I.J. Engineering and Manufacturing, **2012,4, 49-53**
Published Online August 2012 in MECS (http://www.mecs-press.net)
DOI: 10.5815/ijem.2012.04.06

Available online at http://www.mecs-press.net/ijem

Proactive Security of E-business

Wu Huanwei

Huaihai Institute of Technology, Lianyungang City, Jiangsu Province, China

Abstract

After giving a brief statement to the theory of proactive security, based on the differences between passive defense and proactive security, the article describes the main idea about the proactive security theory of e-business network from aspects of network environment, security technology and service, network management. At the same time it analyses the barriers existing in the actual use of proactive security in e-business network.

Index Terms: proactive security; e-business; network security; passive defense

1. Introduction

Network security is a crucial problem in the construction of e-business. As the improvement of network openness, sharing and interconnection, the security problem is becoming more serious. However, with the rapid development of e-business, more security requirements are needed for new business patterns and services. Most products of "passive defense" don't have the ability of "proactive security"; the attack of hacker and virus often adopts new methods so that the network cannot make any response under unknown attack and often leads to severe losses. So it is important and valuable to study proactive security of e-business network.

At present there are two difficulties about network security: one is the attack's "rapidity". It probably takes one day from the crack being discovered to the first wave of attack; perhaps the virus will infect thousands of computers in several hours. The other is the comprehensive threat, which refers to attack method and transmission way. First, network often faces the attacks launched by virus, worm, troy horse, spy-ware, as well as inner threat. Secondly, there are various ways including email, resource sharing, immediate news etc. Network needs more advanced, comprehensive technology and product from the attack. On this condition more people put forward the problem of "proactive security", who are unsatisfied with the present and wish to ensure the security of network[1].

* Corresponding author.
E-mail address: Wuhw6@139.com

2. Concept of "proactive security"

2.1. Understanding of "Proactive Security"

Seeing from technological development and practice, isolated technology or product can not meet the need of system security. The system must be established for better protection, in which there are relative technique, security policy and e-commercial self-management to protect information security and network availability; no matter anything happened, e-commerce user's primary services will not be interrupted. Generally speaking, such system does not focus on certain technology and product, but the whole safety effect, which is so-called proactive security.

In the system of proactive security, there are four crucial parts: first, early warning, very important part of the system; secondly, safety protection, the most basic requirement of the system; thirdly, emergency response, the necessary part of this system if any security problem happened; lastly, security management, including user safety, strategy and product assignment etc.

Based on the above knowledge, the author thinks: first, proactive security is not a single product or specific technology. From the point of security, technology is only a part of proactive security. Secondly, proactive security is not to adopt many techniques in a product or several products and it can prevent any attacks, which is also a mistaken idea of proactive security. Thirdly, proactive security not only can prevent various viruses but also contain other elements. In a word proactive security is a brand new idea of network security, which focuses on open-ended, all-inclusive and preventive protection against system.

2.2. Contents of Proactive Security

There are four parts in the proactive security.

1) Early warning: Under present security environment, different network can face the same problem, so the system of proactive security needs to help network manager understand what he sees, that is, early warning. Through timely alert, network manager can realize all the situations, potential security leaks and how to eliminate the threats.

2) Information security: There are a great deal of information in e-business network, including digital product information, customer information, dealing information, payment information, e-business management information and network management information etc. When network manager believes he is facing threats, the system of proactive security can ensure the safety of all the information.

3) Emergency response: Security problem can happen any minute. If it were true, effective emergency response would limit possible damage. Emergency response is not simply to deal with security incident passively, but make emergency action or do anything else before it.

4) Effective management: Effective management have very good effect on the comprehensive security system, because it could know what are happening, or what will happen, or what has happened in the network and take effective measures in good time. There is also network itself security and strategy, as well as allocation of concrete products.

3. Technology and service of proactive security

The reasons why network is easy to be attacked are below: first, the time of virus outbreak or the crack to be attacked is getting shorter and shorter; secondly, the safety system packed with various products and plans cannot prevent all the dangers and perhaps only a crack will cause total collapse. Obviously, the old passive defense is doomed not to continue, so the network security needs a new idea in technology and service.

3.1. On the Technology

Passive protection not only makes network security lose its decided advantage, but also makes the communications of different security products become the weak point of the whole system. As for proactive security, it is necessary to break the old pattern of passive protection and create a flexible and reliable network environment. Different e-business systems have different requirements for network environment because of different services, yet the main reliable environment is all the actions and results can be predictable and controlled.

For e-business system, "reliable network" can at least lead to a new idea about network security: it is not an absolutely safe network that users care about, but how to ensure all the information and services carried by network are normal, safe and reliable. Though there are many security shortages in present network, if customer's visit and digital resources can be ensured by proper security strategies, it is thought to be a safe network which can meet customer's requirements[2].

