NOLEGEIN Journal of
Information Technology & Management

ISSN: 2581-6802
Volume 5, Issue 2, 2022
DOI (Journal): 10.37591/NJITM

http://mbajournals.in/index.php/JoITM/index

Review NJITM

Review on Computer Network Security

Soumen Chakraborty[1,*]

Abstract

Computer network security is crucial in protecting computer networks and their associated devices, software, and data from unauthorized access, attacks, and damage. The rapid advancement of technology has greatly improved our productivity, but it has also brought significant security risks, especially in the era of big data. These issues require everyone's attention. This study focuses on recent computer network security issues and proposes preventive measures. It is recommended to hire a professional team to conduct regular security audits, promote security awareness, change passwords regularly, download and install network firewall software, timely disclose security vulnerabilities, and for the government to introduce online privacy regulations.

Keywords: Computer network security, infection, organization, huge information, network safety

INTRODUCTION

The information age has arrived quietly, affecting everyone around us. With the advent of the information age, the popularity of computers and the internet has become our most natural inclination. Nowadays, computer network security issues have endangered all of us. Not only do we face a more insecure organizational environment, but our personal data is also at risk. Whether it is due to current network viruses or system vulnerabilities, these are signs of computer network security issues and they pose a significant threat. In this era of information, we are facing an inevitable issue. Therefore, we must actively explore logical methods to overcome the issue of computer network security and make the internet more reliable and secure [1].

ANALYSIS OF COMPUTER ORGANIZATION SECURITY IN THE PERIOD OF LARGE INFORMATION

The prevalence of the Internet has undoubtedly improved our work efficiency and facilitated our daily needs. However, in the era of big data, we cannot ignore the issue of computer network security, especially when it comes to our personal information, which could be compromised, leaked, or lead to a catastrophic crisis on the network. Generally, the most common network security issue for our personal computers is malware infections. For criminals, spreading network viruses is easier than taking responsibility for their actions. At the same time, viruses have the characteristic of being easily reproducible. After a virus has entered our computer system, it can quickly replicate and spread, taking over our entire system in no time, ultimately resulting in the paralysis of the computer network. If a computer is connected to other PCs in a network, and it becomes compromised, it could potentially disable most of the other PCs in that network [2].

Furthermore, there is a more common network security threat that is a human-made hacker attack.

***Author for Correspondence**
Soumen Chakraborty
E-mail: soumen.chakraborty@cutm.ac.in

[1]Assistant Professor, School of Engineering & Technology (SOET), Centurion University of Technology and Management, Odisha, India

Received Date: March 18, 2023
Accepted Date: March 31, 2023
Published Date: April 14, 2023

Citation: Soumen Chakraborty. Review on Computer Network Security. NOLEGEIN Journal of Information Technology & Management. 2022; 5(2): 1–4p.

Since some criminals have mastered advanced computer technology, they may be tempted by financial gain, providing data for large organizations or groups, resulting in all companies in the group facing paralysis of the system and theft of valuable information. This not only endangers the operation and development of the organization but also leads to large-scale leakage of employee information, customer information, and project information within the organization [3].

COMPUTER ORGANIZATION SECURITY SAFETY MEASURES

Recruit An Expert Group to Really Take a Look at in Time

Large enterprises and groups are the most vulnerable to computer network virus attacks. At the same time, when this part of the enterprise is compromised by computer network security, it can result not only in data leakage but also in financial losses, potentially leading to bankruptcy. Therefore, for large corporations, enterprises, and groups, professional computing services should be employed immediately.

To achieve continuous analysis and support for network security, companies should first strengthen the recruitment of talent in this field. When recruiting remotely, it is important not only to hire management talent, but also to focus on network security assurance positions. To promote the corresponding recruitment requirements, companies must ensure that the skills they hire have professional academic qualifications and certifications, as well as relevant work experience. Likewise, subsequent to framing an expert group, you additionally need to make relating prerequisites for the cooperation. Besides the fact that you really want to routinely and consistently lead security reviews of your organization's neighborhood, however you likewise need to construct a safer organization stage around the organization's genuine requirements and organization qualities to set a key for the organization's inner LAN security. A few more modest organizations with less HR cost spending plans can likewise utilize outsider rethinking, and a three-party proficient computer network security group will consistently take a look at the organization’s status [4].

