The Idea of Effectively Building the Next Generation of Information Security Protection System

Ying WU
Shanghai University of Political Science and Law
Shanghai, China
wuying@shupl.edu.cn

***Abstract*—Under the condition of the global situation of network security is becoming increasingly serious, the Chinese enterprise security defense level there is still a large gap compared with abroad. We put too much focus on the external attacks and threats, but ignored the enterprise information security have a defense of their own. In this paper, starting from the current situation of enterprise information security defense, analyzes the network security and defense level gap, this paper puts forward the idea of the next generation of information security protection system.**

Keywords— information security protection; security defense; IT the immune system

I. INTRODUCTION

Matters for the enterprise to information security, it has been more and more cause the attention of the enterprise managers. On the other hand, with the development of the enterprise business computing environment and technology change, companies face the various aspects of security threats and attacks also becomes much more complicated and diverse, the focus of the security defense changed also. At the same time, with the tightness of the combination of enterprise security and business more and more high, to explore the future trend of the information security defense system has become one of the focus of nowadays enterprise managers the most attention.

Now the domestic circle of information security talk about a lot of offence and defense, but rarely talk about defense. We put too much focus on the external attacks and threats, but ignored the enterprise information security have a defense of their own.

Domestic enterprise information security development has experienced several important stages: from 2004 to 2009, based on is still in the construction conform to the requirements of the compliance, solve the problem of information security foundation stage; From 2009 to 2013, based on the basic compliance projects begin thinking how to make information security guarantee system more effectiveness; By the year 2014 to 2016, the effective information security protection system how to be born as key; While begin from 2016, entered the how in compliance construction on the basis of exploring effective to build the next generation information security guarantee system of the landing stage.

II. THE CURRENT SITUATION OF ENTERPRISE INFORMATION SECURITY DEFENSE

In the global situation of network security is becoming increasingly grim situation, China enterprise security defense level there is still a large gap compared with abroad. According to authoritative consultancy IDC survey last year, according to China's enterprise network security investment accounts for only 1% of enterprise information investment, and the figure is 8% in Japan, in the United States is as high as 10%. This figure has reflected the level of China's security industry at present.

Specific to the enterprise business, the domestic many enterprises serious lack of awareness of security defense also. Enterprise itself very lack of safety consciousness, in some domestic enterprises or even just begin to do the information transformation, far not reached the level to consider security issues. While most of the enterprises at the beginning of the informatization construction will not to give too much consideration to the safety problems. Therefore our country enterprise security defense capabilities as a whole are still very weak at present.

Whereas poses a serious threat to enterprise network security groups of hackers, it is with the current enterprise network security level is in stark contrast. Based on the powerful interests drive, hacking team in collaborative division of labor, to form the underground black industry chain has been very mature. So, instead of hacking team is very strong. From the point of the future trend, the enterprise security defense capabilities as well as IT construction speed is very low compared with hacking team, if we still can't change the status quo, keep such security gap, the future will lead to largest gap with the threat. So, now we face the overall network security situation is very dangerous.

III. THE NETWORK SECURITY AND DEFENSE LEVEL GAP ANALYSIS

Why can cause the current situation of network security so tough and defense level gap? We are analyzed from two aspects.

On the one hand, for the enterprise, once security incident occurs, the impact of the core value of the enterprise will be very great. Especially with a lot of information store customer data as the core of financial, medical and other industries, in the event of data breaches and attacks, consequence even unimaginable. And enterprises in this aspect's defense are often the t weakest link.

And remove the pure technical defense level factors, the data itself for businesses and for the gap between the value of the hacker can also cause a lot of the core data leakage. , for example, when the data is far greater than the value of the hackers, the value of the enterprise itself, many data will even be artificially leaking out. If the agency has no legal, public opinion and the control of the market of third party effective regulation to crack, so only by security technology to protect data is often not work. And this also is at present in domestic and abroad security defense of huge gap is one of the reasons.

On the other hand, from aimed at the core of enterprise operation, the degree of protection, IT is also no progress in China than the European and American countries. Along with the advancement of big data, information industry, the value of the enterprise more and more will be digitized. Only when the enterprise to realize that the data once the attack has been leaked, the enterprise's losses will be so much, then the enterprise will take these data.

