Threat and Countermeasure Analysis of Website Information Security Based on Network Security Technology

Bo Xu*

Department of Electrical Engineering, Yingkou Institute of Technology, Liaoning 115014, China

*Corresponding Author email: vipxb01@163.com

Keywords: Network security; Information security; Threat

Abstract: Computer network system is the basic environment to support all kinds of information transmission, interaction and sharing inside and outside enterprises. However, due to the interconnection, openness and loopholes and deficiencies of the network system itself. Starting with the definition of computer network security, this paper analyses the unstable factors of computer information network, and puts forward corresponding security countermeasures. The main problems of current network information security are analyzed from the aspects of network information security vulnerability, main technologies of network security, common network attack methods and countermeasures, and network security construction. Research shows that we evaluate site security from an attacker's perspective, including: information gathering, port scanning, privilege escalation, overflow testing, SQL injection, cross-site attacks, and web application testing. Research shows that combined with the development of information technology, the research on network information security technology prevention measures is improved, and the use risk of customers' network systems is actively reduced. Combining system operation with other security protection measures can more effectively prevent various types of virus intrusion.

1. Introduction

With the rapid development of computer technology, the development of today's society has been inseparable from the information network. Because the information transmitted by computer network involves finance, science education, military and other fields [1]. It contains enormous economic or national interests, so cyber attacks from all sides are indispensable. The manifestations of cyber attacks are also diverse. Protect the hardware, software and data resources in the computer network system from being destroyed, altered or leaked for accidental or malicious reasons, so that the network system can run continuously and reliably, and the network service can be orderly [2]. Computer network security includes two aspects, namely physical security and logical security: physical security means that system equipment and related facilities are physically protected from damage, loss, etc [3]. At the same time, a variety of Trojan horse programs also ravage the network, the old Trojan horse program after the "additional flower", "packing" after the increase in killing ability. These Trojans and viruses often enter the network unconsciously, enter the file information management system, lurk in it, and wait for an opportunity to commit crimes [4].

In 2013, the PHY layer method framework to defend against security threats in cognitive radio networks was studied by relevant scholars [5]. Since then, the persistent threat of network security has been proposed by relevant scholars [6]. Since the network of security evaluation in 2017, the persistence of advanced network threats has been studied by relevant scholars [7]. Network information security mainly protects computer system by establishing computer network technology system to avoid data damage, change and leakage in computer system [8]. From the essence of network information security, computer network security is mainly the security of information system. The network is an open platform, and government websites can be browsed by domestic and foreign Internet devices at any time. Once the website is attacked, the news is likely to spread rapidly by social networks, resulting in adverse effects [9]. The use of Trojans for information theft has

  DOI: 10.25236/eeems.2018.044

formed a huge industrial chain, and the huge interest temptation has further contributed to the proliferation of Trojan horse programs. These pose a threat to the existing archive information network. We advocate the construction of network security, and vigorously guarantee the security of network information is to protect the hardware and software of the network system. The main purpose is to protect the data in the system from being destroyed, altered, and leaked, and finally the entire network system can operate normally and provide services.

Strong security awareness is the precondition of website security. Many websites construction units do not know enough about the information security of websites. It is not clear that the website is a complex system, and website security involves design, development, operation, management and other aspects. In order to protect the transmitted data from being eavesdropped or modified during transmission, it is necessary to encrypt the data (encrypted data is called ciphertext). In this way, even if someone steals data (ciphertext), it can not be restored to plaintext (unencrypted data) because there is no key [10]. This ensures the security of the data. To determine the fault characteristics of each device, at the same time, it is also necessary to implement the fault filtering function, according to the priority of the fault, determine the processing mode to prevent excessive faults from causing flooding on the network. Fault management is divided into fault detection, fault diagnosis and fault correction from the operation content. The security status of archival information will also change. At present, a considerable part of the archive information website is constructed by outsourcing, and the technical level of network operators is relatively low. The ability to find problems and fix vulnerabilities is also weak, which also leaves the hacker with an opportunity. Therefore, this paper studies the website information security threats and countermeasures of network security technology.

2. Materials and Methods

We find that there are many ways of computer virus transmission, from floppy disk and CD-ROM transmission to network-based mode. Of course, you don't have to worry about viral infections to view documents, browse images or fill in forms on the Web. However, downloading executable files and receiving E-Mail files with unknown origins require special vigilance. In addition, LAN file or folder sharing also provides conditions for virus transmission. Standardized security management is the basic guarantee for website security, mainly reflected in the security management mechanism and personnel. According to the time of the user connection, the length of the network spanned by the connection, the user information, etc., an algorithm is used to calculate the usage of the network resources by the corresponding user, and the data is recorded in the accounting database. In terms of system, many units lack a sound website security system, and management information such as website information update, inspection, and backup is unrestricted. Some units have established a security system. The types of security vulnerability types on the website are shown in Table 1 and Figure 1.

