Applied Science and Innovative Research
ISSN 2474-4972 (Print) ISSN 2474-4980 (Online)
Vol. 8, No. 1, 2024
www.scholink.org/ojs/index.php/asir

Original Paper

Computer Network Virus and Computer Network Security Prevention

Sifei Chen[1]

[1] Xihua University, Chengdu, Sichuan, 610039, China

Received: January 18, 2024 Accepted: February 15, 2024 Online Published: February 19, 2024
doi:10.22158/asir.v8n1p108 URL: http://doi.org/10.22158/asir.v8n1p108

Abstract

With the rapid development of information technology, network security management is becoming increasingly complex, especially, from the point of view of data security, the protection of data should be strengthened, now, the popularity of computers and smart phones will bring a large amount of information, which is inextricably linked with our property and personal privacy, in the human society, with the continuous development of intelligent technology, people's personal information and property protection are also paying more and more attention. Therefore, in order to achieve the purpose of network security and preventing information leakage, it is necessary to analyze and categorize all kinds of data and build a unified management platform on this basis. In recent years, the development of China's computer technology has been more and more attention, especially with the rapid development of big data, data storage, processing capacity, security and other aspects of the rapid development of all walks of life has brought great economic benefits, and the development of social productivity has played a huge role in promoting, but also brought a huge security risks, but the combination of big data technology and computer network security is a good technology, and its advantages are fully reflected in daily life.

Keywords

Computer, Network virus, Security prevention

1. Introduction

Along with the rapid development and popularization of the Internet, there are more and more computer users, and users are able to access rich resources and quickly obtain a variety of information with the help of the network. In recent years, the development of China's computer technology is highly valued, especially in the context of the development of big data blowout, data storage, processing capacity and security of the rapid development of the various sectors of society has brought economic benefits, to a large extent, to promote the development of social productivity, and at the same time, but also bring a greater security problems. Assuming that the network data can not be effectively used, the application value of the data can not be maximized. Computer network security integration of big data technology has a better application value, and its advantages are especially reflected in all aspects of people's lives. With the rapid development of information technology, network security management is increasingly complex. Especially from the perspective of data security, it is necessary to strengthen the protection of data. Nowadays, the popularization of computers and smartphones will bring a large amount of information, which is closely related to our property and personal privacy. In human society, with the continuous development of intelligent technology, the protection of people's personal information to their property is getting more and more attention. Therefore, in order to realize network security and prevent information leakage, it is necessary to analyze and classify all kinds of data and build a unified management platform on this basis. This paper analyzes the computer network security prevention technology, as well as analyzes the causes of network security in the context of big data, and also researches the prevention program of computer network security problems.

2. Risks and Dangers of Computer Network Security

With the advent of the new era, computer technology has been widely used in many industries, making the value of information resources increasingly prominent. Especially with the development and popularization of network technology, information resources have become a very important part of the process of social and economic development, and have a very positive role in promoting the modernization of China. In daily life and production activities, people's thirst for information is also increasing. Therefore, in order to ensure the security and reliability of their information data, it is necessary to strengthen the protection of network information to ensure that it can be effectively managed. However, in the current environment, the implementation of information security has become particularly critical. A comprehensive security protection system needs to be constructed according to the specific security attributes of data and information to ensure the security and accuracy of information data. Software designers can design and develop any type of computer application or operating system, so ultimately, computer software or technical systems will have their own technical and software weaknesses. However, software attacks can be even more damaging and threatening because users are directly affected by external intrusions when installing and using computer software. Once quickly detected by hackers, the user's personally identifiable information can be stolen, causing great harm to the user's own society and economy. With the rapid development of information technology, the spread of ransomware on computers and the Internet has become more and more complex and diverse. Currently, a new highly insidious ransomware virus is quietly emerging. If users cannot establish a good sense of network security in a short period of time, they are likely to be attacked by this type of network and cause huge economic losses in a short period of time.

Some business users do not fully consider network security when simulating real computer network applications, which makes it difficult for them to effectively protect their existing computer applications, especially for personal use. Due to the current high level of openness of personal data, it is difficult to verify it in real time, which greatly increases their own security risk. If users do not have a high level of cybersecurity awareness, this can cause some degree of damage to the integrity and security of their current personal data, which can lead to user data security issues and ultimately to the user's personal security issues. Although the development of computer information network technology is a state of rapid progress, but the public's application of information network technology level is uneven, the computer network users, although many, but most of them are non-network professionals, the application of information network technology is in a very basic state of development, which gives a lot of network lawless elements, such as network hackers, provides an opportunity to take advantage of, lawless elements is to The use of ordinary users to operate the computer network capacity is low, malicious and illegal invasion, to carry out a variety of illegal and criminal behavior, from which to illegally seek economic benefits.

