Original Research Article

Open Access

Omniscient Pte.Ltd.

The Problems and Countermeasures of Computer Network Security

Hang-Hang Yang[*]

Wuhan Metro Bridge and Tunnel Management Co., Ltd.Wuhan City, Hubei Province,430060,China

***Correspondence to:** Hang-Hang Yang,Wuhan Metro Bridge and Tunnel Management Co., Ltd.Wuhan City, Hubei Province, 430060,China,E-mail:hbwhyhh@qq.com

Abstract: With the rapid development of information technology, computer network security issues are becoming increasingly prominent. This article thoroughly analyzes the key problems faced in the current network security field, such as insufficient identity authentication mechanisms, incomplete data encryption measures, and lack of data backup strategies. In response to these issues, corresponding countermeasures are proposed, including strengthening identity authentication and access control, enhancing data encryption and transmission security, and implementing regular data backup and recovery mechanisms. These countermeasures aim to improve the overall security of computer networks and reduce security risks. The importance of computer network security is emphasized in this article, along with the urgency and necessity of implementing these countermeasures.

Keywords: computer network; existing problems; effective countermeasures

Introduction

With the rapid advancement of technology, computer networks have deeply penetrated into various aspects of our lives. Whether it's work, study, or entertainment, we rely heavily on network support. However, with the widespread use of networks, network security issues have become increasingly prominent. Network security incidents such as identity theft, data breaches, and malicious attacks occur frequently, posing serious threats to personal privacy, property security, and even national security. This article delves into the core issues in the current network security field, aiming to reveal the nature of these threats and propose corresponding response strategies to build a safer and more reliable network environment, ensuring the safety and security of people's daily lives and work.

1. The Importance of Computer Network Security

Computer network security is the cornerstone of the normal operation of modern society. Whether it's financial transactions, business collaborations, or everyday communications, they all heavily rely on the stability and security of computer networks. Once network security issues arise, they may lead to serious consequences such as traffic interruptions and financial service disruptions, causing severe impacts on the normal functioning of society. Secondly, computer network security concerns our country's security and sovereignty. With the rapid development of information technology, cyberspace has become a new battlefield for our country's security. New threats such as cyber-attacks, cyber espionage, and cyber terrorism pose serious threats to our country's economy, culture, and other sectors. Therefore, strengthening computer network security is an important means to safeguard our country's security and sovereignty. Additionally, computer network security also safeguards personal privacy. In the digital age, personal information is collected and processed on a large scale, and network security issues directly relate to the risk of privacy breaches. Once personal information is obtained by malicious actors, it may lead to a series of problems such as fraud and identity theft, resulting in significant losses for individuals. Finally, computer network security is of great significance to economic development. With the widespread application of technologies such as e-commerce, cloud computing, and big data, network security issues have become an important factor restricting economic development. Strengthening network security construction helps ensure the security of economic activities and promotes healthy economic development.

2. Computer Network Security Issues

2.1 Technical Vulnerabilities and Defects

Technical vulnerabilities and defects are core issues in the field of network security, acting as invisible security doors that provide potential entry points for hackers and malicious attackers. It is essential to recognize that whether it's complex network systems or everyday software applications, they are all designed and coded by humans, inevitably leading to some oversights and errors. These vulnerabilities may stem from programming negligence, design flaws, configuration errors, and various other reasons. They act as open doors, allowing hackers to exploit these vulnerabilities for attacks. For example, buffer overflow is a common type of vulnerability where attackers can execute malicious code, or even gain complete control over the victim's system. Another example is SQL injection attacks, where attackers can steal, manipulate, or delete sensitive information from databases. The existence of these technical vulnerabilities and defects can lead to severe consequences such as data loss, system crashes, and more critically, the leakage of personal privacy and financial information, resulting in immeasurable losses for individuals and organizations.