Table 1 Types of security vulnerabilities in websites

	Number	Proportion
Bypass validation	5	11%
Weak password	2	4%
Cross-site scripting vulnerability	35	76%
Information leakage	4	9%

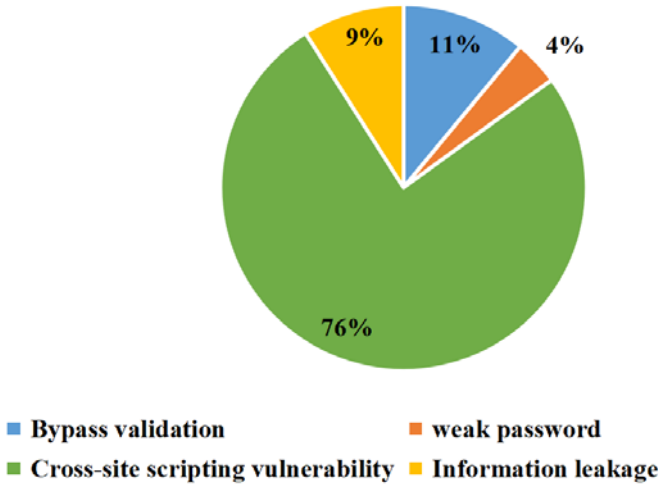

Figure 1 Types of security vulnerabilities in websites

Scientific management is the premise of ensuring network information security. Only by combining the reality of diversified construction of University websites, can we reverse the passive situation of lacking administrative functions in network centers, realize the new pattern of co-management of administration and technology, and realize standardized management, can we ensure the quality of website construction and promote its sustainable development. According to different data processing methods, firewalls can be roughly divided into two systems: packet filtering firewall and proxy firewall (application gateway firewall). Packet filtering technology examines each packet according to defined filtering rules and determines whether the packet matches the filtering rules. If the filtering rule allows, the packet will be forwarded according to the information in the routing table. If the filter rule rejects the packet, the packet is discarded. Establish mapping relationships between sensitive network resources and user sets. Data link encryption key distribution and management security log maintenance and inspection auditing and tracking to prevent virus disaster recovery measures. And some guidelines to detect intentional or unintentional illegal intrusions, take the necessary measures to investigate or track after detecting an illegal intrusion. The characteristics of network information security are shown in Table 2. The principle of packet filtering firewall implementation is shown in Figure 2.

Table 2 Characteristics of Network Information Security

	Function	Implement
Completeness	11.50	8.26
Confidentiality	13.20	9.65
Controllability	11.06	8.62

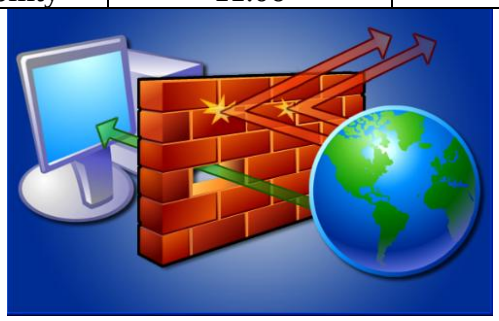

Figure 2 Implementation Principle of Packet Filtering Firewall

The openness of the Internet enables all individuals who have the ability to access the Internet to become both users and destroyers of the network. The consequences of intentional or unintentional intrusion into some e-government information systems are as small as the dismantlement of government mail, theft of government information, theft of state political, economic, military and

technological secrets, and paralysis of the entire government website. Integrity of network information means that in the process of transmitting, exchanging, storing and processing information, it is necessary to ensure that the data information is not modified and destroyed, and keep the original data information in the system. Timely vocational and technical training for network maintenance personnel to enable staff and users to have in-depth understanding of network security. The network management department should also use various opportunities in a timely manner to popularize the relevant knowledge of network application to the personnel of the unit, so that they can actively and consciously abide by various information system security systems and measures to prevent problems before they occur. In a sense, hackers are even more harmful to information security than ordinary computer viruses. Although the vulnerability of the operating system and various software can be overcome by the continuous upgrade of the version, a certain security vulnerability will make the previous upgrade work worthless. When the problem is discovered until the upgrade, a small loophole is enough to get rid of the entire network. The threat factors of computer network information security are shown in Table 3 and Figure 3.

