International Journal of Multidisciplinary Research and Growth Evaluation.

Reflections on network information security in the context of big data

Yafeng Wu
Guizhou Provincial Institute of Socialism, Guiyang, Guizhou, China

* Corresponding Author: **Yafeng Wu**

Article Info

ISSN (online): 2582-7138
Volume: 04
Issue: 03
May-June 2023
Received: 22-04-2023
Accepted: 14-05-2023
Page No: 588-591

Abstract
In recent years, there have been frequent incidents of big data information leakage in the worldwide, and information security issues have become an objective fact that cannot be ignored. The author explores the security and protection of computer network information in the context of big data, introduces the concepts of big data and computer network security under big data, as well as the characteristics of computer network information security in the era of big data. Secondly, this article explores the factors that affect the security of computer network information in the era of big data. Finally, in order to create a good development environment for ensuring the security of computer user privacy and computer networks in the context of big data, several considerations are put forward for the protection of computer network information security in the era of big data.

Keywords: Big data background, Computer network security, Protective measures

1. Introduction

With the continuous development of science and technology, the world is in the era of big data. In order to achieve the goal of significantly improving productivity, the demand for data and information from all walks of life is growing. According to the Statistical Bulletin of the National Economic and Social Development of the People's Republic of China in 2021 released by the China Internet Network Information Center (CNNIC) in 2022, the number of Internet users in China has reached 940 million, and the number of mobile Internet users has reached 932 million, the internet penetration rate reached 73.0%. The people have greatly enjoyed the convenience brought by computer networks, but the potential risk of network threats is ubiquitous, especially in the context of big data. Network security presents endless problems, such as network viruses, information leakage, hacker intrusion, malicious software, security vulnerabilities, etc. In addition, modern companies, government departments, universities, research institutes, and other departments, as well as individuals, when using computer networks, Weak awareness of network security, frequent occurrence of network security incidents, often causing serious losses. According to research statistics, in the second half of 2019, the Lasso virus targeted the hosts of universities, enterprises, and individuals. It used user file encryption to force victims to pay a certain fee before decrypting, but at the same time, it destroyed and tampered with the data of the files, resulting in heavy losses for the attacked objects. In 2020, hacker organizations launched a "phishing email" campaign against Chinese officials. It is possible to embed malicious software on users' computers and steal a large amount of data from government network systems. Therefore, the author believes that computer information security technology should keep up with the times, innovate on the basis of existing technology, take necessary measures to ensure the security of network information, comprehensively improve the security of computers during operation, not only adapt to the information processing requirements of today's era, but also promote the sustainable development of China's industry and create more economic benefits.

2. Big data and computer network information security concepts

2.1. Big data

Big data, a new product developed with the computer field [1], refers to the amount of information involved is so large that it cannot be captured, managed, processed, and organized into data information to help business decisions with the help of mainstream software.

Big data mainly comes from business data, Internet data in the development of the era of big data, people for a variety of information data can be more comprehensive perception, analysis, integration, preservation and sharing, for people to better understand the world, access to information to create convenient conditions, to a large extent, to promote the development of social change.

2.2. Computer network information security

The International Organization for Standardization has defined computer network security: Computer network security refers to the protection of hardware, software, and data resources in computer network systems from accidental or malicious damage, modification, or leakage, ensuring the continuous and reliable operation of network systems and the normal and orderly operation of network services [2]. Based on the perspective of ordinary users, computer network security can protect user privacy transmission and reduce theft by others. For network providers, computer networks involve many influencing factors. It is not only necessary to ensure the user information security of computer networks, but also to conduct in-depth analysis of natural disasters, unexpected events, and their adverse effects on network operation [3].

3 Characteristics of Network Information Security

3.1. Invisibility

Computer networks have the characteristics of virtualization, where trojans and viruses are invisible lines of code that are highly covert and difficult to detect. In addition, computer information security is affected by the coverage of the Internet. Due to its large scope, it originates from virtual users. Hackers who invade computers will hide their true identity, making the entire operation difficult to detect. Therefore, the potential risks and hidden dangers of network security are more hidden [4].

3.2. Suddenness

Network information security threats have a certain degree of suddenness and unpredictability, there are differences in the incubation period of different viruses, security threats can not be predicted accurate outbreak time point, once into the computer network system at any time there may be an outbreak of the possibility of threatening network information security, and therefore has the characteristics of suddenness and difficult to accurately predict [5].

3.3. Vulnerability

There are a large number of people using the internet, and everyone has the right to use the internet. Retrieving the information and materials they need on the internet has developmental characteristics, which to some extent means that every link in the process of network use may be threatened by hackers and adverse factors, increasing the vulnerability of computer network security and easily leading to the insecurity of network data.