2.2 Malware and Viruses

Malware and viruses are among the most concerning threats in the field of network security. They often infiltrate computer systems in subtle ways, disguising themselves as harmless files or links, deceiving users into opening or downloading them. Once malware and viruses invade a system, they rapidly proliferate and launch attacks, causing significant damage to users' computers and personal information. Malware can take various forms such as worms, trojans, ransomware, etc., with the goal of stealing users' sensitive information like bank accounts, passwords, credit card details, etc. Once these pieces of information fall into the hands of malicious actors, they may be used for illegal transactions, identity theft, or other criminal activities. Moreover, malware can also disrupt system files, occupy system resources, degrade computer performance, and even lead to system crashes. Viruses, on the other hand, are malicious programs capable of self-replication and infecting other computer programs. They attach themselves to other files or programs and spread to other computers through actions like user copying, sharing, or execution. Once infected, viruses rapidly multiply and disrupt the normal operation of computer systems, potentially causing serious consequences such as data corruption and system crashes.

2.3 Insufficient Identity Authentication and Access Control

Identity authentication and access control are core components of network security, determining who can access specific network resources and what operations they can perform. However, regrettably, many systems have significant deficiencies in this regard. When identity authentication mechanisms are weak or missing, attackers may exploit this vulnerability to obtain legitimate users' credentials through guessing, brute force attacks, or other means, and then impersonate legitimate users to perform illegal operations. Furthermore, insufficient access control mechanisms are also concerning. If a system fails to reasonably divide and restrict users' access permissions, attackers who obtain a low-level account may exploit permission escalation vulnerabilities in the system, gradually elevate their permissions, and ultimately gain system administrator-level access. Once attackers have sufficient permissions, they can freely access, modify, or delete any data in the system, or even execute system commands, causing severe damage to the system.

2.4 Poor Management and Human Error

In the field of network security, poor management and human error are often overlooked but critical factors. These issues are typically caused by management deficiencies and improper behaviors within organizations. Firstly, unreasonable password policies are a typical example of poor management. Many organizations set password policies that are either too simple or too complex, making it difficult for users to remember or comply with them, thereby reducing the security of passwords. Additionally, requirements for regular password changes may become ineffective due to users mishandling them, such as writing new passwords in conspicuous places or sharing them with others. Secondly, the lack of security audits is also a manifestation of poor management. Security audits are essential means of examining the effectiveness of network security measures. However, many organizations may overlook the importance of security audits due to limited resources or insufficient awareness, leading to long-term existence of security vulnerabilities and increased risk of attacks. Finally, insufficient security training is another significant issue. Many employees lack basic awareness of network security, making them susceptible to attacks like phishing and malware.

3. Effective Measures for Computer Network Security

3.1 Strengthening Identity Authentication and Access Control

Implementing robust identity authentication mechanisms is the first line of defense for network security. This means that systems need to authenticate every user attempting to access them, ensuring they are legitimate and authorized users. This can be achieved through various methods such as using strong passwords, dynamic tokens, biometric technologies, etc. Through these means, systems can accurately identify user identities, preventing unauthorized users or attackers from masquerading as legitimate users to gain access to the network. Additionally, setting appropriate access permissions is crucial for preventing unauthorized access and operations. Based on users' roles and responsibilities, systems should assign them the appropriate access permissions. For example, administrators may have higher permissions allowing them to perform more operations, while ordinary users may only access the resources they need. This way, even if attackers successfully pass authentication, they can only access authorized resources, preventing them from causing serious damage to the entire network. Lastly, continuous monitoring and regular assessment of the effectiveness of identity authentication and access control mechanisms are crucial. System administrators need to periodically check user permissions, audit logs, and abnormal behavior to identify potential security risks.

3.2 Enhancing Data Encryption and Transmission Security

Data encryption is an effective means of protecting sensitive data from unauthorized access or disclosure. By encrypting data, even if intercepted during transmission or storage, attackers cannot directly read the data's content. Data encryption can employ various algorithms and technologies such as symmetric encryption, asymmetric encryption, etc., depending on the sensitivity of the data and actual requirements. Additionally, ensuring the security of data transmission is equally important. Using secure communication protocols such as HTTPS, SSH, etc., can encrypt and verify the integrity of data during transmission, preventing data theft or tampering. Moreover, Virtual Private Network (VPN) technology can provide secure remote access channels, protecting user data from man-in-the-middle attacks. Lastly, achieving encryption and transmission security requires comprehensive consideration of multiple aspects. Besides selecting appropriate encryption algorithms and communication protocols, it is necessary to strengthen key management to ensure the secure storage and distribution of keys. Additionally, regularly updating encryption algorithms and protocols to address emerging security threats and vulnerabilities is key to maintaining data security.

