CSCanada
Canadian Social Science
Vol. 9, No. 2, 2013, pp. 28-33
DOI:10.3968/j.css.1923669720130902.9322

ISSN 1712-8056[Print]
ISSN 1923-6697[Online]
www.cscanada.net
www.cscanada.org

Shallow Talk about Information Security in the Corporate Office

WU Xia[a],*

[a] Heavy Oil Company Liaohe Oilfield Branch Company Petrochina, China.
*Corresponding Author.

Received 10 February 2013; accepted 15 April 2013

Abstract

Information security refers to the information network hardware, software and its system of data protection, not subject to destroyed, changed or leaked by accidental or malicious reasons. System can be running continuously、reliably and normally. Information services can't be interrupted. The confidentiality, authenticity, integrity, unauthorized copying and its parasitic system security of the information is ensured. Information security in the Corporate Office is the key of enterprise modern office. Once be neglected, it is easy to bring a series of negative impacts. In this paper, the information security in enterprises office is to be discussed briefly.

Key words: Information; Security; Threats; Strategy

WU Xia (2013). Shallow talk about information security in the Corporate Office. Canadian Social Science, 9(2), 28-33.Available from: http://www.cscanada.net/index.php/css/article/view/j.css.1923669720130902.9322
DOI: http://dx.doi.org/10.3968/j.css.1923669720130902.9322

INTRODUCTION

For too long,information security has been considere daseparate discipline, is olated from the enterprise architecture. With the continuous development of computer science and network technology, information security has been a quite important problem. Network information security is a dynamic, the overall project. How to ensure network and information security has become a concern of the whole society. Information security problems are directly related to the informatization construction of Enterprises. The enhanced functions of the information utilities, the sustained accumulation of information resources lead the information security to be part of the safeguard of the corporations. Information security risk assessment is the foundation and the precondition of information security of organization, and is one of the front subjects in information security field.

Information as a kind of enterprise resources, its universality, sharing, Increment, handlability and Multiple utility, make it has special and important significance for enterprise production. For Liaohe oilfield Branch Company, up to now, with the rapid increase of the amounts of information in various aspects, it requires large capacity, high efficiency to transmit the information. In order to adapt to this situation, the development of information technology application makes a lot.

Information security in the Corporate Office is the key of enterprise modern office. Once be neglected it is easy to bring a series of negative impacts. In this article, we have summarized the concept and styles of cyber information security and the technique about firewall, data encryption and so on. The dissertation bases on what the author actually works for, the information security technologies and situation researched in current network, and the main content proposed. This paper takes an application example, to provide organization the best practice of information security risk evaluation.

1. THE THREATS OF INFORMATION SECURITY IN THE CORPORATE OFFICE

Corporate office information system is based on corporate firewalls, server, access the web, E-mail, company internal network, office PC hardware, database, Internet technology and the corresponding auxiliary equipment. It is a comprehensive management system. From the point of security situation, there is serious security threat in the enterprise office information system. Equipment provides

the convenient information and resource sharing, but at the same time in security is fragile and complicated, pose a threat to data security and confidentiality. Potential security threats mainly have the following several aspects:

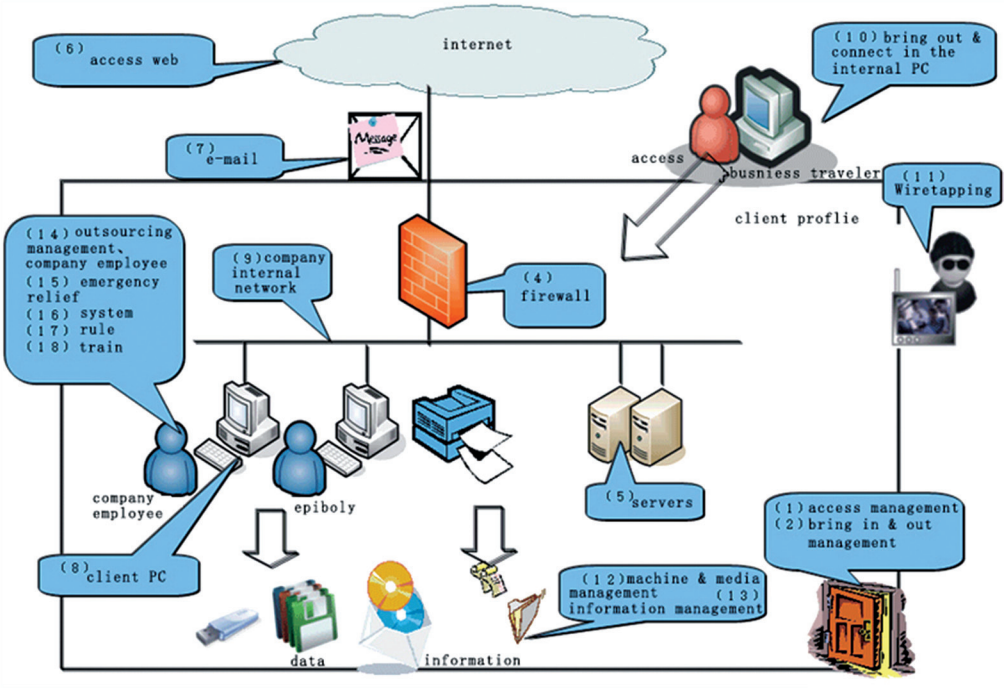

Chart 1
Information System in the Corporate Office

(1) Information disclosure: the information is disclosed or disclosed to unauthorized entities.

(2) Destroy the integrity of information: data is not authorized to add or delete from loss, modification or destruction.

(3) Denial of service: the resources of information or other lawful access was blocked unconditionally.

(4) Unauthorized access: some resource be used by any unauthorized person or ways.

(5) Hacking: stealing the information in the system resources and sensitive information by any possible legal or illegal ways. For example monitoring signal wire in the Line transmission, or capturing useful information by electromagnetic leakage created in the work process of communication equipment etc.

(6) Business flow analysis: through the long-term monitoring of the system, studied on some parameters by using statistical analysis method, discover some valuable information and rules from it.

(7) Counterfeit: through deception communication system (or user) to illegal users to pretend to be legitimate users, or small user privileges as become a privileged user. Hackers are mostly adopts the counterfeit attack.

(8) The bypass control: the attacker gain unauthorized rights or privileges by using system security flaw or the vulnerable parts of the security.

(9) Authorization assault: authorized to use a system to an end or resources of someone, but the permissions for other unauthorized purposes, also known as "internal attack".

(10) Trojan Horse: software is contained in a segment that is perceptible harmful. When it is executed, it damages the user's security.

(11) The trap door: the "authority" set in a system or a component, allowed to violate the security policy in particular the data input.

(12) Denial: this is a kind of attack from the user, such as: denied that he had published a message, forge a letter each other, etc.

(13) Replay: for illegal purposes, Copy certain legal communication data intercepted and send it again.

(14) Computer virus: a kind of program which can make the infectious and damage function during the computer system running process.

(15) People accidentally: an authorized person leak the information to an unauthorized person for certain benefits, or because of carelessness.

(16) Media waste: information is captured from discarded disk or storage medium already have printed in.

(17) Physical invasion: the intruder bypasses the physical control and gains access to the system.

(18) Steal: important safety items such as token or identity card are stolen.

(19) Business fraud: a dummy system or system component deceive legitimate user or system voluntarily give up sensitive information etc.