Table 3 Threatening factors of computer network information security

	Transmission	Influence
Natural factors	22.05	18.92
Human factor	22.03	15.34

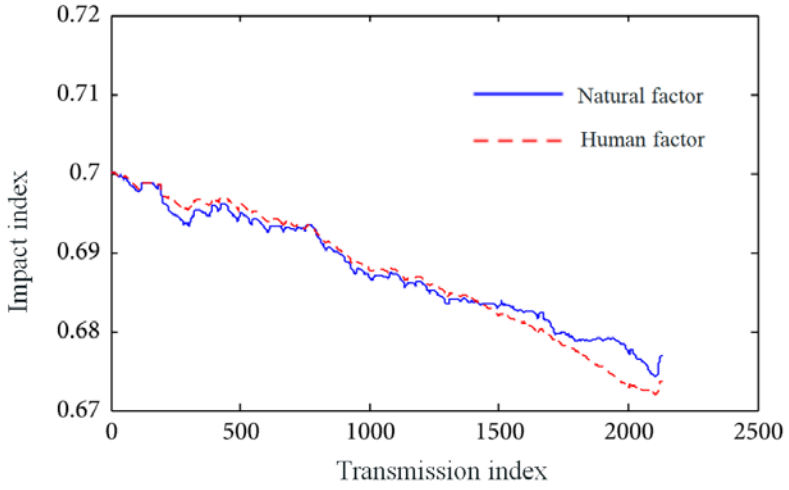

Figure 3 Threatening factors of computer network information security

3. Result Analysis and Discussion

The database system is the place where important information is stored and the task of managing these data information is undertaken. The security problem of database has existed since the birth of database technology, and has been deepening with the development of database technology. At the same time, the main consideration of the database is to facilitate the storage, utilization and management of information, but less security considerations. Physical isolation of one segment from another is achieved. In this way, the security of a network segment can be prevented from affecting the security of the whole network. In addition, IP address binding technology can also be used, that is, all MAC addresses and client IP addresses are bound.In this way, the IP address can be prevented from being fraudulently used, and the IP address management of the daily network is greatly facilitated. In a computer network system, the construction of the corresponding LAN cable and communication cable may affect the hardware in the computer system. Although natural factors have certain contingency, they cannot be ignored. Natural factors may pose a threat to a small number of network systems.

In order to evaluate the network security, we must first determine the quality of the indicators that affect the sub-characteristics. According to formula:

$$P_{t+\Delta t} = p_t + \Delta t p_t u_t(y) \tag{1}$$

By calculating the membership degree of different quality grades, the problem of indistinct boundaries between quality grades is well solved:

$$P_{t+\Delta t} = p_t\left(1+\Delta t u_t(y)\right) + p_t\left(1+\Delta t u_t(y')\right) \tag{2}$$

The membership function constructed is:

$$s_{t+\Delta t}(y) = \frac{p_{t+\Delta t}}{P_{t+\Delta t}} = \frac{p_t + \Delta t p_t(y)}{p_t\left(1+\Delta t u_t(y)\right) + p_t\left(1+\Delta t u_t(y')\right)} \tag{3}$$

Strengthening the security awareness of internal network personnel and improving the preventive ability of computer network information system are the basis of improving the security of computer information system. As a network manager, different passwords should be chosen for unauthorized users when accessing data and applying network resources, so as to make the operation of data legitimate. Key is the key data to ensure the security and reliability of encryption operation. According to cryptographic requirements, the key should be random and unpredictable. However, the key generated by the "vulnerability" algorithm is unqualified, and only 32 bytes of data can be collected to predict all the keys, and these keys can be used to decrypt all the encrypted data to obtain information. If the information system uses related products with "vulnerabilities" algorithms, it can be easily intruded and directly threaten information security. Guarantee the security of file information data. At the same time, we must also do a daily backup of the file information data, in order to prevent the file information network from being attacked quickly to recover data and ensure the normal operation of the network.

When making a comprehensive evaluation according to the formula, first make a single factor judgment:

$$s_{t+\Delta t}(y) = \frac{p_{t+\Delta t}}{P_{t+\Delta t}} = \frac{s_t(y)\left(1+\Delta t u_t(y)\right)}{s_t(y)\left(1+\Delta t u_t(y)\right) + s_t(y')\left(1+\Delta t u_t(y')\right)} \tag{4}$$

Normalize the quality of the indicator:

$$s_{t+\Delta t}(y) - s_t(y) = s_t(y)\frac{\Delta t u_t(y) - \Delta t \overline{u}_t^{\,p}}{1+\Delta t u_t} \tag{5}$$

According to the formula, the quality of safety can be calculated as follows:

$$S = 2L + W = \frac{c}{2f\sqrt{\varepsilon_{eu}}} \tag{6}$$

Computer virus is an important aspect of network information security. It mainly destroys the data in the system by manually compiling the program in the computer system, thus destroying a group of codes of the computer system function. There are two kinds of viruses: benign viruses and malignant viruses. Viruses can replicate themselves and choose effective anti-attack security facilities. Archives information management system should choose hardware products with good quality and high credibility, and choose appropriate network configuration according to the specific types and requirements of the network. Program vulnerabilities can cause damage to data files, and hardware errors can damage the entire disk. Damage caused by file loss can be large or small, and repairing is very time consuming. To ensure that no files are lost, the basic responsibility of the system administrator is to copy all the files in the system to other locations. Administrators also want to ensure that backups occur in a timely manner, and that backup tapes and other media need to be securely stored. Establish a safety management system. Improve the technical quality and professional ethics of personnel including system administrators and users. For important departments and information, strictly check the virus and check the data in time. Enhance settings for network directory and file access permissions. In the network, files that can only be executed by the server are restricted. Scanning the same port to a certain number of hosts at a certain time is shown in

Figure 4.