4. Analysis of high risk factors in computer network information security

4.1. Hacker attacks

Hacker attack is the act of logging in to a user's server through covert channels without the user's permission, and performing arbitrary operations on a computer system without authorization. It is also a product of the continuous development of computer network technology, and has obvious deliberate and malicious human aggression. The goal is mostly to invade computers, intercept and steal business secrets and confidential information from customers and units, and obtain illegal benefits. Once attacked by hackers, the data of the computer system will be lost to a certain extent, causing data distortion problems and affecting some functions of the computer. People's use of computers for normal office work is affected, and work efficiency is greatly reduced. In severe cases, it can cause system paralysis. Hacker intrusion is a type of risk that seriously damages the security of network information, demonstrating the weakness of the Internet in the era of big data. It involves a large amount of information circulating within a unit of time, but due to low security protection levels and system vulnerabilities, it increases the difficulty of ensuring loose information structures. However, the problem is leading to technological upgrades. Based on the current situation of malicious intrusion, technical personnel should optimize security defense and repair systems, patch system vulnerabilities, and ensure sufficient security of computer network information.

4.2. Trojan horse and virus invasion

Trojans and viruses are another major threat factor to computer network systems besides hacker attacks. In the state of computer networking, computers receive massive amounts of information every moment. In the context of big data, information spreads quickly and with a large amount of information. During the process of information dissemination, computers are easily attacked by viruses and trojans. Trojans and viruses have the characteristic of concealment, making them difficult to detect during normal information dissemination [5]. Once discovered, they can cause significant damage to network information, pose security risks to the entire internet, and affect the reliability of computer systems.

4.3. Weak network security awareness among users

In the era of big data, one of the most important factors affecting computer network information security is the security awareness of computer users. However, in practical operations, most computer users have relatively weak security awareness and lack protective measures for the use of computer networks. Personal privacy protection awareness, anti-fraud awareness, and network information recognition ability all show relatively weak characteristics. In addition, the network environment is mixed, making it easier to be influenced by criminals. The common QR code trap is a fraud method that people encounter, By luring and scanning hidden viruses, the information of individual users is leaked, resulting in the loss of cash on personal phones and damaging one's own economic interests. In addition, the login account name and password settings of computer users are relatively simple, which brings great convenience to hackers in cracking. Hackers can easily crack user passwords, log in to personal accounts, and steal personal data information of computer users, personal confidential information, and even information of other family members, as well as core government secrets and business secrets of enterprises, thus engaging in illegal transactions [1].

4.4. Bad emails and junk software

When using computer networks, the threats to network information security include junk software and malicious

emails, which are mainly spread through unauthorized means such as emails and news, forcing users to enter their computers and plagiarizing various information and data, including high-value economic policies and commercial information from government departments, research institutes, enterprises, etc, affects and disrupts computer users' network systems, posing a significant threat to computer network security.

4.5. Improper personal operation

Improper or improper personal operation by computer users is also an important factor affecting the security of computer network information. For example, some people may use the same USB drive or mobile hard drive to copy files and information on multiple machines, but do not pay attention to antivirus. For example, some users may install various software on their computers without paying attention to the security of the software, resulting in the computer being attacked by viruses. Furthermore, due to users' lack of knowledge about network information security and neglect of operational details, it can also affect the security of computer network information to varying degrees [6].

5 Analysis of computer network information security strategy in the context of big data

5.1. Strengthening the improvement of network information security laws at the national level

At present, our country has issued a series of laws and regulations on network information security management, such as the adoption of the Law of the People's Republic of China on Network Security at the 24th meeting of the Standing Committee of the 12th National People's Congress in November 2016, proposing a fundamental law to comprehensively regulate issues related to the security management of cyberspace [7]. In June 2021, the Standing Committee of the 13th National People's Congress, The Law of the People's Republic of China on Data Security was adopted at the Twenty-ninth Session. In order to regulate data processing activities, safeguard data security, promote data development and utilization, protect the legitimate rights and interests of individuals and organizations, and safeguard national sovereignty, security and development interests [8]. In order to protect the rights and interests of personal information, regulate personal information processing activities, and promote the reasonable use of personal information, the 30th meeting of the Standing Committee of the 13th National People's Congress voted to adopt the Law of the People's Republic of China on the Protection of Personal Information at August, 2021[9]. However, with the rapid development of the big data era, many legal provisions have emerged in the actual use of new problems, making it difficult to solve new problems and in urgent need of re-revision. Currently, countries around the world have begun to actively seek a balance between developing the economic value of data and protecting personal information security by revising or increasing the definition of the boundaries and content of personal information protection in laws and regulations. In general, China's network information security legislation protection is still in the groping stage, and there is still a long road to explore in the future.

