Research on risk control of computer network security under the background of artificial intelligence

Jiaxin Shi
Dalian University of Finance and Economics, Dalian 116023, China

Abstract: Computer network security is an important issue, especially in the era of artificial intelligence needs our attention. With the development of artificial intelligence, the risks faced by computer network security become more diversified and complicated, so we need to take effective measures to control these risks. This paper will discuss the research of computer network security risk control under the background of artificial intelligence, discuss its importance, main influencing factors and feasible control measures, hoping to improve everyone's understanding and coping ability of computer network security risk control.

Key words: Artificial intelligence; Computer; Network security risk control; measures

1. The importance of computer network security risk control

1. to prevent personal information disclosure

With the popularization of the Internet, the protection of personal information has become the focus of attention of all sectors of society. The risk control of computer network security is the basis of protecting personal information security. In the process of computer network application, personal information is often stored in the computer system, if the hacker or network attack, personal information may be leaked. For example, personal information on social platforms, payment information on online shopping platforms, medical information, personal privacy and so on, these are all important information stored in the network, leakage will bring immeasurable losses to people. Therefore, the importance of computer network security risk control lies in protecting the security of personal information, preventing the disclosure of personal information, and protecting the legitimate rights and interests of the people.

2. Safeguarding national information security

Computer networks have become an important part of national security. The importance of national information security is becoming increasingly prominent. Once it is invaded by network attacks or hackers, the disclosure of national confidential information will bring irreparable losses to the country. For example, the security of state secret documents, military secret information, energy, transportation and other important infrastructure needs the support and guarantee of computer network security risk control. Therefore, the importance of computer network security risk control lies in maintaining national information security and ensuring national security.

2. The main influencing factors of computer network security in the context of artificial intelligence

First, the development of artificial intelligence. With the continuous development of artificial intelligence technology, there are more and more security loopholes in computer networks, which makes hacker attacks more and more frequent, posing a great threat to network security. The original security precautions and technical means gradually lose their effectiveness, which makes new security threats emerge constantly. For example, through artificial intelligence technology, hackers can carry out network attacks more effectively, and can achieve deep penetration of the network, so as to carry out "invisible" attacks in the network. In this case, traditional network security measures have been unable to fight against hackers' attacks; Second, the computer itself equipment problems. Vulnerabilities and errors in computer hardware equipment and software systems are often exploited by hackers in various ways to carry out attacks. For example, vulnerabilities in operating systems or applications can be exploited by hackers to carry out remote attacks. In addition, the problem of hardware devices is also a problem that cannot be ignored. For example, complex hardware architectures and signal transmission technologies can lead to security vulnerabilities, which are often difficult to detect and repair; Third, improper personnel operation and management. Because in terms of computer network security, it largely depends on human operation and management. Different personnel concepts, lack of security awareness, inappropriate behavior or negligence will bring threats to computer network security. For example, some employees may accidentally or intentionally disclose important information, or overlook details in the use of security equipment. Therefore, strengthening the security awareness training and management of employees is one of the important measures to ensure the security of computer networks; Fourth, the illegal attack of hackers. Hackers attack networks through various means to steal, tamper with or destroy the security of data, information and systems, causing huge economic and security losses. For example, hackers use tools and techniques to carry out attacks, targeting servers, mail systems and databases in the network. These attacks may cause system paralysis, data loss or destruction, causing serious losses to businesses and individuals.

3. Computer network security risk control measures

1. Optimizing computer hardware equipment

Optimizing computer hardware equipment is an important risk control measure for computer network security. Computer hardware equipment is the foundation of network system, and its security directly affects the security of the whole network. In the context of artificial intelligence, it is not only necessary to ensure the normal operation of computer hardware equipment, but also to strengthen its security to prevent risks such as hacker attacks and information leakage. First of all, it is necessary to reinforce and optimize the security of computer hardware equipment. Various hardware and software technical means can be used to reduce the vulnerabilities and security risks of hardware devices. For example, the use of hardware encryption technology to encrypt hard disks can effectively prevent the risk of data leakage. In addition, the use of trusted computing technology can ensure the safe start-up and operation of hardware devices and prevent the tampering of malicious software. Secondly, reasonable configuration and management of hardware equipment is also one of the important measures. The reasonable design of network topology and the reasonable configuration of hardware equipment can reduce the security vulnerabilities and risks in the network. For example, the use of firewalls to limit the traffic entering and leaving the network can effectively filter malicious attacks and illegal access. At the same time, the reasonable configuration and management of hardware key management, permission control and access control can also effectively reduce the risk of hardware attacks. Finally, regular hardware device security assessment and vulnerability scanning is also an important measure to ensure computer network security. Through the security assessment of hardware devices, the existing security loopholes can be discovered and patched in time to prevent hackers from using these vulnerabilities to attack. At the same time, regular vulnerability scanning can also help discover potential risks in hardware devices and prevent possible attacks in advance. In addition, strengthening the monitoring and logging of hardware devices is also an important measure. By monitoring the running status and events of hardware devices in real time, you can discover and deal with anomalies in time to reduce possible risks. In addition, by periodically analyzing and auditing hardware log records, you can track and troubleshoot security events, and improve your perception and response capabilities to security threats.

