Computer Network and Information Security Strategy and Analysis

Xiaoshai Shi

Yancheng Kindergarten Teachers College, Yancheng, Jiangsu Province, 224000, China

Keywords: Information technology environment, Information Security, Problem and solution

Abstract: Computer network, also known as website, is penetrating into our daily life along with the sky-rocketing development all over the nation. At the same time, it also brings us a lot of problems, which inevitably have a great impact on society. This paper focuses mainly on security problems of website nowadays and moreover, and proposes some pertinent strategies.

1. Introduction

Nowadays, information technology gets more and more functional, and thus computer network is applied to many fields, accounting for a large part in our work and life. However, with wide application of the Internet, a lot of problems are aroused, causing threaten to Information Security and potential risk everywhere. Especially in some areas where computer network is frequently used, many terminals connected to the Internet is vulnerable to attacks, which attracts more and more attention and remains an unsolved problem. Soft Engineering is generated based on this big trend to ensure that personal computer could avoid these attacks, by developing some techniques like firewall, channel control system, agent server and intrusion detector. Even though, hacking PC is still rampent in both developed and developing countries, which largely spoils the sense of safety among society. Under the current circumstances, more intensified hacker activities force more people to join the hacker team, increasing the difficulty in protecting PCs from attacks.

Computer Science is a complicated system, covering program design, server management etc. Above all, Information Security has won the priority, playing the basic role of keeping PCs work normally, which also bring about that research in Information Security field is exclusively important. Therefore, we are going to discuss the status quo, solution to existed problems in this area in the following passages.

2. Strategies for Information Security on Website

The new definition of Information Security of Computer Network is to maximizing the probability of avoiding attacks from the Internet. Moreover, the core concept of Computer Network and Information Security is ensuring the safety of information and data, protecting computers from vicious attacks from the Internet, leaking and damaging personal information. Normally, the Internet should guarantee data integrated, continuous, reliable and classified, while Information Security has many remained severe problems in our daily life. As one of the critical problems to solve, network safety problem, which arouses peoples' attention, has many reasons for increasing number of its occurrence, including the Internet internal and external influences. Therefore, it is an impeding hot issue in the whole society that how to launch profound researches and discussions of Computer Network to secure the safety of the information on the Internet. It is valuable to solve the problem of Information Security on the Internet. First and foremost, with the broader using of computer network among different social roles, permeation and share of information has been leveled up, not only enhancing the work efficiency, but also boosting the development of many industries. Exposing information on the Internet to interception and attack will cause the loss of group or individual to different degree, which reminds people that keeping information safe is an enhancing key factor. Secondly, the Internet requires its extremely high confidentiality, playing a critical role on the development of the whole industry. Once some important message is leaked, besides the bad influence on the victims, it will moreover bring out the clue of evil events. On the

  DOI: 10.25236/isaicn.2019.087

other hand, if Information Security on the Internet remains a problem for a long time, it will cause a huge potential black-swan risk to a national government, national owned companies, and other bureaus, arousing many negative factors to threat to the national safety. As we can see, whether individual, group or even the whole nation, ensuring Information Security is exclusively important.

3. Main issues on Information Security

3.1 Improper Operation by Internet User

Improper operation is one of the main reasons for personal information leakage. A large part of PC users is lack of enough conscious of Internet Safety, neglecting Information Security problems when surfing the Internet, which cause many uncovered opportunities of information leakage. When doing business online, many users will deliver their genuine information to developers, offering great chances to evil vendors or hackers to commit crime, like obtaining user's information via network flaw to impair users' Information Security.

3.2 Leakage of Information and Potential Risk of Security by Hackers

Interne hacker is the one who gains important information on the Internet via technology flaw illegally, through two main ways by human manipulation, active attack and passive attack. Active attack means hackers intrude private information and damage data through some specific approaches. Passive attack means hackers intercept users information illegally when information is being conveyed. This action is secretly exerted and often neglected, but always bring huge risk to the Internet users. Human manipulating attack is mainly through detecting the network flaws, which will easily cause Computer Network system paralleled and have a great negative impact on Information Security.

3.3 Threat of Data and Information Security Affected by Virus

In recent years, improving completeness of network system and increasing penetration of computer virus, more ways of commitment has been developed. Computer virus, along with free software, could be attached to PC when users download these resources from open website. And for its self-replicated character, it is hard to be eradicated once PC is affected. On the other hand, the changing ways for computer virus permeation, brings big challenges to network safety defenders. For example, traditional Trojan Horse virus is becoming a new prevailing form, and influencing our network safety and real life profoundly, which should arouse our attention.

3.4 Spam and Stealing of Information

Computer Network technology brings a lot of convenience to people life, at the same time, also generates a lot of redundant information. When using email, we can easily detect some junk mails which do not include any useful information. Besides, spam software is also growing its number, usually disguised as the normal one to surveille and steal users information secretly, threatening their property safety. Junk mail and spam software impact the development of Computer Network, which should be the focus.

