Research On Government Websites Information Security Regulatory Mechanism And Countermeasure

Yu Yao[1,a], Runze Gao[1,b]

1.Key Laboratory of Operation Safety Technology on Transport Vehicles Ministry of Transport, PRC
Research Institute of Highway Ministry of Transport
Beijing, China
[a]y.yao@rioh.cn
[b]rz.gao@rioh.cn

Keywords: government websites; information security; management system; suggestions

Abstract

There are many hazards such as Trojans, back doors and other attack means all the time threatening the development of government websites. This paper firstly collects the latest data to introduce the grim situation of information security faced by the government websites in our country. Secondly, this paper analyzes the existing problems of information security management for government websites. Thirdly, this paper focuses on the research of information security regulation and puts forward the strategies, which could provide new ideas for the development of the government websites in our country.

1 Introduction

In recent years, with the rapid and continuous development of the Internet, the number of China's internet, broadband fiber users has ranked first in the world. However, the construction of network security infrastructure, the security awareness of citizens, the corresponding laws and regulations and institutional environment have not kept pace with the pace of development of the network.

To solve the zombie websites, sleep websites and other issues, from March to December 2015, the General Office of the State Council had carried out the first census of the national government websites. The purposes of the census were to find out the basic situation of the national government website, and to solve "not timely, inaccurate, non-response, not practical" and other issues. However, the information security problem faced by the government website was not one of the important indicators to evaluate the government website.

2 The grim situation of government websites information security

In December 2015, The China Software Testing Center evaluated nearly a thousand government websites, from the ministries and commissions to the districts and counties, and the assessment data showed that more than 90% of the websites had a variety of risk levels security vulnerabilities, 31% of the websites were classified as extremely dangerous, 17% of the websites were classified as highly dangerous, and nearly 30% of the websites were monitored for more than 30 vulnerabilities, and even more than 60 websites exceeded the number of security vulnerabilities of the 100.

In January 2016, The China Information Security Testing Center released the "2015 Information Security vulnerability situation report". As shown in Figure 1, since 2010, the number of new vulnerabilities has shown an overall increase trend, there is an annual increase of 6781 vulnerabilities, and since 2012, the number of new vulnerabilities are maintained at more than 7,000 per year, there are 3 annual rate of increase of 20%.

The report shows that 7,754 new vulnerabilities monitored in 2015, from the type of these vulnerabilities, the buffer overflow category accounted for the largest percentage, to 14.03%, compared to the number of 787 in 2014, an increase of 38.25%. From the hazard level of these vulnerabilities, the total proportion of critical and high-risk vulnerabilities was 30.8%, the number increased by 300 over 2014, an increase of 9.62%. These figures show that the current information security situation of government websites in our country is still very serious, and the security threats cannot be ignored.

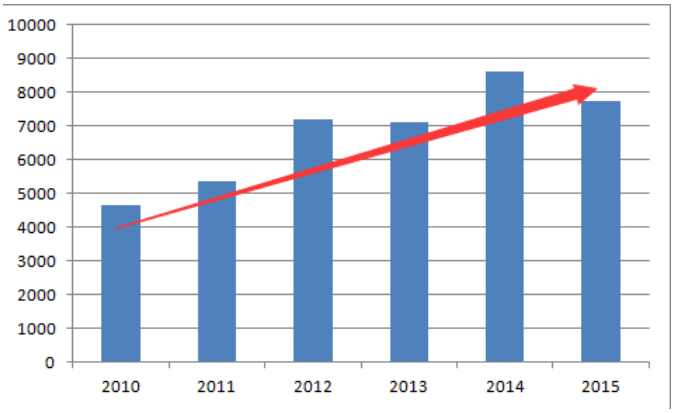

Figure 1: The number of new vulnerabilities from 2010 to 2015.

3 The problems of government websites information security management

There are several major reasons leading to the grim situation of government websites information security. This section will analyze and explain these issues one by one.