2. Encryption of network information

In the computer network security risk control, the network information encryption is an important measure. Encryption refers to the process of converting plaintext into ciphertext, which can better protect the confidentiality of information and prevent data from being stolen, tampered with or destroyed by hackers. Below, we will discuss how to encrypt network information in detail from two aspects of encryption technology and application cases. On the one hand, symmetric encryption technology. Symmetric encryption, also known as shared key encryption, means that the same key is used for encryption and decryption. In this technique, the sender and recipient need to agree on a key, and then use that key to encrypt and decrypt the message. Common symmetric encryption algorithms include DES, 3DES, AES, etc. AES algorithm is the most commonly used encryption algorithm at present. On the other hand, asymmetric encryption technology. Asymmetric encryption, also known as public key encryption, means that different keys are used for encryption and decryption. In this technique, a public key is used for encryption and a private key for decryption. Common asymmetric encryption algorithms include RSA, DSA, etc. RSA algorithm is the most commonly used asymmetric encryption algorithm.

The following are a few application cases:

(1)HTTPS protocol

The HTTPS protocol is a secure HTTP protocol that encrypts communications by adding an SSL or TLS protocol layer to the HTTP protocol. In HTTPS, when a client sends a request to a server, it first sends a client Hello, which contains a list of encryption algorithms supported by the client. The server will select an encryption algorithm from the list and send a server Hello to the client, which also contains the encryption algorithm chosen by the server. After that, the client and server communicate with each other using the agreed key.

(2)VPN

A Virtual Private Network (VPN) is a secure communication technology that encrypts user data. The VPN technology can build a private network on the public network and send the user's data to the target network after encryption. In VPN communication, the data sent by the user is encrypted to protect the security of the user data. Common VPN technologies include PPTP, L2TP, and IPSec.

(3) Secure email

Secure email is a measure that protects the confidentiality of emails through encryption. It encrypts sensitive data such as email account number, password and email text to protect the security of emails. In secure mail, the commonly used encryption methods are S/MIME and PGP. S/MIME is to embed a digital certificate in the mail and use asymmetric encryption to encrypt it. PGP (Pretty Good Privacy) is a kind of widely used encryption software. It can encrypt and digitally sign email content to ensure the confidentiality and integrity of email content.

3. Optimize the firewall Settings

Firewall is an important component of network security system. Its function is to control illegal traffic and attacks between internal and external networks, and protect the security of network system and data. In the era of artificial intelligence, as the first line of defense for network security, the firewall needs to be optimized to ensure network security.

Optimizing firewall Settings is a systematic and complex process, which requires us to consider and implement from many aspects. The following are some common optimization measures: First, the optimization of firewall rules. Firewall rules are one of the key factors to ensure the correct operation of the firewall. The setting of the rules should be based on the actual needs of the enterprise, but also take into account the strategy and technical means of the attacker. In order to improve the readability and maintainability of the rules, the rules should be classified management, using comments and labels to increase the readability; Second, firewall upgrade and vulnerability repair. Firewall upgrade and vulnerability repair is an important measure to ensure the safety of firewall operation. With the continuous development of network technology and the continuous exposure of vulnerabilities, firewalls also need to be constantly upgraded and patched to ensure security. Enterprises need to keep abreast of vulnerability information and patches, and upgrade and patch them in a timely manner; Third, access control strategy optimization. Access control policy is one of the important functions of firewall. Different access control policies should be set according to different service requirements to implement functions such as access audit and security detection. When implementing access control policies, we should consider strengthening access control and access security to effectively reduce security risks. Fourthly, firewall log analysis. Firewall log is one of the important bases to identify security events and attacks. It is necessary to make full use of firewall log analysis tools to monitor and analyze firewall logs in real time. According to the log analysis results, adjust the firewall rules and policies in time to improve security.

The above are some common firewall optimization measures, but the specific implementation needs to be based on the actual situation and requirements of the enterprise. Here are some examples to illustrate:

Example 1: A company uses a firewall to defend against network security. However, improper rules result in multiple insecure ports between the Intranet and the Internet, which are easily exploited by attackers. After optimizing rule Settings, upgrading the firewall, and strengthening log analysis, the network security is improved.

Case 2: An e-commerce company found that its website had suffered a DDoS attack, resulting in service interruption and data leakage. After optimizing the firewall rules and access control policies, and adding DDoS attack protection technology, the enterprise successfully fended off the attack and ensured the service and data security of the enterprise.

Conclusion: Computer network security risk control is an important issue, we need to constantly strengthen the understanding and understanding of relevant knowledge, explore more effective control measures to protect our personal information and national information security. In the context of artificial intelligence, we need to pay attention to the development of artificial intelligence, computer itself equipment problems, personnel operation and management of improper and illegal attacks by hackers and other main influencing factors, take corresponding measures to ensure network security. Through continuous research and exploration, we believe that we can better cope with computer network security risks and realize safe and reliable information exchange and interconnection.

References:

[1] Shideng Ma. Discussion on Computer Network Security risk control under the background of Artificial Intelligence [J]. Network Security Technology and Application,2023(07):164-165.

[2] Jianmin Hu. Computer Network Security Risk Control under the background of Artificial Intelligence [J]. Digital Communications World,2023(04):186-188.

[3] Kunping Yang,Weifeng Li. Research on University Computer Network Information Security based on Artificial Intelligence [J]. Yangtze River Information and Communication,2022,35(09):137-139. (in Chinese)

[4] Lili Wang. Computer Network Security Risk Control under the background of Artificial Intelligence [J]. Network Security Technology and Application,2022(09):171-173.

[5] Jian Liu. Research on Computer Network Security Risk Control in the era of Artificial Intelligence [J]. Electronic Technology and Software Engineering,2020(23):244-245.