Analysis and Countermeasures Research on the Computer Network Security at the New Stage

Qi Wang

Xijing University, Xi'an Shaanxi, 710123, China

Key words: Computer, Network security, Analysis at the new stage, Countermeasures, Research.

Abstract. At present, the computer network security has become a global problem, it is because of this open characteristic of computer network, the risk of infringement is increasing. Even at home and abroad the prevention and management of computer network security have been improved, network security always needs to be addressed. Under the background of the new stage, the computer network security problems also present new features. Therefore, we must pay more attention to the problems and take measures to solve them. The article will take the computer network security as the research focus, elaborating the analysis of network security and putting forward the targeted measures for reference.

Introduction

Since reform and opening up, especially the domestic organic combination of industrialization and informationization has further promoted the development of computer network as well as provided a strong guarantee for economic and social progress. However, the current domestic computer network security problem is very serious, and cyber crime problem often appears, this has led to serious loss and brought about negative impacts. Whether social organization or the people, in the process of application of computer network, once ignoring the important role of prevention and management, the probability of invasion will increase while ultimately the running of the system will be affected and the loss is immeasurable. And under the background of the new era, the computer network security also has new characteristics, therefore, we must have correct cognition of the characteristics of computer network security at the new stage, only in this way the normal work of prevention of computer network security can be ensured.

The explanation on computer network security at new stage

Network security threats present a trend of intelligent development, therefore, the computer network security also enters into a new stage. The so-called new stage, specifically embodied in aspects such as the network and system interconnection gradually increased, more value targets, attacker's motivation more diverse etc. And the research and analysis of network security has been transferred from network worms to Trojan hackers, then to the research of the botnet, and even failure of the supply of the router and colony technology and digital cannon, etc. At the same time, the mode and technology of destruction and attack are also rising. In the process of the development of information technology, more destructive ideas at the new stage will also form, so, the scope of actually attack will also expand continuously[1]. Under this background, the people will also pay more attention to the network security threats. Through the analysis of network security events it can be found that network threats have entered into a new stage. Therefore, the traditional professional technology has been difficult to meet the specific requirements on the aspect of prevention and control of network security threats mainly because network attack methods are more diversified. Therefore, the management staff must learn new network security technology to ensure better responding to the computer network security problems at the new stage.

In the new stage of the computer network security, traditional experience and professional technology are difficult to meet the specific requirements. Thus it indicates that the network security has been changed with the arrival of the new stage. So, compared with the network security problem before, attacker's motivations and goals and even abilities have been changed, completely different from the network security threats before. Under the background of the continuous development of science and technology, the network attack motivations also present the differences, while threats have also been changed. The following will be research and elaboration on motivations of the destroyers from four attack stages:

The first stage: before 2004. At this stage, the attacker's destroy motivation was making influential attack. Among them, the relatively typical events are Amazon attacks and Red Code event, and so on. And the incidents above are sensational, already spread in the communication industry and the computer industry, etc, besides also having adverse effect on the destroyer's action.

The second stage: from 2004 to 2007. At this stage, the attacker's main purpose was to make money, more common was the appearance of the phenomenon of network fraud. In addition, most websites with nature of business also gradually applied by underground industry chain, by way of attack taking the place of normal operation competition.

The third stage: from 2007 to present. At this stage, there was a certain difference between the attack at present and that of before, embodied in the aspect of secret stealing. In this case, people would have comprehensive protection on the valuable content through the way of password setting. However, the attacker could use more ways to bypass the password settings[2]. At the end of 2007, there had been a lot of Internet leak problems. Thus, in addition to business, network secret leak in many industries had already been spread through the network. However, the attacker's goals and ways were different.

The fourth stage: the new stage. There are certain differences between the ways of network secret leak, while the main purpose of the network attackers is not only for secret stealing. Under this background, the network attack is different from before, even if 99% existed security threats have been found, the remaining 1% are ignored. It also becomes the attacker's main goal, eventually bringing immeasurable loss.

Through the above research and analysis, network security threats of the new stage have certain crypticity, likely to have been hidden for a long time while management staff have not found. Only when the damage becomes more obvious and threats level becomes greater, managers could begin to realize the importance but have been powerless. At this stage, the understanding of the ways of new network security threats is not deep, so, the adopted measures are difficult to meet the practical needs. In this case we still need to attach importance to network maintenance work to avoid unnecessary bug risk. The most important thing is to focus on network management staff's professional knowledge and skills training.

Analysis on the computer network security at the new stage

The main reason for in-depth analysis of computer network security problem is the open characteristic of the network. The vast majority of criminals can use network technology to attack and destruct, eventually making a lot of potential safety hazard of computer network, while threat level deepened thereupon. Among them, the relatively more common threats include five kinds, they are physical threats, system threats and identity authentication, network connection and the threats of virus programmes. In the new stage, especially, the main characteristics presented by computer network security include three types:

The user's safety awareness is weak

At present, under the background of the development of computer network technology, network security event risk is increasing constantly, and at the same time constantly exposed under the action of the media, the economic losses brought by which are incalculable. However, the recognition of security issues of computer network by many of the social organizations and the public is not clear. Even if the corresponding preventive measures have been taken, in the overall perspective, the emphasis has always been inadequate. Among them, taking enterprise and public institution as an example, there are few of them taking computer network security into the enterprise internal management work content. And uploading and downloading at will often appear, the key is the use of copyrighted software. On a personal point of view, for the electronic bank accounts and online shopping and many other aspects, the consciousness of security and protection does not form. It is also because of negligence, more damage criminals take this opportunity to destroy network security[3]. Thus, the absence of consciousness of computer network security in computer network security at the new stage has become a prominent characteristic as well as a very obvious problem demanding prompt solutions.