3.5 Lack of Completeness of Information Security Legislation

Computer network develops rapidly in the last decade, and yet it has not been established a complete legislation among the industry, which means the problems above is stilling threatening our property safety. It is recommended we should form up a Network Information Security Expert Group to constitute a regular to secure the benefits and even basic human rights of computer users.

4. Enhance the Safety of Information Security in Big Data Era

4.1 Keep Firewall and Security System Working More

Firewall is one of the earliest technologies to protect the Computer Network safety, and broadly

used in various systems, keeping user data safe powerfully. Firewall builds a digital sieve to percolate the harmful information from the Internet mainly through a set norm. When detecting bad data influx, it could process and prohibit them from damaging PC. Most Firewall software could enhance the success probability of intercepting suspect information through the combination of dynamic and static data analysis. Some other prevailing technologies like packet browse filtering are also widely used. Firewall technology is separated into two categories, namely packet filtering firewall and proxy service firewall. There are some differences between the two, especially in protection ways. Packet filtering firewall is the way of percolating information through a set regulation, which includes important network information including IP address, transmission source destination port, etc. It will transfer and then percolate the suspect information according to the relative catalog after comparison and selection. Proxy service firewall is setting an intermediate server between the Internet and users. All of the information conveyed to users must pass the proxy server to test its reliability, making its interaction to users indirect. In which case, users Information Security have been ensured to some extent. Proxy server firewall always has its good property of protection and is better at identifying and processing the dangerous information, which leads its wide using among the Computer Network system.

4.2 Implement the Safe Access to Websites

It is important to pre-detection before user enter into the Internet, since such detection can protect user from cyber criminal attack effectively. Network administrator plays a critical role in user setting, in other words, user log in at network administrator should be encouraged. By doing this, administrator could monitor user's surfing range, and urge user to keep his or her own passwords to the Internet and renew it regularly. Besides, network administrator should restrict the abuse of the Internet through some specific approaches. For example, they should have the right to close accounts temporarily or adjust them according to the realistic scenarios. This facilitate the case that access could be terminated when the account is closed and be regained when the account is activated by administrator. Another example is workstation limit, which is a scheme that user's access, time spot to the Internet and span of surfing the Internet is determined by workstation confirmation.

4.3 Deliver Skills of Protecting Computer and Account against Virus

Development of the Internet security protection technology is pretty important, however, enhancing user conscious of internet security is vital to this problem. First of all, user should grow a good habit of using the Internet, amending flaws and updating virus database among the whole Internet system, to ensure PC could run safely. On the other hand, user should set different keys to different accounts, know and command the framework and principle of the network system. Besides, different users should be allocated different access rights to prevent the important documents from being stolen and damaged. Although Inter security protection is very important, ensuring a thorough protection among the large variety of network activities is very hard. This requires users to improve their own sense of Information Security, learn the knowledge actively and enhance their own ability to the outside activities.

4.4 Apply the Digital Signature and File Encryption

User should regard account setting as the fundamental work when using computers. Firstly, for example, setting more difficult and complicated passwords, along with regular adjustment could ensure PC to run in relative safe range, and thus minimize the probability of the case that PC is attacked or personal information is stolen by illegal hackers. Furthermore, enhancing the frequency of updating the virus database of anti-virus software is another powerful way, especially in prohibiting some strong Trojan Horse program. This means anti-virus software is prevailed widely because of its fast-speed updating of virus database and powerful prohibition from attack, leading its important role in Internet security work. Last but not least, such skills should be improved like the knowledge on computer virus and sensitivity to hacker activities. It could be seen that Information Security would be more completed if each user could boost their own sense of defend.

4.5 Digital Signature and File Encryption Technology

File encryption is a critical move on keeping PC safe, generally including end-to-end encryption and route encryption. Another way is to encrypt on the process of file transmission, which on large account for protecting PC Information Security. The second main approach is to transmit words into cyber, which is implemented by using different software to encode and decode. At the same time, we should keep an eye on developing information storage encryption, which is a frontier way of guarding the data from a wide rage stolen effectively. This approach use encryption templating technology to monitor the internal Information Security. Finally, detection on information integrity has been unveiled its significant progress, which allows agent to testify whether user meets the requirements or not by keys or passwords verification.

5. Conclusion

As these mentioned above, the normal operation of Computer Network can not be striped of data and information protection. In order to speed up constructing the Network Information Security, conglomerates, national-owned companies, intermediate or even small businesses should release different policies to cope with the potential risks and problems among the whole process of dealing with data. All in all, ensuring the integrated Information Security needs the efforts from all parts of the society.

References

[1] Cundong Huang, Technical Research on Computer Network Information Security Issues [J] Software, 2003, 34(1):140-141

[2] feifei Xin, Kai Liu, Research on Computer Network Information Security Issues and Protection Measures[J]. Jiamusi Education College Journal, 2013(12):442-442, 446

[3] Baoqi Bai, Analysis on Computer Network Information Security Problems and Prevention [J]. Commodity and Quality, 2015(40): 33-33