3.2. On the Services

In recent years, an inevitable trend has appeared in network security that visible security products are becoming increasingly blurred; users need a "safe" network and "sustainable safety" guaranteed by professional services. In a few years there will be no independent security products in the market and the security demand will be switched from good products to reliable services. This change shows in e-business network security: first, "passive defense" should be changed into "proactive defense", that is to say, risk management will take the place of the action of discovering problems and solving them; secondly, network security will develop into "centered management" from "isolated product". Along with the development of e-business network, people have realized only security product is not enough; professional services are becoming an important part of network security, which has been a crucial element to appraise the firms. Security vendors have taken personalization services in e-business as the focus on the competition, even permit users to have a free trial of security products. Seeing from these changes, as far as security essence is concerned, security industry is the service industry, which is the inevitable result that the proactive security reflects from the technology to the market.

4. Management of proactive security

Technology and service is important to proactive security, however, effective management is the key force of network security. The common knowledge of security area, "30 percent technology, 70 percent management", fully shows the importance of management.

E-business network is usually very great and the biggest threat is always the inner persons. For the sake of simplicity, there is no much defense to inner persons; in addition, some staff is familiar with network more than anyone else, if someone had bad ideas, he would make fatal loss to the network and resources easily. More and more e-business enterprises have begun to realize this and tackle the threats squarely[3]. Most network safety devices has spied on the questionable activities in the network and warned or forbidden them. But inner threats always are what anyone cannot despise for e-business system. No one can ensure that anyone will not become desperate out of own benefit. After all, the most difficult thing in the world is to know man and control him.

4.1. Management of Equipment and Behavior

It is well known how much the internal staff may do harm to network, intentionally and unintentionally, which cannot be predicted beforehand. Therefore, it is necessary for network inner management to take preventive measures according to "proactive security". For instance, management of three ways of leakage of

information as mobile devices, peripheral units and network behaviors must be made. The identity authentication technology in the generally used mobile devices (mobile disk, u-disk, SD/CF card); access control, data protection and log files on all the interior important information storage and transmission; centralized management control mechanism; careful audit analysis report and so on, all the above will protect the important digital resources, the literature information and the functional software effectively.

4.2. Management System of Proactive Security

First, good system of information management should be built, as well as basic safety supporting system. Based on distributed e-commercial framework, VPN must be used to build up the connection between the enterprise and the long-distance users, branches and equipment providers, which ensures safe transportation of data, and, in turn, expands the intranet of the enterprise. Secondly, there should be institutional safety system and can be carried out effectively. Thirdly, the leaders attach great importance to network and information security. Among the above, it is the most difficult how security management system is built effectively and carried out well. This refers to e-commercial management style, service mode and safety dependence.

4.3. Security Risk Evaluation

First of all, network managers must learn the most important risk, for instance, what behaviors could lead to losses? What losses? Which safety action aims at the main function? On this base, by means of monitoring and correlation analysis on network resources and behaviors, network security view can be obtained after security conditions have been analyzed in the whole opinion.

4.4. Thorough and Detailed Security Policies

Network security strategies must be carefully applied to all safety equipment for the desired results. For the large e-commerce network, it is a complex course and very error prone to create and maintain safety regulations. As time goes, the maintenance of a huge quantity of safety regulations will turn out to be heavy burden, and it is very easily for webmasters to make mistakes. As safety devices, routers and switch requirements have their own filter language, if artificial set, only the experts can finish it. Moreover, the design of rules is dull and easy to go wrong; if the rules are more than several hundred, it is much easier to go wrong. So it is necessary to have an automatic system of management and abandon the conventional way[4].

5. Conclusion

Although proactive security has the possibility in the theory, technology and products, as well as there are more and more discussions about it, it is a complicated course and the outlook is hard to predict.

There are two important reasons behind this.

First, despite that e-commerce network has accepted the concept of “proactive security”, “overall defense”; it is far from the specific implement period. Proactive security needs strong safety strategies and rules to support, however, many e-commercial firms don’t understand the application rules and configuration of firewall, let alone integration and management of numerous equipment. Furthermore, e-commercial safety products come from different firms, which make the coordination hard to finish.

Secondly, a set of network with proactive security is not a security product or safety technology, but an organic, overall and systematic solution. This involves many security vendors’ different products. In fact it is a problem of industrial environments. On the national level, there should be a widely recognized security framework, based on which national standards of security technology and service should be made; from the level of firms, a vendor coalition should be built through communication. It will be a long time before the above

conditions come true. But at any rate, the network of proactive security with self-immunity has showed an ever clearer outlook.

Acknowledgment

The author sincerely thanks his family, for they are his strong support.

References

[1] Abdoul Karim Ganame, Julien Bourgeois, Renaud Bidou, Francois Spies. A global security architecture for intrusion detection on computer networks[J]. Computers & Security, vol. 27, pp. 30-47, March 2008.
[2] Gunilla Widen-Wulff, Reima Suomi. Utilization of InformationResources for Business Success : The Knowledge Sharing Model [J] .Information Resources Management ,:pp.46 – 67, 2007, (20).
[3] Huo Guoqing. Enterprise inforrmation integrated management[J]. Journal of the China Society for Scientific and TechnicalInformation, pp.2-9, January 2001 (in Chinese).
[4] Liu Ping. Research on a Management Model of Enterprise InformationResources[J]. Journal of Wuhan University of Technology, pp.:93-95, May 2004 (in Chinese).