3.1 Heavy application and light security

At present, the construction of government websites is a common phenomenon of "heavy application and light security". There are two main reasons for this phenomenon. First of all, the construction units of government websites usually pay more attention to the functional requirements and performance requirements, but overlooked security issues. In the tender documents, rarely see the security requirements. Another important reason for the phenomenon is that the information security problem faced by the government website was not one of the important indicators to evaluate the government website. For example, majority of the websites performance evaluation indicators proposed by the China Software Testing Center are formulated from the point of view of the information disclosure and business applications, while the weight of websites security only 2%. The lack of security baseline and security planning seems to be the root cause of the problem.

3.2 Lack of professionals in information security

In reality, managers of the government websites are mainly software development personnel or operation and maintenance personnel, while network information security is a highly specialized subject, the existing managers cannot adapt to the current situation of network security needs. At present, our country is very lack of excellent information security theory and technical personnel, although some colleges and universities have set up courses on information security. However, on the one hand, due to starting late, long training cycle, there are few students have graduated; on the other hand, relative to practice, the schools pay more attention to theoretical education, graduates cannot adapt to the actual work requirements.

Based on the description of the page loading process, it can be found that, for the high concurrent website, the page quality seriously affect the running speed of the website. If the page is too large, it will consume huge network bandwidth when the page loads, so the page design should be as simple as possible, in order to reduce unnecessary network traffic, to ease the bandwidth pressure brought about by the high concurrency. Therefore, the optimization of the front-end of the Web can be constructed from the following aspects.

3.3 Key technology dependent on foreign seriously

Our country's core technologies and industry support capabilities have made great progress, but compared with the Western developed countries, there is still a big gap, and information security task is especially arduous. Many of important information systems are based on the United States Intel's computers and Microsoft's operating system, running on Cisco's network. The US server provider IBM, the database provider Oracle, and the storage equipment provider EMC, formed the IOE's troika. Such a single channel poses a potentially great threat to our information security. Take the operating system as an example, because Microsoft is in a monopoly position, it can force users to upgrade, after upgrading to Windows8, you cannot uninstall, which is credible for Microsoft, but for us it is not. Although the use of these devices generally does not cause problems, at a critical moment, we cannot rule out the possibility that the opponent country maybe through remote wireless control system to start information theft, data deletion and system attacks, which could paralyze our important information systems.

3.4 Lack of institutionalized security management

Many government website units did not establish the corresponding security management mechanism, in the whole process of operation, there is a lack of effective security inspection and response protection system. At the same time, imperfect management mechanisms make network administrators or insiders do the crime thing easily and anonymously. According to the survey, many cybercrime behaviours come from internal networked computer and due to the lack of high quality security management.

4 Suggestions on strengthening government websites information security management

This section will focuses on the research of information security regulation and puts forward the suggestions on improving the information security management, hoping to provide new ideas for the development of the government websites in our country.

4.1 To set up information security management department

The first thing the government websites units should do is to establish information security management department, and hire information security professionals to engage in information security management. The main responsibilities of the department include the design and implementation of new website or new system in the information security level, upgrading and transformation of in-use information system in order to meet the security requirements, periodic vulnerability scanning and rectification.

4.2 Use of own-brand operating system

After several years of development, our country's own-brand operating systems have got a certain foundation, construction of government websites should be encouraged to use own-

brand operating systems. At present, China's own brand operating systems are mainly Linux-based secondary development systems, and the representative products include GDLC, Deepin, isoft, WiOS, StartOS and so on. China should provide more support for own-brand operating system in the government procurement links. Especially for some industries, there is a worry about taking responsibilities in the event of occurrence problem when using a domestic operating system. In this regard, the departments concerned should take the exemption from liability measures.

4.3 To establish a completed information security management system

As shown in picture 2, a completed information security management system should consists of four parts, which include the overall approach, security management organization system, unified security policy, and security operational norms. The purpose of establishing the system is to integrate the websites security design, websites security infrastructure, websites security operation and maintenance services.