Due to the above two aspects of the key factors, constitutes the current network threats in the Chinese market situation is more serious. At the same time we also see that in the current network attack, such as APT attacks on "tall" method is frequently used to come in, in the face of such attacks, the security defense against the attack of the enterprise real defense capability is very small. Hackers, in contrast, the first attacked union. If you want to fundamentally change the situation, you need to clear the whole security industry, what is the driving force, if not out of the strong demand for enterprise security, but out of liability for safety for the purpose, will never get security industry. Of course, as the Chinese market to the change of enterprise security concept and gradually pay attention to, this situation will also get the corresponding change.

IV. THE IDEA OF THE NEXT GENERATION OF INFORMATION SECURITY PROTECTION SYSTEM

"With changeless should change" security defense idea is: to build a system of stable defense, resist change of cyber threats. Build a system of stable defense, cannot only depend on the previous traditional defense system, traditional security 3 big: antivirus, IDS, IPS, this 3 big although against threats have certain effect, but based on the known characteristics of defense, that is to say, for known threats can be defensive, but for unknown threat only when the normal behavior, can't meet the demand of today's network security defense. Through a series of recent APT attacks can see, traditional security defense is not suitable for today's defense needs. So it is necessary to build a stable defense system, the following ideas from three aspects:

A. The safety risk assessment is the first step for the present enterprise information security defense

At present, both the government and enterprises, for their own information security are extremely concerned about. Therefore, the enterprise information security risk assessment once again aroused the concern of the industry.

For an enterprise to clear existing and potential risks in information system, fully assess the likely impact of threats and risks, will be the enterprise implementation of safety construction must first solve the problem, is also the foundation of security strategy and the basis.

Risk assessment of the significance lies in the understanding of risk, the risk process, can be considered in the management cost, choose suitable for their own control method, for the same kind of risk factors in the same baseline control, to help on the premise of guarantee the effect of reduce the cost of risk assessment. Here are six ways to safety risk assessment:

- Customize your assessment method

Although there have been many standard evaluation methods and processes, but in the process of practice, should not only the form and the copy of these methods, but take them as reference, according to the characteristics of the enterprise and the ability of safety risk assessment, to reorganize, "gene" custom evaluation method of individuation, make assessment services can be cut and flexibility. Assessment types generally have a overall evaluation, IT security assessment, network structure, penetration testing, boundary assessment, vulnerability scanning, policy evaluation and application of risk assessment, etc.

- The safety of the overall framework design

Risk assessment is the purpose of provide foundation and basis for risk management. As the direct output assessment, for the safety of the overall risk management framework, at least should be clear. But because of different enterprise environment difference, the difference of demand, and in practice can be the reference templates are very few, the overall framework application is less. But, the enterprise should complete the recent 1 ~ 2 years at least framework, so as to achieve a law.

- Multiple user decision evaluation

Different levels of users can see different problems, to get a comprehensive understanding of risk, multi-user communication evaluation must be conducted. Will review process as a multi-user "decision making" process, to know and understand the risk, management risk, to carry out the action, has great significance. In fact, many users to participate in the effect are very obvious. Multi-user "decision-making" assessment, also need a specific processes and methods.

- Sensitivity analysis

As a result of the enterprise system increasingly complex and interconnected, makes the risk is more and more visible. To improve the effect of evaluation, we must further correlation analysis, such as in an old hole, rather than simply analyze its influence and solutions, but rather to infer that may be related to other technologies and loopholes in management

rules, and find the "root", opened a "prescription" effectively. It needs strong evaluation experience knowledge base support, evaluators have keen analytical capability is also required.

- Centralized decision-making management

Safety risk assessment needs to have a variety of knowledge and ability of people to participate in, to the ability and knowledge management, help to improve the effect of the evaluation. Centralized decision-making management, is the guarantee of assessing project success one of the conditions, it is not only the project management problems, and is the combination of knowledge, ability and so on "genes". We must choose people with special skills, to perform the corresponding key tasks. Such as console audit and permeability tests, performed by no offensive and defensive experience and knowledge, will not any effect.

