ISSN 2616-7433 Vol. 5, Issue 8: 153-156, DOI: 10.25236/FSST.2023.050820

Analysis and Management of Computer Network Information Security

Fu Quan

Inner Mongolia Minzu University, Tongliao, 028000, China

Abstract: *Currently, electronic technology is developing rapidly, and the popularity of internet applications is constantly increasing. Computers have become an important component that cannot be obtained in people's social production and life. The invention and application of computers have brought convenience to people, changing work, learning, and lifestyle patterns. However, at the same time, the information security issues of computer networks are also exceptionally prominent, leading to significant risks in network information security. Once such risks occur, the losses to users are enormous. This article analyzes the factors that threaten computer network information security, studies effective protection technologies for computer network information security, and explores strategies for sacrificial network information security management.*

Keywords: *Computer; Network Information Security; Protective Technology; Administration*

Because computer network systems themselves have a certain degree of openness and sharing, which determines that there are inevitably some vulnerabilities in their applications. These vulnerabilities become opportunities for criminals to use computers to attack target users' computers, steal information from others, carry out illegal infringement actions, and cause huge losses to users. Some criminals also attempt to engage in online fraud through computer networks, causing many users to suffer greatly. It is necessary to do a good job in analyzing the security of computer network information, strengthen the management of computer network information security, and ensure the improvement of computer network information security.

1. Current threats to computer network information security

1.1. Disadvantages of the network system itself

The implementation defects of the network itself are an important factor leading to the development of related work, and are also highly susceptible to security attacks. When users visit a website, they are susceptible to hacker attacks, information is difficult to keep confidential, and are easily intercepted by criminals. The current computer operating system itself has some vulnerabilities that are easily attacked. The reason is that computer systems have certain defects in their software, hardware, and programs, which result in incomplete computer functionality [1]. In this way, hackers will exploit these vulnerabilities, increasing the likelihood of attacking and damaging computer networks. In addition, the IP protocol itself has certain security risks, which cannot provide effective control when transmitting information, making it easy for others to steal and intercept it. Due to the incomplete fixation of the protocol and the lack of identity authentication, it provides convenience for hacker attacks, and information and basic data are easily stolen, posing a threat to computer network security.

1.2. Hacker attacks

As mentioned above, hacker attacks are a significant threat in computer network applications. Hackers obtain important information about social life and enterprise production by attacking computer systems and network data packets. This type of attack usually does not affect the user's computer system, but precedes network attacks. Using stolen data to engage in illegal and criminal activities that harm the company [2]. There is also the use of malicious code from some programs for attacks, posing a threat to social life and industry information security. Based on the influence of malicious software code factors, for specific computer network programs, the impact on computer systems is relatively severe. Hackers use malicious software code to attack, installing malicious software code into users' computer systems through external devices and networks. This attack method is usually used as a virus

ISSN 2616-7433 Vol. 5, Issue 8: 153-156, DOI: 10.25236/FSST.2023.050820

carrier, and the related viruses have strong replication and high harm, which can be used to install viruses. On relevant systems, virus replication is used to disrupt user computer systems and achieve attack objectives.[3]

1.3. Trojan virus

Trojan virus is one of the major threats to information security during the operation and use of computer systems. These viruses are highly contagious, and once in contact, they can damage the internal data of computers and even lead to a complete collapse of computer systems. Trojan viruses usually infect application software, hardware, and other media. With the help of these media, viruses can enter computer systems, destroy computer data, and even directly cause computer crashes in severe cases.[4] Computer malfunctions and internal data corruption. Network viruses have a certain degree of infectivity and reproduction, and if not prevented and cleared in a timely manner, it can lead to computer system paralysis and malfunction. Network viruses typically hide information by placing it on web pages or software. However, computers attacked by malicious viruses are difficult to completely destroy, which will further damage the computer's own protective system, seriously damage computer hardware, and ultimately shorten the lifespan of the computer. In addition to Trojan and crawler viruses, some new viruses may also secretly damage your computer system, which is one of the risk factors that need to be prevented in current computer information security technology.[5]