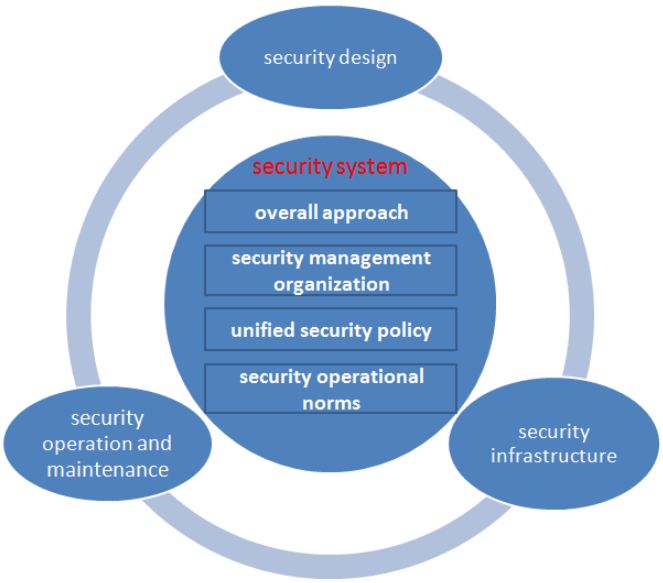

Figure 2: The information security management system architecture.

The formulation of the overall approach should be referred to the domestic and international information system security management standards, the national information system security protection regulations, and information system security level protection basic requirements. The security management organization system aim to improve the information system security management responsibility, clearly define the internal security management organization, and promote the work of information security management in the entire organizational system. The unified security policy elaborates the action strategies based on identity, rules and roles, from the aspects of engine room security, network security, system security, application security, data security, emergency management, security audit, security testing. The content of security operational norms should include the websites security management method, the computer network security management regulations, the internet information release confidentiality system, the engine room security management system and so on.

5 Conclusion

In summary, to strengthen the government websites information security is an urgent and arduous task. It is imperative to establish and improve the organization system, work operation mechanism, management system, emergency response mechanism, technical protection system, supervision mechanism, and training mechanism of the security management organization. At the same time, we must also handle the relationship between information security and the development of government websites dialectically: security is a prerequisite and development is the ultimate goal. We have to make sure the rapid development of government websites in a security condition.

Acknowledgements

This work was supported by Soft Science Research Project, Ministry of Transport, "Research on China's Automobile Network Security Supervision Mechanism"(2015-362-A25-370).

This work was supported by Independent Research Project, Research Institute of Highway Ministry of Transport, "Research on Construction of Vehicle Information Service Platform and the Development of Fuel Consumption Review Module"(2014-A301).

References

[1] Hou Yajie. Based on the government website required by e-government information security research [J]. Popular Science and Technology, 2015,06: 201-202.
[2] Liu Zihan, Zhao Qianqian, Lv Pengju, Hou Linlin. Research on Safety and Protection of Government websites [J]. Popular Science and Technology, 2015,23: 56-58.
[3] Gu Yan. The Influence of Information Security on China's National Security and the Government's Policy Response in Internet age [D]. U niversity of Intwrnatiovial Business and Economics, 2015.
[4] Wang Xi. Analysis for Security Management of Government Website——Take the Website of National Administration of Surveying, Mapping and Geoinformation for an Example [J]. Computer Security, 2014,07: 58-61.
[5] Du Yulin. Fushun city Fushun urban construction bureau e-government netword security sysytem construction [D]. University of Electronic Science and Technology of China, 2014.

[6] Lv Jian. Discussion on Government Network Security Management [J]. Computer Knowledge and Technology, 2015,31: 20-23.
[7] Zhang Yimin. The Implementation of Network Security Management Based on Architecture [D]. Jilin University, 2015.
[8] Casado M. Architectural support for security management inenterprise networks [D], Stanford University, 2007.
[9] Jiang Zelan. Research on Network Security System of a Department Level Governmental Sector [D], Guizhou University, 2009.
[10] Wang Yifei. An Exploration and Analysis on Chinese Cyber Security Strategy [D], Jinlin University, 2015.