5.2. Enhance users' awareness of network information security

Under the development of big data era, computer users need to continuously improve their own awareness of network use security, improve computer network security protection measures, and reduce the probability of personal information being leaked. First of all, both for individual and enterprise users, they should recognize the impact of dangerous operations on their own information security, and understand the various factors that endanger network information security, improve network identification ability, need to have the ability to identify some common types of Internet application scams, system tampering, information theft and other network attacks, consciously implement network security protection measures, and improve their own operating behavior standardization and reduce risks. In addition, improve the security awareness and legal concept of personnel within the enterprise, so that they can recognize the important impact of their own operating behavior on enterprise information security and consciously practice security protection measures. At the same time, it is necessary to strengthen personnel training, continuously improve their information literacy, and improve their ability to prevent and control information security issues and deal with them. Finally, enterprises should also strengthen the authority management internally, set the access rights of computer network, avoid over-level access and increase the risk of information security [10].

5.3. Reasonable use of firewall technology

In the use of computers, the reasonable use of firewall technology can greatly reduce the various security threats to the computer system. Firewall types include five types: filtering firewall technology, proxy firewall technology, agent firewall technology, configuration technology and protocol technology [11]. Firewall can effectively manage insecure services, especially manage some computer network services with low security, especially when internal network data and external network data are transmitted to each other, it can guarantee the security of network data transmission through authorized services, or protocols, to prevent important internal network data from being leaked, avoid malicious attacks on internal network and external network, and improve Computer network security factor [12]. In addition, some residences require special protection when accessing and transmitting data, and only other hosts with whom permission has been obtained can exchange data. Such effective protection measures can reduce unnecessary access and avoid the situation of illegal theft of data resources. Furthermore, the application of firewall technology facilitates the detailed recording of data transmission and data access to the intranet and extranet circulation, and generates logs of them. The role of logs is very significant, and they are an important basis for the study of possible attacks, and it is important to give full play to the role of logs and implement targeted protective measures.

5.4. Use of digital signatures and encryption technology

In the current context of big data, digital signature and encryption technology is an effective way to prevent unauthorized users from maliciously invading the network, both of which have a dual protective effect on network resource protection. Digital signature can accurately identify the logged-in user, digital signature cannot be impersonated, and digital signature will be bundled with the information content, which can well ensure the consistency of signature and information. The encryption technology is to rearrange

the original data in a certain way, so that hackers have to re-analyze and decode the data when stealing, making it more difficult to steal and prolonging the stealing time. Encryption methods include link encryption, node encryption, and end-to-end encryption. The application of various encryption technologies, only need the user to do a good job of key management, can make the network information security can be greatly enhanced and protected [10].

5.5. Strengthen the use of virus detection and killing software

Virus checking and killing software can help users discover the virus in the computer system in time and deal with it effectively, and strengthen its application, which can make some regular Trojan horse programs and computer viruses to be dealt with effectively to avoid its negative impact on the normal operation of the computer and information security. Of course, in order to better improve the effect of its security protection for information, users need to regularly implement the full scan and antivirus processing activities, and timely update the virus database, in order to ensure the security of user information.

6. Summary

In total, with the comprehensive popularity of the Internet, big data technology continues to change people's lives. Through the application of big data technology, users can get more targeted and personalized customized services, and can get timely products that meet their needs. In the context of big data, the application of network technology allows people to quickly disseminate and share information, which not only enriches the ways of knowledge dissemination, but also significantly improves work efficiency. Therefore, we should take active security strategies to protect the privacy of users and continuously improve the ability of big data application centers to prevent information risks, so as to effectively defend against diverse network threats and achieve the purpose of fully paying attention to the deterioration of network information security.

7. References

1. Yu JJ, Song QL, Li WB. Computer network information security protection in the era of big data. Electronic components and information technology. 2023;7(02):213-216.
2. Ma HX. Protection measures for smartphone information security in the context of big data era. Network security technology & application. 2023;04:89-90.
3. Zhou YS. Discussion on the influencing factors and preventive measures of computer network security technology. 2023;01:159-161.
4. Hao JC, Xu LY, Zhao WH, Cao PC. Computer network information security and protection in the era of big data. Digital Technology & Application. 2023;41(04):219-221.
5. Fan WK. Research on the threats and countermeasures of computer network information security under the new situation. Electronic Components and Information Technology. 2018;09:61-64.
6. Yang M, Han X, Song WP, Liu L. Research on information security protection of computer network based on big data. Information recording materials. 2023;24(03):74-76.
7. Network Security Law of the People's Republic of China; [2016-01-07] http://www.npc.gov.cn/npc/c30834/201611/270b43e8b35e4f7ea98502b6f0e26f8a.shtml.
8. The Law of the People's Republic of China on Data Security; [2021-06-10] http://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b056d7938f99a788a.shtml.
9. Personal Information Protection Law of the People's Republic of China; [2021-08-20] http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml.
10. Li ML. Analysis of computer network information security protection strategy in the era of big data. China New Communications. 2023;25(06):107-109.
11. Ji JJ. Exploration of the application of firewall technology in computer network security. Digital Technology and Applications. 2023;41(01):231-233.
12. Cui LJ. Research on the application of firewall technology in computer network security. China New Communications. 2022;24(19):110-112.