3. Computer Information Security

Computer information security involves the application of computer technology. When a computer is placed in the predicament of a network, the data and information stored within the computer system may face security risks. Only by adopting scientific and reasonable protective measures can we ensure that computers are always in a safe operating state and avoid the leakage and damage of data or information. Therefore, for computer application personnel, we should continue to improve their own technical level, strengthen the importance of the computer network, so as to ensure that in their daily work and life, can be more reasonable use of information technology to solve the actual existence of network security problems. In the context of the current social development, personal information security has become a technical focus of social concern. In order to ensure that the relevant staff in the use of computer technology can scientifically and rationally deal with the problem of information security, it is necessary to combine the actual situation with systematic adjustments, and to take appropriate measures to prevent and stop the attacks of unscrupulous actors, so as to improve the overall performance of the computer.

4. Factors Affecting Information Security Protection of Computer Networks

4.1 Human Factors

Human intervention is a common problem in information security, especially when network hackers use illegal ways to steal personal data in the computer network or steal the company's trade secrets. In this case, a technique called "hacking" is often used to prevent it. These problems can be divided into several different categories, including destructive and non-destructive attacks. A destructive attack is the use of various techniques to gain access to a user's sensitive personal information. The destructive supply method is a way of implanting a virus or Trojan horse in the network environment, which can cause significant damage to the normal operation of the computer in order to obtain the necessary data and information. The non-destructive attack method is a way of exploiting the existence of loopholes in the computer hardware and equipment itself, so as to obtain the necessary data and information of the user, and this kind of behavior also belongs to the man-made destruction. Although this type of damage to the personal information of a relatively small threat, but in the overall network environment, it will trigger a greater attack and security risks, resulting in a large number of computers can not operate normally. The non-destructive demand approach, on the other hand, allows access to relevant information resources through a number of technical means. In the process of processing, it has been the focus of attention in the past.

4.2 Natural Factors

The natural factors referred to are actually a kind of unintentional behavior, in the process of users using computer systems, they may be subject to certain viruses. Because these viruses are highly contagious and harmful, so it is necessary to take relevant measures to prevent, to avoid the phenomenon of its destruction, so as to ensure that the computer system can operate stably and reliably. For example, in the network environment, the use of certain websites, videos and software applications may lead to virus problems. Such viruses are programmed artificially to enter the computer user's system and tamper with and set up the system so as to transmit personal information to the system. This behavior seriously affects the operational stability and security of the system, and also puts an operational burden on some of the equipment of the computer system, leading to wear and tear at the physical level.

5. Characteristics of Computer Network Viruses

(1) very contagious, when the virus works alone, it can be transmitted between a computer with a floppy disk, and can spread rapidly on the network communication platform, through the relevant tests of the system, found that in a normal PC network, as long as there is a workstation where the virus occurs, then within ten minutes, there will be hundreds of computer equipment is infected; (2) the diffusion of a large surface , on the Internet, the virus spreads very quickly and widely, within a short period of time, it will infect many computers, it can also be transmitted to places thousands of kilometers away through a remote workstation in a very short period of time; (3) the spread of a variety of ways; (4) it can not be thoroughly cleaned, if the virus is in a single computer, it can be completely cleaned of the virus, just remove the files with the virus files, or change the low-level format in the hard disk to a low-level format. If a workstation is unable to kill the whole network thoroughly, it will affect all the devices of the whole network system; there is also a situation that a workstation will be infected by another workstation after completing the virus cleanup. In response to these problems, only the corresponding virus detection and For these problems, virus detection and removal on the workstations only cannot fundamentally solve and eliminate the threat brought by the virus to the whole network.

6. Computer Network Viruses and Computer Network Security Precautions

6.1 The Establishment of a Systematic Computer Network Security Defense System

The Internet of Things, big data and cloud computing are the inevitable trends of the upcoming artificial intelligence era. The development of artificial intelligence depends on data, algorithms and computing power. Among them, data is the foundation, algorithm is the main, and computing power is the core. First of all, there must be accurate data, because data is the foundation of artificial intelligence. If the data source is wrong or the data source is contaminated, use the algorithm to analyze the data, which will greatly reduce the accuracy of the algorithm; secondly, in order to obtain the best results under the current computational workload, it is necessary to optimize the algorithm after obtaining the accurate data; and lastly, it is necessary to improve the computational power, and theoretically the stronger the computational power, the stronger it will be. In this AI era, attackers can attack data, algorithms, or devices, all of which are uncertainties in an attack. Therefore, in this era of artificial intelligence, what people need to think about is no longer a technical confrontation, but a diverse and complex attack method to solve the problem, and it is necessary to establish a complete network security protection system.