Advocate Good Judgment and Change the Secret Key Routinely

Currently, although computer network security issues occur frequently, the cause is not always due to hacker attacks and virus intrusions, but more importantly because computer network users themselves lack a sense of security and do not take precautions against viruses, Trojans, and hackers. There needs to be a proper understanding. For instance, a few clients frequently peruse some pages including vulgar brutality while utilizing computer organizations, and these website pages frequently contain some covered up infections. Computers are targeted, and viruses can hide in computer systems. When payment passwords are entered, the resources in them can be stolen. Therefore, traditional media outlets should actively fulfill their social responsibilities and promote common sense practices for computer network security in public places as much as possible. This includes, but is not limited to, encouraging people to frequently change their login passwords and account information, and promoting some common network security practices such as avoiding email-transmitted viruses and virus transmission through downloaded images in QQ and WeChat groups. Of course, currently, domestic well-known browsing systems have been able to prevent accidents [5].

For example, for some high-risk points of interaction, only a few systems have been able to display corresponding prompts on the page. When the user clicks on this link, a prompt message that accompanies the program will appear first. This is a warning for users. At the same time, Alipay currently has requirements and restrictions on passwords, such as the minimum number of characters and no repeating characters [6].

Download and Purchase Organization Firewall Programming Projects

To prevent computer network security issues at their root, it is essential to establish a robust network firewall on the computer equipment. Therefore, it is strongly recommended that everyone downloads some well-known firewall software.

For example, Tencent and other companies have developed anti-virus software for technical advantages. In fact, some common viruses can be prevented by firewalls to reduce the risk to computer users. However, it should be noted that downloading firewall software to prevent computer network security issues is not a cure-all. Precautions must be taken, and firewalls and anti-virus software must be downloaded before logging into the network or using computer equipment, rather than after viruses have been detected. For instance, currently, the well-known 360 security software can scan and eliminate Trojan viruses present in the computer, and can automatically patch vulnerabilities when the computer is turned off, ensuring the security of the user's network information [7].

Track Down Security Weaknesses and Fix Them So as to Time

Enterprises and organizations require connecting various computer devices in the vicinity to form a comprehensive network system, increasing the likelihood of potential threats. When a virus targets any device within the system, it can affect the entire network adversely. Therefore, it is crucial to establish a corresponding early warning system to mitigate risks [8].

For instance, if the computer network hardware intended for use by the sales team suddenly sends a request to enter the financial department system, the email addresses of the financial department, sales team, and key executives of the company will promptly receive an email. Additionally, to avoid the inconvenience of email viewing, there will also be a timely notification by a phone network administrator. Furthermore, the computer network security maintenance team not only needs to conduct timely inspections of computer network equipment, but also needs to be prepared for any unforeseen circumstances. At the same time, despite identifying and assessing security vulnerabilities and potential security risks, it is crucial to ensure that there is no room for error. Following the principles of delivery, these potential risks should be investigated individually and vulnerabilities fixed as soon as possible. The author suggests that extensive use of firewall technology should be employed, not only to establish a special periodic inspection system, but also to create a security protection wall. This will enable the computer network to have specific protection capabilities against external viruses and reduce the possibility of vulnerabilities [9].

The Public authority of India Issues Network Protection Regulations

Since the establishment of this organization, the issue of network security has become a major concern that we are increasingly focused on. Regardless of the industry, country or region, every entity is bound to face the threats posed by network security, especially for sensitive information. Once this information is leaked, it poses a significant risk to national security. In this regard, the government must take an active role and establish regulations and guidelines related to network security. On the other hand, the relevant network management departments must formulate effective and systematic security management systems to implement more reasonable restrictions on the network based on the current computing network operating conditions. At the same time, the relevant organizations must also fully consider security issues and potential problems, and take effective measures to resolve them in order to provide users with a secure network environment [10].