3.3 Regular Backup and Data Recovery

Data backup is a crucial measure for preventing data loss or damage. Regularly backing up important data means that even in the event of accidents such as natural disasters, hardware failures, malicious attacks, etc., we can quickly recover data from backups, minimizing losses. Setting reasonable backup frequencies and retention policies ensures the freshness and availability of backup data. Additionally, the formulation of data recovery plans is equally important. This plan should detail how to quickly and effectively recover data from backups in the event of data loss or damage. The plan should include clear recovery steps, required resources, Recovery Time Objectives (RTO), and Recovery Point Objectives (RPO), among other key elements. Furthermore, conducting regular recovery drills is necessary to ensure that the recovery plan can be smoothly executed in real events. Lastly, to ensure the security and integrity of backup data, a series of security measures need to be taken. For example, backup data should be stored in secure and reliable environments to prevent unauthorized access and tampering. At the same time, backup data should be regularly verified and tested to ensure its availability and integrity.

3.4 Monitoring and Responding to Security Threats

Monitoring and responding to security threats are crucial aspects of maintaining computer network security. Firstly, using network monitoring tools and security devices is key to detecting potential security threats. These tools can monitor network traffic in real-time, identify abnormal behavior, and promptly issue alerts upon discovering suspicious activities. Through real-time data analysis, we can quickly identify potential attack patterns, malware infections, or other security vulnerabilities, allowing for swift action. Secondly, establishing a security incident response team is crucial. This team should possess professional security knowledge and skills, responsible for receiving, assessing, and handling security incidents. They need to quickly analyze the nature, scope, and potential impacts of threats, and take appropriate measures to respond. Additionally, the team needs to collaborate closely with other relevant departments to ensure timely information sharing and coordinated responses. Lastly, timely response and handling of security incidents are key to minimizing losses. Once security threats are discovered, we must take prompt action to prevent attackers from further exploiting vulnerabilities or stealing data. This may include isolating affected systems, removing malware, restoring data, etc.

3.5 Enhancing User Security Awareness and Training

Users are the first line of defense for network security. Their daily operations and behaviors often determine the overall security status of the network. Therefore, enhancing users' security awareness and skills is crucial. Only when users have sufficient security knowledge can they effectively identify and avoid security threats such as phishing attacks, malware, etc. Secondly, strengthening user security education and training is an effective way to achieve this goal. This includes imparting users with basic concepts, principles, and practices of network security, teaching them how to identify and respond to phishing emails, how to securely download and install software, how to set and manage complex passwords, etc. Through these training sessions, users can become more vigilant in the face of network threats, reducing security incidents caused by negligence. Lastly, enhancing user security awareness and training needs to be continuous. As network technology and threats continue to evolve, users need to continuously update their security knowledge and skills. Therefore, organizations should conduct regular security training activities, encourage user participation, and provide necessary resources and support.

Conclusion

The issue of computer network security, as a major challenge in the information age, has far-reaching and complex implications. Problems such as the leakage of personal information and threats to corporate security highlight its severity. Faced with these challenges, we cannot stand idly by but should actively seek effective solutions. This not only requires continuous innovation and improvement in technology but also necessitates raising awareness of security and enhancing preventive capabilities. Only in this way can we build a more secure and reliable network environment, ensuring the security and smooth flow of information.

References

[1] Li, L. (2019). Analysis of Computer Network Security Issues and Prevention Strategies. *Digital Technology and Applications*, (11), 192-193.

[2] Qiao, Y.(2018). Discussion on Computer Network Security Issues and Countermeasures. *Electronic Manufacturing*, (24), 54-55.

[3] Wang, X., Guo, Y., Huang, J., et al. (2018). Analysis of Computer Network Security Vulnerabilities and Prevention Measures. *Computer Security*, (01), 90-91.

[4] Xie, P. (2018). Problems and Prevention Measures Facing Computer Network Security. *Electronic Technology and Software Engineering*, (02), 86-87.