If you want to ensure a unified protection of the system, you need to create a virus warning platform at the computer network node. The platform needs to be installed with an anti-virus cloud system that can dynamically monitor and analyze signals from input and output network nodes. If a dangerous program is found, it can be blocked or killed, and then notify the management of other sites. Moreover, it analyzes the correlation characteristics of viruses and reports them to the cloud-based virus signature database at the first time. To ensure that the alarm platform can efficiently block the virus, it is necessary to irregularly update the virus signature library, optimization, so that the virus can not find any loopholes.

6.2 Focus on Strengthening the Application of Firewalls

The most commonly used technology is the firewall. Firewalls can effectively resist a variety of viruses and Trojan horse attacks, and can be continuously updated to enhance their own protection capabilities. In addition, the firewall has the characteristics of simple installation, easy promotion and simple operation, which is easy to be accepted by the majority of users. The firewall has a low cost and can be widely used. Firewalls can monitor, analyze, and restrict data flow, and set appropriate protection measures when necessary to monitor and protect network security. Many users lack a deep understanding of protecting personal information security. When downloading relevant software, viruses may invade and pose a threat to the normal operation of their computers. Firewall in operation can be a comprehensive scan of network communications, timely detection of various risks in the operation of the computer, and develop appropriate solutions, such as opening the blocking alarm function, timely closure of infrequently used ports, cut off the path of virus propagation, and the firewall technology has a real-time detection of the characteristics of the gateway technology can be a variety of network data requests for a comprehensive detection, to avoid A variety of undesirable programs to attack the computer system, to ensure that the user in the process of using the computer network environment in a safe state. When carrying out electronic bidding work, all unused gateways should be closed and the corresponding data monitoring work should be done in advance to avoid the invasion of viruses, which affects the effective development of bidding work and reduces the economic losses brought by various enterprises. Because of the rampant computer viruses to the user has brought greater economic losses, the relevant technical personnel through the more common types of viruses to carry out an in-depth analysis, and the development of the corresponding anti-virus wall technology, the principle of operation of this technology is to filter data information at the entrance of the network detection, in the discovery of viruses will be carried out on the application of the removal of the operation, in order to eliminate the invasion of viruses, but due to the increasing number of virus types, the user needs to regularly monitor the anti-virus wall. However, due to the increasing variety of viruses, users need to regularly upgrade the anti-virus wall to ensure that it can maximize its effectiveness in cleaning up viruses. Users in the installation of such software, should be downloaded from the regular site, or ask a professional technician to install, to avoid improper personal operation led to the performance of the firewall and anti-virus wall can not play a role, so as to fundamentally improve the security performance of the computer, for the user's data and information to provide a strong protection.

6.3 Network System Security Monitoring

Computer viruses are very destructive and spread rapidly, which usually has a direct correlation with the improper management of computer networks. Because the management is not perfect, the system is not rigorous, people's security awareness is weak, etc., will inevitably cause the virus continues to appear, repeatedly prohibited, etc.. And, all along, people on the network security construction is often implemented to treat the symptoms but not the root cause of the strategy, which is also caused by the virus continues to appear a fundamental factor. In order to completely solve the problem of unrestricted spread of viruses, people must build a perfect and efficient network security management mechanism. And constantly improve the security defense ability of technicians and enhance security awareness. Moreover, it is also necessary to continuously improve the Internet infrastructure mechanism, and strictly follow the principles of high standards and high requirements to ensure that the construction of relevant hardware and software systems must be able to cover all potential security loopholes, so as to achieve the purpose of all-round defense. With the development of big data technology, various types of information on the Internet have become increasingly complex. However, in order to enhance the security of the network and further promote the use of computers, we must strengthen the maintenance of the network to ensure the good operation of the network. Starting from the security monitoring of the network system, we can enhance the participation of the government and all relevant units, so as to achieve the purpose of purifying the network environment. The new monitoring technology can analyze the data in the network, identify the potential security risks, and fight against cybercrime. In short, we need to speed up the purification of the network environment, so that people have easier access to computers and other high-tech services.

6.4 Focus on Timely Virus Checking and Killing

Research shows that viruses in computers have become an important threat to computer information security. Many viruses not only steal computer data, but also on the computer work to cause some interference, resulting in computer failure; in addition, the virus will be spread on the Internet, many users of the computer to cause great harm. In order to solve this problem, it is necessary to detect and eliminate computer viruses, which can detect and deal with viruses in a timely and effective manner to ensure the safety of the whole computer.

6.5 Enhance Network Security Awareness

Computer network security management is an important part of it. Strengthening the awareness of prevention, establishing a professional management organization, equipping professional technicians, clarifying work responsibilities and improving the management system is the key to ensure the safe operation of the network system and the safe operation of the computer and network system. In order to prevent the loss of data, it is necessary to immediately keep it confidential, and regularly check and maintain the computer network system with appropriate security measures.