1.4. Insufficient security protection capabilities of network users

The lack of security awareness among current computer system users is also a major factor leading to an increase in computer network security threats. Failure to strictly follow established requirements when performing related operations will lead to an increase in computer network security risks. Some users do not set passwords to protect important confidential information, or intentionally leak operating passwords, resulting in the loss of important information. These issues also lead to an increase in network vulnerabilities, making computer network systems vulnerable to attacks and posing a threat to computer security. Some users have incomplete understanding of computer networks and believe that computer networks are not outside the law, so they are easily exploited by others, leading to being deceived.

2. Computer Network Information Security Protection Technology

2.1. Vulnerability scanning technology

Vulnerability scanning technology is the application of automatic remote vulnerability detection software to detect computer network vulnerabilities, in order to timely discover vulnerabilities and carry out vulnerability repair work. With the application of this technology, it can provide protection for computing network systems, timely fill gaps, and build protective barriers. Vulnerability detection technology is a common computer network security detection technology, and existing vulnerability scanning technologies include passive and active strategies. Passive strategies are host based, while active strategies are network based. It utilizes the network to communicate with remote target hosts, send requests over time, analyze the returned data, accurately determine whether the target host has vulnerabilities and locate them, providing support for vulnerability repair and timely processing.

2.2. Identity authentication technology

In computer attacks, hackers typically use attacks to obtain a user's account and password, in order to gain access to the user's permissions and perform certain operations. Therefore, it is necessary to effectively set the user's login identity and permissions to prevent hackers from stealing. The application of identity authentication technology in network security can effectively resist identity theft. The application of virtual network technology can provide effective technical support for network security issues.[6] The decentralized DIDs and IDs associated with the platform are controlled by virtual network authentication. Virtual networks store the identity information of legitimate users, effectively identify identity theft in the network, and take action against these illegal behaviors. Virtual networks can record all user transactions and data information, provide distributed ledger level security, and improve transaction transparency.

In addition, with the support of computer network technology, all verification, processing, and

ISSN 2616-7433 Vol. 5, Issue 8: 153-156, DOI: 10.25236/FSST.2023.050820

transmission of identity card data must go through the system's security chain. By examining virtual networks, consensus protocols, and decentralized storage, data security is effectively improved, network vulnerability attacks are effectively resisted, and personal user data and account security is ensured. With the current development of online shopping and banking business, the application of identity authentication technology is also quite extensive, which has a good application effect in effectively reducing and handling hacker attacks.

2.3. Virtual Network Technology

Virtual network technology plays an important role in computer network security protection, enabling distributed decentralized node architecture support, and the data required by the corresponding system can be fully stored in multiple devices. The corresponding virtual network nodes contain complete data, and the reliability of the data in the corresponding nodes can be checked [6]. In this way, even if some nodes are damaged, the entire network data information system remains secure under external hacker attacks and will not experience large-scale paralysis. Based on the remaining nodes, the security and normal operation of the entire virtual network system can be ensured, and the system also has the ability to recover node data and functions. Therefore, with the help of virtual network technology, it is possible to build a database system that can resist distributed denial of service attacks. The application of virtual network technology in Domain Name System can timely repair single point of failure, achieve distributed denial of service (DDoS) attack targets, and ensure the overall security of the system. Virtual network technology has a significant impact on preventing distributed denial of service attacks and enhancing network security. This distributed denial of service is one of the biggest threats to global network security, and the resulting attack losses may be enormous. Distributed denial of service attacks are typically malicious attacks carried out by botnet or botnet armies. Relevant technology research and development teams constantly introduce new technologies to improve the power, popularity and concealment of distributed attacks, and increase denial of service attacks and website crashes directly [7]. Once a hacker attack occurs, the normal resource access of legitimate users or software platforms to the website platform will also be affected. With the help of virtual network technology, it can effectively activate the decentralized function of the Domain Name System server, which is equivalent to establishing a mutual trust protocol between the server and the user, effectively avoiding attacks from the central control point and the attacker, and has a certain preventive effect on reducing the occurrence of network security vulnerabilities.

