possible security risks, it is necessary to ensure that there is no mistake. According to the principle of release, we will investigate these hidden dangers one by one and fix the vulnerabilities in a timely manner. In this regard, the author recommends that you can use firewall technology in a comprehensive manner, not only to set up a special periodic inspection system, but also to form a security protection wall to make the computer network when the device is attacked by external viruses, it can have certain protection capabilities to reduce the possibility of vulnerabilities.

3.5 The Government Of India Issues Cybersecurity Laws

Since the emergence of this network, the issue of network security has become an important issue that we are increasingly concerned about. No matter what industry or industry, or any country, it is bound to face the threats brought by network security, especially for state secret information. Once this information is leaked, it is very likely to pose a huge threat to national security. In this regard, our government needs to actively play its role and functions, and promulgate laws and regulations related to Cyber security. On the other hand, the relevant network management departments must formulate dynamic and scientific security management systems to achieve more reasonable constraints on the network based on the current computing network operating conditions. At the same time, the relevant agencies must also Fully consider security issues and possible problems, and take effective measures to solve them in time to provide users with a safe network environment.

IV.   CONCLUSION

All in all, in addition to actively using the computer network for daily production, living and working, we also need to diaelctically look at this technological advancement, and need to be aware of the potential security risks and threats it may bring. At the same time, as We, the beneficiaries and users of computer networks, need to emphasize the protection of our own information security. To establish this awareness, we must not give criminals an opportunity to take advantage of, and we must actively maintain the security of computer networks. Only in this way can we truly make the computer network world more secure and reliable, and can we enable each of our computer network users to benefit from it, rather than worrying too much about the leakage of self-information.

V.   REFERENCES

[1]   Voor, H.G., Klievink, A.J., Arnaboldi, M., Meijerc, A.J. ―Rationality and politics of algorithms. Will the promise of big data survive the dynamics of public decision making‖, Government Information Quarterly, 2019, Vol. 36(1), pp. 27–38. DOI: 10.1016/j.giq.2018.10.011.

[2]   A.M.AlMadahkah,"Big Data In computer Cyber Security Systems," International Journal of Computer Science and Network Security (IJCSNS), vol. 16, p. 56, 2016.

[3]   C. Everett, "Big data–the future cyber-security or it's the latest threat?," Computer Fraud & Security, vol. 2015, pp. 14-17, 2015.

[4]   Y. Ashibani and Q. H. Mahmoud, "Cyber-physical systems security: Analysis, challenges, and solutions," Computers & Security, vol. 68, pp. 81-97, 2017.

[5]   P. Vinod, R. Jaipur, V. Laxmi, and M. Gaur, "Survey on malware detection methods," in Proceedings of the 3rd Hackers' Workshop on the computer and internet security (IITKHACK'09), 2009, pp. 74-79.

[6]   A. Sirageldin, B. B. Baharudin, and L. T. Jung, "Malicious Web Page Detection: A Machine Learning Approach," in Advances in Computer Science and its Applications, ed: Springer, 2014, pp. 217-224.

[7]   Aniello L., Baldon iR., Chockler G., Laventman G., Lodi G., Vigfusson Y, Agilis, An Internet-Scale Distributed Event Processing System for Collaborative Detection of Cyber Attacks. MidLab Technical Report 04/(2011).

[8]   M. Mayhew, M. Atighetchi, A. Adler, and R. Greensta dt,"Use of machine learning in big data analytics for insider threat detection," in Military Communications Conference, MILCOM 2015-2015 IEEE, 2015, pp. 915-922.

[9]   Mounika Reddy, Avula Deepak, Ekkati Kalyani Dharavath, Kranthi Gande, Shoban Sriramoju (2014). ―Risk-Aware Response Answer for Mitigating Painter Routing Attacks‖ in ―International Journal of Information Technology and Management‖, Volume VI, Issue I, Feb 2014 [ISSN : 2249-4510]

[10]   Liao Y, Vemuri VR, "Use of K-Nearest Neighbor classifier for intrusion detection. Computers & Security", Department of Computer Science University of California, Volume 21, Issue 5, Page 439-448 (2002).

[11]   Eduard Babulak, James CHyatt, "Logistical Control for Consumer Satisfaction in a Global Society," Advances in Information Sciences and Service Sciences, vol. 11, no. 1, pp. 30-35, January 2019.

[12]   N. S. Raviadaran, H., Dastane, O., Ma'arif, M. Y., & Mohd Satar (2019). Impact of Service Quality Dimensions on Internet Banking Adoption, Satisfaction and Patronage. Journal International Journal of Management, Accounting and Economics. Volume 6 (10). 709-730.

[13]   Vinod Kumar et al., "Apache Hadoop YARN: Yet Another Resource Negotiator ", in ACM, 2013. Bekata R., "Big Data And Hadoop: A Review Paper", in RIEECE, 2015.

[14]   Mounica Doosetty, Keerthi Kodakandla, Ashok R., Shoban Babu Sriramoju (2012). ―Extensive Secure Cloud Storage System Supporting Privacy-Preserving Public Auditing‖ in ―International Journal of Information Technology and Management‖, Volume VI, Issue I, Feb 2012 [ISSN: 2249-4510]

[15]   Eastman R, Versace M, Webber A. Big data and predictive analytics: on the cybersecurity front line. IDC Whitepaper, February. 2015.

[16]   Big Data Cyber security Analytics Research Report - Ponemon Institute© Research Report Date: August 2016

[17]   Fang, H. (2015). Managing data lakes in big data era: What's a data lake and why has it became popular in data management ecosystem. 2015 IEEE International Conference on Cyber Technology in Automation, Control and Intelligent Systems, IEEE-CYBER 2015, 820–824.