6.6 Improve Data Encryption

In order to enhance the security awareness of computer networks, users must strengthen their security awareness when using computers. They not only need to frequently use anti-virus software for system cleanup, but also need to set up firewalls to enhance network security. In the operation of computer networks, encryption of data can effectively prevent data corruption and destruction. Currently the mainstream encryption techniques include link encryption, end encryption, hybrid encryption and so on. Link encryption refers to the use of passwords to encrypt data on the link during data transmission and ensure that each link is individually encrypted. However, the disadvantage is that the vulnerability of the system often exists between multiple nodes, which is easy to cause information leakage, and is highly dependent on hardware and software, making it difficult to effectively improve network security; endpoint encryption refers to the transmission of data communication between the system and the user. By converting the information into a password, the transmitted content can be locked. It is highly reliable and can realize data protection; end encryption technology has the advantages of high reliability and feasibility, and can make full use of the advantages of software and hardware. Combining the first two encryption techniques and summarizing the advantages of each, its security is higher.

7. Conclusion

Overall, after stepping into the era of informationizion, people's concern for information security and stability has gradually increased. Therefore, in order to ensure the stable operation of information security, it is necessary to start from all aspects and take scientific and effective measures to ensure information security. Only when we ensure that the security of the information system in actual operation is enhanced in all aspects and maintained in a stable working state, can we always ensure the robustness of the system in the construction of the system and security measures. The development of China's information and communication industry is very rapid, and computer network security issues are highly emphasized. In the era of big data, computer network security has more problems, data and information leakage, hacker attacks, network security system has not been improved, insufficient monitoring efforts for network security and other reasons, resulting in a greater threat to the security of the computer network. Preventive strategies related to network security should be developed based on the background of big data to ensure the security of China's computer network. In the next step, it is hoped that a simulation experiment will be completed for these theoretical studies to summarize the deficiencies and advantages of the preventive techniques, so as to provide a strong research basis for the subsequent real guarantee of network security.

References

Chao, J. (2023). Analysis of computer network security precautions based on big data. *Electronic technology*, (11), 112-113.

Chen, Y. (2023). Research on computer network security prevention under the background of big data. *Network Security Technology and Application*, (06), 66-68.

Cheng, J. J. (2023). Computer network information security prevention and processing. *Digital Technology and Applications*, (07), 222-224.

Chu, Y. L. (2023). Exploration of computer network security precautions and router troubleshooting methods. *East China Science and Technology*, (10), 96-98.

Dong, C. C. (2023). Problems and prevention strategies in computer network security. *Automation Application*, (S1), 214-216.

Hu, J. M. (2023). Analysis on computer network security prevention technology. *Digital Technology and Application*, (05), 227-229.

Huang, J. (2023). Analysis of preventive and processing measures of computer network security. *Information and computer (theory edition)*, (21), 196-198.

Jiang, M.-D. (2023). Discussion on Influencing Factors and Preventive Measures of Computer Network Security Technology. *Electronic Components and Information Technology*, (05), 174-177.

Jin, C. (2023). Research on the influence factors and prevention of computer network security technology in the environment of Internet of Things. *China New Communication*, (18), 125-128.

Jin, S. G. (2023). Research on computer network security and preventive measures based on big data background. *Information Record Material*, (11), 48-50.

Jing, J., & Guo, W. Q. (2024). Application analysis of big data in computer network security prevention. *Network Security Technology and Application*, (01), 75-76.

Kong, X. Y. (2023). Research on computer network security risk and prevention strategy. *China New Communication*, (12), 116-118.

Li, M. (2023). Influencing factors and preventive measures of computer network security technology. *China High-Tech*, (18), 122-124.

Luo, P. (2024). Analysis of computer network security and its prevention strategy. *Digital Technology and Application*, (01), 221-223.

Sun, L. Y. (2023). Analysis of computer network security prevention in the era of big data. *Digital Technology and Application*, (07), 237-239.

Tu, Y. F. (2023). Research on computer network security prevention in cloud computing environment. *FinTech Times*, (09), 14-18.

Wei, S. Y. (2023). A few thoughts on computer network security problems and its preventive measures. *China New Communication*, (11), 91-93.

Yuan, L. (2023). Analysis of computer network construction and security prevention points. *Digital communication world*, (10), 60-62.

Yun, Y. Y., Zhang, A. N., & Yuan, G. R. (2023). Research on preventive measures of computer network security vulnerability. *Wireless Internet Technology*, (15), 155-158+165.

Zhou, Y. H., & Geng, W. T. (2023). Discussion on computer network security and preventive measures in the era of big data. *Digital Technology and Application*, (12), 237-239.