CONCLUSION

Overall, as we continue to rely on computer networks for our daily production, living, and work, it is important to take a critical look at this technological advancement and be aware of the potential security risks and threats it may bring. As users of computer networks, we must prioritize the protection of our personal information security. To promote this awareness, we cannot allow criminals to take advantage of the system, and we must actively maintain the security of computer networks. Only then can we truly make the computer network world more secure and reliable, and allow all computer network users to benefit from it without worrying too much about the leakage of personal information.

REFERENCES

1. van der Voort HG, Klievink AJ, Arnaboldi M, Meijer AJ. Rationality and politics of algorithms. Will the promise of big data survive the dynamics of public decision making? Gov Inf Q. 2019 Jan; 36(1): 27–38. [Internet] Available from: https://www.sciencedirect.com/science/article/pii/S0740624X17304951 [cited 2023 Apr 1]
2. Manzoor Hashmani, Muslim Jameel Syed, Aidarus M, Raza K. An Ensemble Approach to Big Data Security (Cyber Security). Int J Adv Comput Sci Appl (IJACSA). 2018; 9(9): 75–77. ResearchGate. SAI Organization; 2018. [Internet] Available from: https://www.researchgate.net/publication/327985602_An_Ensemble_Approach_to_Big_Data_Security_Cyber_Security [cited 2023 Apr 1]
3. Varela-Vaca ÁJ, Rosado DG, Sánchez LE, Gómez-López MT, Gasca RM, Fernández-Medina E. CARMEN: A framework for the verification and diagnosis of the specification of security requirements in cyber-physical systems. Comput Ind. 2021 Nov; 132: 103524. [Internet] Available from: https://www.sciencedirect.com/science/article/pii/S0166361521001317 [cited 2023 Apr 1]
4. Vinod P, Laxmi V, Gaur MS. Survey on Malware Detection Methods. Proceedings of the 3rd Hackers' Workshop on Computer and Internet Security, Kanpur. 2009 Mar 17–19; 74–79. References - Scientific Research Publishing [Internet]. Scirp.org. 2018 [cited 2023 Apr 1]. Available from: https://www.scirp.org/%28S%28351jmbntvnsjt1aadkposzje%29%29/reference/referencespapers.aspx?referenceid=2372436
5. Vineeth Krishna C, Narayana Swamy C, Viji Amutha Mary A, Selvan MP. Identification of Phishing Urls Using Machine Learning. J Phys: Conf Ser. 2021 Mar 1; 1770(1): 012009. [Internet] Available from: https://iopscience.iop.org/article/10.1088/1742-6596/1770/1/012009/meta [cited 2023 Apr 1]
6. Al-Shehari T, Alsowail RA. An Insider Data Leakage Detection Using One-Hot Encoding, Synthetic Minority Oversampling and Machine Learning Techniques. Entropy. 2021 Sep 27; 23(10): 1258. [Internet] Available from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8535057/ [cited 2023 Apr 1]
7. Yeshwanth Rao Bhandayker. Security Mechanisms for Providing Security to the Network. Int J Inf Technol Manag. 2017 Feb; 12(1): 193–198. Ignited Minds Journals [Internet]. Ignited.in. 2017 [cited 2023 Apr 1]. Available from: http://ignited.in/a/58540
8. Mounica Doosetty, Keerthi Kodakandla, Ashok R, Shoban Babu Sriramoju. Extensive Secure Cloud Storage System Supporting Privacy-Preserving Public Auditing. Int J Inf Technol Manag. 2014 Feb; 6(1): 1–5. Ignited Minds Journals. Ignited.in. [cited 2023 Apr 1]. Available from: http://ignited.in/p/2572
9. Fang H. Managing data lakes in big data era: What's a data lake and why has it became popular in data management ecosystem. In 2015 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER). 2015 Jun 8; 820–824.
10. Bishop M. What is computer security? IEEE Security & Privacy. 2003 Jan; 1(1): 67–9.