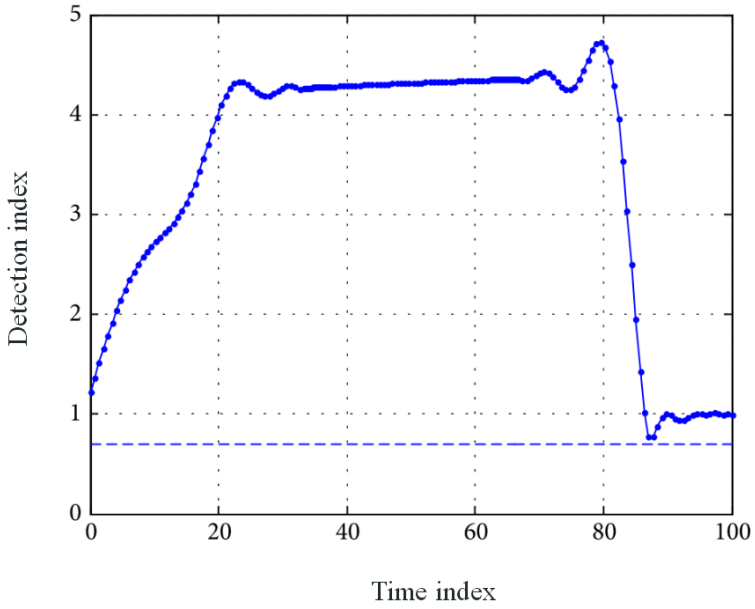

Figure 4 Detection scan

4. Conclusions

Because of the development of network security products, computer hardware and software, and the development of virus and hacker technology, network security is dynamic. Therefore, network and information security should be the integration of technology and management. In addition to taking some technical security measures, we should also carry out network security education for internal users, establish and improve various management systems, and seriously deal with acts that threaten and destroy enterprise information and data security. Now we only need security construction on our own level. In the future, we will need to build security as a whole. This is the transition from a certain point to the overall situation. The development of the entire network security will change from "network security" to "application security", and the discipline of security management will be hot. Capture data frames from the network, and filter, interpret, and analyze the source, content, and other information of these data, and record them for later review. At the same time, once the attack behavior is found to be able to sound the alarm in time, the security of the file information data is ensured by automatically shutting down the server and cutting off the physical line in an emergency. Therefore, under the new situation, it is particularly important to strengthen the research on network information security technology.

References

[1] Jouini M,Rabai L B A,Aissa A B.Classification of Security Threats in Information Systems[J]. Procedia Computer Science, 2014, 32:489-496.

[2] Lin H,Yan Z,Chen Y, et al. A Survey on Network Security-Related Data Collection Technologies [J]. IEEE Access, 2018:1-1.

[3] Puthal D,Mohanty S,Nanda P, et al. Building Security Perimeters to Protect Network Systems Against Cyber Threats [Future Directions][J]. IEEE Consumer Electronics Magazine, 2017, 6(4):24-27.

[4] Khan N,Al-Yasiri A.Identifying Cloud Security Threats to Strengthen Cloud Computing Adoption Framework[J]. Procedia Computer Science, 2016, 94:485-490.

[5] Wen H,Li S,Zhu X, et al. A framework of the PHY-layer approach to defense against security threats in cognitive radio networks [J]. IEEE Network, 2013, 27(3):34-39.

[6] Brewer, Ross. Advanced persistent threats: minimising the damage [J]. Network Security, 2014, 2014(4):5-9.

[7] Yang L X,Li P,Yang X, et al. Security Evaluation of the Cyber Networks Under Advanced Persistent Threats[J]. IEEE Access, 2017, 5:20111-20123.

[8] Wolf M,Minzlaff M,Moser M.Information Technology Security Threats to Modern e-Enabled Aircraft: A Cautionary Note[J]. Journal of Aerospace Information Systems, 2014, 11(7):447-457.

[9] Karoui, Kamel. Security novel risk assessment framework based on reversible metrics: a case study of DDoS attacks on an E-commerce web server[J]. International Journal of Network Management, 2016, 26(6):553-578.

[10] Trabelsi Z,Zeidan S,Masud M M.Hybrid mechanism towards network packet early acceptance and rejection for unified threat management[J]. Iet Information Security, 2017, 11(2):104-113.