Research on Computer Network Security under the Background of Big Data

Liu Changsong

Hunan Institute of Engineering, Hunan 411101, China

ABSTRACT. *In the context of the era of big data, computers and the Internet are affecting people's daily lives, working methods and thinking patterns. But when people use computer networks, they will inevitably face certain security risks. Information leakage caused by computer networks under the background of big data has also caused serious problems for people.*

KEYWORDS: *Big data era; Computer; Internet; Network security*

1. Computer Network Security under the Background of Big Data Era

Big data refers to data sets that are characterized by large scale, high speed, and diversity, and are large and complex, making it difficult to process with existing database management tools or data processing applications. According to different sources, big data can be divided into three categories: from people, that is, various types of data generated by people during the use of mobile Internet in internet activities, including information such as text, pictures, videos, etc.; from machines, that is, computers Various types of data generated by information systems exist in the form of files, databases, multimedia, etc., and also include automatically generated information such as audits and logs; from objects, that is, data collected by various digital devices, such as digital signals generated by cameras, various human characteristic values generated in the medical internet of things, a large amount of data generated by astronomical telescopes, etc..

Big data has brought a series of problems while promoting the rapid development of accounting informatization. For example, the lack of accounting information system security and system supervision information [1]. At present, people's words and deeds on the Internet are in the hands of Internet merchants, including retrieval habits, reading habits, shopping habits, contact information of friends, and so on. Multiple practical cases show that even when harmless data is collected in large quantities, personal privacy can be exposed. In fact, the meaning of big data security is more extensive. The threats faced by people are not limited to the leakage of personal privacy. Like other information, big data faces many security risks in the process of storage, processing, and transmission. It has data security and privacy protection requirements. Realizing big data security and privacy protection is more difficult than other previous security issues (such as data

security in cloud computing). This is because in cloud computing, although the service provider controls the storage and operation environment of the data, users still have some ways to protect their data, such as implementing secure storage and secure computing of data through cryptographic technical means, or through trusted calculation method realizes the safety of the operating environment. In the context of big data, Internet merchants are both data producers and data storage, managers, and users. Therefore, it is extremely difficult to restrict the use of user information by merchants through technical means to achieve user privacy protection.

2. Computer Network Security under the Background of Big Data Era

Under the background of big data era, computer network security prevention should make full use of big data security awareness technology, and collect the network attack events that have occurred or are occurring through targeted mining and capturing the loopholes of network communication facilities, network security products, network system software and application software. Record and automatically integrate the massive data such as the website, time, attack method and traffic generated, and generate vulnerability feature database, network traffic anomaly feature database, hacker behavior feature database, etc.. Based on the vertical and horizontal matching association analysis, the multi-dimensional integration of big data from network security technology to network security management is realized, and a complete security defense system is further formed.

The foundation of network security construction in the context of big data is the network security awareness capability consisting of asset awareness, vulnerability awareness, abnormal behavior awareness, and security event awareness[2]. The realization of network security construction depends on big data network security fusion capabilities represented by security technology fusion, security business fusion, and security management fusion. The guarantee of network security construction is the big data network security service capabilities around basic security services, security product services, and security operation and maintenance services.

2.1 Big Data Network Security Awareness

Utilizing the 4V characteristics of big data, network security awareness can make full use of the fast processing and data storage of big data, and analyze the network operation information, network and security device logs, various application logs, and various data acquisition networks traffic characteristics, user behavior characteristics, and APT attack characteristics effectively identify normal access behaviors and abnormal attack behaviors. Big data-oriented network security perception capabilities can sense the existence of vulnerabilities, sense the release of viruses, sense hackers' attacks, sense changing applications, sense whether people's behavior is abnormal in the vast network, sense web pages, whether the content of forums, microblogs, etc. are in compliance with regulations, laws and regulations.

2.2 Big Data Network Security Convergence Capabilities

A single network security protection technology and network security management method can no longer adapt to the big data environment, including terminal virus protection, system firewall settings, identification and user access control and other security protection methods, as well as network security strategies for IP at the network boundary network firewall, intrusion detection technology, security isolation, illegal external connection and illegal access monitoring, and gateways such as virus and spam filtering. Instead, from the user to the terminal to the network boundary to the data center, various security technologies achieve multi-dimensional integration in different positions of different objects. We should emphasize terminal control and data protection, emphasizing virtualization and security integration; in the protection of network borders, we will focus on access control for users, applications, and content. Through analysis of business systems, we will analyze security technologies, services, institutions, and processes. Optimize integration and fully realize the integration of security and technology, security and business, and security and management. Effectively implement the big data security concept, and cover network security to all aspects of network user's terminal equipment (user terminals and servers), transmission equipment (network switches, routers, etc.) and data center storage equipment, forming a powerful automatic defense, network security defense system with automatic repair and automatic learning.

2.3 Big Data Network Security Service Capabilities

Big data network security service capability is the guarantee of network security construction. Network security services are mainly around security product services, basic security services, and security operation and maintenance services. To provide reliable security products and services, the primary purpose is to vigorously develop network security products with independent intellectual property rights. China's self-developed network security products such as firewalls, intrusion detection systems and intrusion prevention systems, vulnerability scanning systems, and integrated network security gateways occupy a certain position in China. However, traditional security products cannot fully adapt to and eliminate the hidden dangers of big data, especially for latent and persistent APT network attacks.

Provide trusted basic security services. First, provide network software including trusted network routers, switches and other network communication devices, trusted computers, servers and other network terminal devices, trusted secure operating systems, secure databases, and secure applications. The second basic security service is to provide reliable encryption services and identity authentication mechanisms. With the large storage volume and multiple types of data storage generated by the big data environment, effective encryption means must be implemented. It is stored strictly in accordance with the requirements of data storage security, and big data transmission encryption is realized through a secure

transmission protocol, which provides effective protection for data stream upload and download.

Provide available security operations and maintenance services. In the era of rapid network development, slight irregular operation or illegal data may cause certain threats to the network environment used by users [3]. Therefore, the analysis and evaluation results must be determined by analyzing the security risks and defects existing in the network and the corresponding risk levels. According to the evaluation results and actual network security level requirements, formulate network security policies, repair, strengthen and optimize network security systems, and implement network security inspection, network security monitoring, and network security management. Once network attacks and damages are discovered, timely warning, response and recovery are conducted, and comprehensive security audits are performed.

References

[1] Shen Nan (2017). Risk analysis and preventive measures of enterprise accounting informatization in the era of big data. Business economy, no.5, pp.28-30
[2] Miao Dan, Wang Zhenyu, Chen Jianshu (2018). Application of virtual network technology in computer network security. Digital communication world, no.3, pp.200-201.
[3] Qin Chuan (2019). Network security analysis in the era of big data. Digital world, no.4, pp.144-145.