Network criminal incidents occur frequently

Influenced by the open characteristics of computer network, especially huge numbers of Internet users at present, therefore, the computer network has gradually become a key platform as well as carrier for people to work and study and even for the daily life and entertainment, throughout various fields. Based on the analysis of the current computer network criminal situation, a vast majority of users have been invaded or phished. The relatively common place been invaded or phished are game accounts or electronic bank accounts, etc. These places have bigger infringement chance than others. This also leads to serious negative impact as well as incalculable economic losses.

Hacker technology developed fast

In the process of the development of computer network, hacker technology also spawned and developed with the computer network development. Hacker technology is also a kind of product of scientific informatization, and under the condition computer network entering into a new stage, hacker technology is changed accordingly. Domestic commercial and trade pattern in the field of computer network has been showing a trend of continuous innovation, while hacker technology is under continuous development, all these make more criminals by any kind of means while pursuing their own interests to steal the network user's data and information content through the application of variety of virus programmes such as Trojans, spywares and worms etc. Even the anti-virus software can effectively play its function, the hacker technology also presents a development tendency. So, the hacker technology brings unfavorable effects in computer network security.

Coping strategies for the computer network security at the new stage

Coping strategies on technique

The factor which has direct impact on network safety is the effect of the structure design of the network system. First of all, continuously strengthening the access control, only in this way the normal operation of the computer network system can be ensured. Among them, on protection and guarding against network security, the specific way is access control. The main purpose of access control is to protect network resources so as to avoid the access by unauthorized users. Besides, it is also the most critical strategy in network security. Second, paying attention to facility management. On the basis of enforcing access control, unauthorized users should also be avoided to enter a computer to sabotage. Therefore, the computer system and network servers, and even printers and peripheral equipment etc. must be protected comprehensively. In addition, the environmental conditions where equipment placed should also be checked regularly with more efforts, especially check on whether temperature moderate, network wire damaged, or the power supply normal etc. Based on this, computer system must be regularly updated, especially update of the firewall software, bugs also needed to be scanned in time[4]. Finally, in the new stage, the computer network security has presented brand-new characteristics, therefore, in order to increase the security degree of computer network, the network security technology innovation must be promoted. State and the related IT enterprises shall attach great importance to the innovation of the network security prevention technology, especially in the area of digital signature and digital certificate. This has a significant effect on improving the computer network security. The country also needs to constantly encourage the effective innovation of the computer network security technology, strengthening the support on policy and funds, and other aspects to ensure the comprehensive innovation of computer network safety technology.

Coping strategies on laws and regulations

During the Fourth Plenary Session of the Eighteenth, the guiding thought and working goal of governing the country according to law had been put forword, at the same time the main work and concrete measures also pointed out. Under the new era background, the computer network security prevention work must be paid much attention to. And so security of computer network should also enter into the development orbit of legalization, while the laws and regulations of computer network security should also be established and improved. In this case, the country needs to improve the importance of computer network security problems, strictly reorganizing the present laws and regulations of computer network safety, introducing computer network security law as soon as possible to provide powerful guarantee for computer network security methods and management work to make it enter the development orbit of legalization, ensuring computer network security management work carried out more smoothly.

Coping strategies on computer network environment

In the new era background, in order to effectively protect the computer network security, the key point is to build a harmonious computer network security environment and atmosphere, especially to enhance the social organizations and the public themselves' awareness of computer network safety[5]. In this case, the state and governments at all levels, and even the related departments, all need to vigorously promote and guide the computer network security, using the media to show the important role of computer network security, highlighting the dangers of potential safety hazard, exposing computer network security events in time to improve the social organizations and the public's awareness of computer network security as far as possible.

Coping strategies on virus prevention

The existence of computer network security problems seriously affect the operation of the computer network, especially computer virus which is very dangerous. Therefore, in order to be able to strictly guard against computer viruses, user's awareness of prevention must be improved, this must be paid attention to, targeted preventive measures must be selected, specially, the legitimate anti-virus software shall be installed, and virus reservoir shall be updated in time. In addition, data, programme or video not allowed to download and link whose resource is not clear, unknown emails can't be opened at will. As for downloaded software, visus must be killed first before use. In addition, one must form a good habit of surfing the Internet and should not open the pop-up ads in the web page.

Conclusion

To sum up, under the background of economic integration, the development speed of international science and technology information has also gradually been improved, and computer network has also made ideal results, but also making the computer network security at the new stage faced with new features and problems. Because of the obvious opening characteristics of the computer network, it is easy to be attacked and damaged. So, the degree of emphasis of computer network security problems must be improved. Under the background in the new era, the new characteristics and new problems of computer network should be fully cognized, reasonable measures taken actively to promote the construction of computer network security. On the basis of constant perfecting laws and regulations, creating secure network environment and strictly guarding against the virus, comprehensively innovating security technology to provide strong guarantee for the safety of computer network operation.

References

[1] Wang Liang. Computer network security analysis and coping strategies at the new stage, *Journal of coal technology*, 2013, 32 (3) : 208-209.

[2] Xu Xiaoguang. Computer network security analysis and coping strategies at the new stage, *Journal of communication world*, 2016 (12) : 16.

[3] Mo Nian Fa. Computer network security analysis and coping strategies at the new stage, *Journal of the technology wind*, 2015 (3) : 230-230.

[4] Min Shengli. Factors affecting the safety of computer network and the coping strategies, *Modern industrial economy and information technology*, 2016 (8) : 88-89.

[5] Wang Xiao. Factors affecting the safety of computer network and the coping measures, *Journal of Heilongjiang science and technology information*, 2014 (26) : 187-187.