3. Effective management strategies for computer network information security

3.1. Apply safety protection technology and establish safety protection barriers

In computer network applications, it is necessary to always establish a sense of security protection and build a security barrier for computer networks to create a good computer network information security environment.[8] Through understanding and learning about the new situation and technology of computer and network security, we aim to raise awareness, constantly tighten the thread of confidentiality, and work together to promote confidentiality in our daily work. For computer network security, simplicity is often the most effective. As long as we ensure that "confidential information does not go online, and online information is not confidential" in our work, we will ensure the security of important secrets and information. In addition to confidential documents, work files and data are also crucial for users, so the protection of work information cannot be ignored. In specific computer applications, the situation and risks of network security can be analyzed from the perspective of domestic and international network security events, emphasizing the importance and urgency of information protection, and learning and applying network security measures such as password and password security, computer protection measures, mobile phone security, and safe browsing of web pages to continuously improve the level and level of computer network information security protection.

3.2. Strengthen computer security management and do a good job in daily investigation and killing work

For computer network applications, both individuals and organizations need to popularize basic knowledge of network security and safety production cases. The main content includes network architecture and online behavior control measures, computer terminal usage, and network security promotional videos. Through typical case analysis, explain the common types and events of network

ISSN 2616-7433 Vol. 5, Issue 8: 153-156, DOI: 10.25236/FSST.2023.050820

security risks, strengthen the management of computer terminal usage, emphasize the safety regulations of computer use, and strictly prohibit computer equipment from connecting to the internal and external networks. Computer network users themselves should also pay attention to protecting the login passwords of all office and business systems, regularly checking for viruses, not installing and working software, using storage media with caution, and ensuring that the screen is locked and turned off after leaving work to protect work and personal privacy. In specific applications, it is necessary to focus on network security laws and regulations, network security compliance checks, office information security knowledge, etc., grasp the basic concept of network security, the legal basis for carrying out network security work, level protection regulations, unit data security and passwords, and office software and hardware security education, so that users are familiar with common attack methods, and clarify the security risks that exist in computer network system applications Multiple knowledge points such as common mistakes and safety techniques and precautions in daily work. The staff of relevant units should have a high awareness of network security, strictly, practically, meticulously, and deeply carry out network security work, and conduct detailed research on common leakage risk issues. Real cases should be used to analyze the causes and harms of these problems in detail, and the concept of "network security is no small matter" should be conveyed to ensure the overall improvement of computer network information security protection capabilities, Suppress the behavior of illegal elements.

4. Conclusion

Computer network information is overwhelming, and information security protection is particularly important. From the current application situation of computer networks, there are still some security threats in the overall development of computer networks. In response to these problems, it is necessary to continuously research and apply advanced network information security protection technologies, build security firewalls, do a good job in computer network information security management, and enhance users' computer network security awareness and protection capabilities.

References

[1] Liu W. Discussion on the analysis and management of computer network information security [J]. Network Security Technology and Applications 2014; (5): 126128
[2] Zhang X. Analysis and management of computer network information security [J]. Computer Knowledge and Technology 2018; 14 (7): 45, 50
[3] Yan G. Research on the implementation of computer network information security analysis and security management [J]. Scientist 2016; 4 (12): 25-27
[4] Liu J. Discussion on computer network information security management strategies [J]. Digital Design (Part 1) 2020; 9 (10): 48-49
[5] Wu T. Analysis of computer network information security and firewall technology application [J]. China New Communications 2022; 24 (21): 110-112
[6] Zhu J, Li J. Research on computer network information security and protection under big data [J]. China New Communications 2021; 23 (5): 147-148
[7] Feng C. Computer network information security based on virtual private network technology [J]. Electronic Testing 2022; (11): 81-83, 52
[8] Bian Q. Exploration of computer network information security and protection based on big data background [J]. Information recording materials 2021; 22 (6): 20-22