- Evaluate the results management

The output of the safety risk assessment and should not be the document stack, but can take a record and management system. It may not be a complete risk management system, but at least is a very important to manage the risk of expression system. Companies need such assessment management system, use it to guide the evaluation process, management assessment results, in order to improve the effect of evaluation on management level.

B. Adaptive security architecture to manage advanced directional attack

Protective function is difficult to deal with the current advanced directional attack, because the enterprise system of sustained attack, continues the lack of defense, and for special way of "emergency response" is no longer the correct mode of thinking, so the adaptive security architecture to manage advanced directional attack. The key ability of adaptive protection architecture:

- "defense" refers to a series of policy sets, products and services can be used for defensive attack. This part of the key goal is to be attacked by reducing the surface to attack the threshold, and intercept attack action before the affected.
- "detection" is used to find those who escaped the defense network attacks, the aspects of key goal is to reduce the threat caused by "lockout time", as well as other potential losses. Detection capability is critical, because enterprises should assume that he is in a state of being attacked.
- The ability to "go back" for efficient investigation and detection function (or external services) remedy is found to transaction, in order to provide intrusion certification and attack source analysis, and generate new prevention measures to avoid the accidents in the future.
- "the ability to predict" so that the safety system from the outside in the hacker action under the monitoring of learning, to take the initiative to lock in the existing information system and a new type of attack, threatening loopholes and delimit the priority and positioning. The information feedbacks to the prevention and detection function, so as to make up the whole process of the closed loop.

Through the above four key capabilities in compliance construction security capabilities on the basis of the superposition and continuous adaptive visualization strategy adjustment, with security policy visualization as the core groups all functions into a system. Continue building IT superposition of the immune system and information security.

C. Corporate IT superposition of the immune system and the ability of information security, gradually achieve comprehensive superposition real-time visualization

Traditional information security is the core of construction of compliance, but it still has shortcomings, such as policy standard lag, attention degree is not enough to the business perspective, etc., so you need to continuously improve the traditional base defense system, and the security policy integration with business as the core, using visualization technology promote control ability, strengthen the immunity ability of the business system.

Today, facing the new era of information security threats, traditional defense system has been unable to cope with new threats and attacks, so need to integrate various against the threat of new technology to improve the defense adaptive ability. Thus, the next generation of information security guarantee system emphasis on, from a business perspective to achieve safety to ensure business continuity and security. And want to build a system on the basis of the traditional compliance, perspective transformation, defense technology stack, achieve sustained visual monitoring system status, and adaptive adjustment in order to enhance the business system's own immune ability.

From the concrete technical level, the safety of the combined with business strategy visual security policy can be stacked linkage adjusting all kinds of ability, for example: by monitoring the users abnormal behavior strategy adjustment protection APT attacks; By monitoring application layer data protection user WEB attacks, by monitoring the business strategy adjustment layer data to optimize business performance, integration of the business layer, the WEB layer, network layer, data layer, the key data and user behavior and external threat intelligence for rapid analysis and visual display and make accurate early warning, in solving the compliance construction against new attack threat at the same time, the imperfect parts of the business and security of uniting, finally realizes the core business security situational awareness.

The construction of the enterprise IT's immune system, its core is the safest strategy. If enterprises can truly achieve the above security strategy, enterprise information security defense system will be very strong.

REFERENCES

[1] Da-peng Yang. Enterprise security defense system of information security technology design Beijing: computer CD software and applications, 2010 (9) : 6-6

[2] Yao Wang. Building enterprise network security system Beijing: Beijing university of technology, 2010

[3] Hao Zhong. Just talk about the construction of enterprise computer network security and protection system Beijing: computer CD software and applications, 2012 (21) : 93-93

[4] Lin Li. Introduction to information security protection system Beijing: information security and technology, 2012.6

[5] Yun-chang Sang. Big data security present situation and countermeasure research. Chongqing: computer science. 2015. S2

[6] Zhi-ying Wang. Small and medium-sized enterprise cloud computing data security risks associated effect research. Sichuan: computer application research. 2015.06

[7] Mao-yue Zhang. Big data era new threats of personal information data security and protection. Beijing: China science and technology BBS. 2015.07