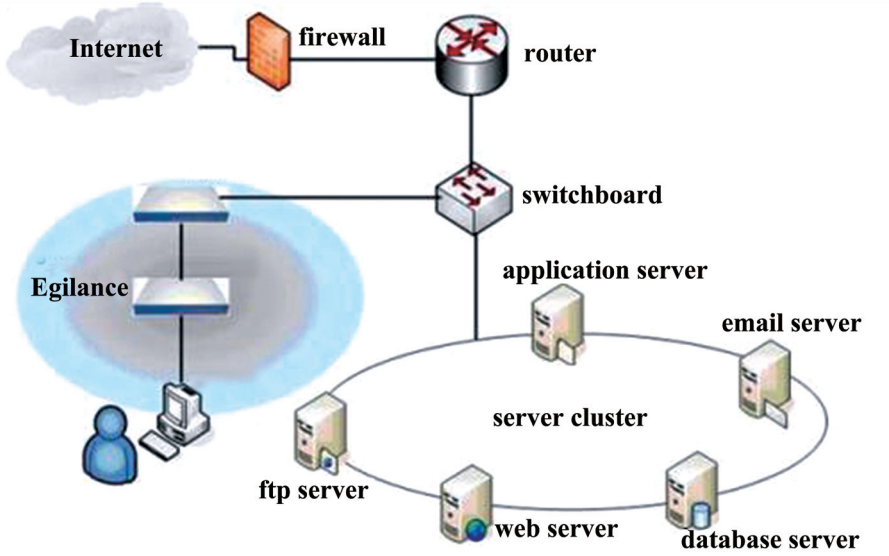

Chart 2
System Structures in the Corporate Office

2. THE INFORMATION SECURITY STRATEGY OF CORPORATE OFFICE

Information security policy refers to some rules to obey in order to provide certain level of security protection. Implementation of information security in the enterprise office mainly includes the protection of network security, application security and protection system to protect the security of the three aspects. Each aspect should consider physical security, firewall, information security, Web security and other media.

2.1 Network Security Protection

Network security is the security for the communication process between protections of internal parties' network end system. To ensure confidentiality, integrity, authentication and access control is an important factor in network security. It becomes an important research project that how to use the service of the network and reduce the loss in the network information security. The main measures to protect the network security are as following:

① Comprehensive planning security strategy of network platform. Information security framework system is the basic approach of information security management.

② Making network security management measures. Nowadays, network intrusion and attack affairs happen frequently, which makes people pay more attention on the spot of network security management technology. And with the increase of the network security products, the topological and structure of network became more complex, network security management becomes necessary. These problems make the unified network security management technology as absolution for the overall security management of the network become one of the most enhanced security technology. Intensifying network security management and working out efficient solution to emergency will ensure whole network working safely. With networks apply in more and more fields; the uniform network security management system is needed. To manage and control numerous, various, complicated, and dynamic security hardware, security applications and security events in the large-scope network is named network security management. With the development of the network security management technology, the configuration and management of the network security equipments become more and more complex. Using password, data encrypt, fire wall, digital signature, network security management technology, etc are mainly focused on. Research on network service system log analysis technology to enhance network security management capabilities has great academic value and practical significance. Network flow monitor is the major task of network security management, and is an important side of scaling network performance entirely.Through centralized network security management, the deploying ability of network security strategy and replying level of network security risks are improved. Network security management system is a system that effectively manages and monitors the host and network equipments within a local domain. Based on comprehensive information security policy of security system, this paper studies the security of local Area Network by network security technology and network security management. In management, it emphasizes on the network security management and emergency response system should be established to guarantee the standardization and institutionalization of network management.

③ Using firewalls. A firewall is a system or group of systems that enforces an access control policy between two networks. A pretty decent firewall can offer a good level of protection for everyone in the enterprise. Firewall gets this information from the connection tracking state of

the packets. A user account policy is needed to spell out the general responsibilities of each firewall administrator. If one of these components fails to start because the connection is refused, the problem might be caused by firewall software running on the server's host. Inside the firewall, there is no anonymity. When communicating with an external, public network like this there may be restrictions on your firewall that limit the communication. The server should be behind a firewall or a router capable of blocking ports. This provides protection from threats external to the enterprise, and limits access in case of an intrusion through the outer firewall (FW1). A home user might want to configure a firewall to lower security level by allowing all outgoing packets to pass through.

④ Recording all the activities on the internet as far as possible. A fundamental tenet of information security is controlling access to the critical resources that require protection from unauthorized modifications or disclosure.

⑤ Noting on the physical protection of network devices. In the majority of modern enterprises, IT assets (both hardware and software), including network devices, servers, system software, and applications, are critical to keeping the business running.

⑥ testing Vulnerability of network platform system. A test platform can be built to test the prototype system in terms of remote control, network security and network parameter configuration.

⑦ Establishing reliable identification and authentication mechanism. In the area of network information security, key agreement is essential between servers and clients.

Intrusion detection is a new technology which developed with the network technology and information security technology. As an effective method to realize copyright protection and safe authentication, the watermarking has become more and more popular in the multimedia information security research area. Information security risk assessment is an important tache for evaluation of information system security.

2.2 Application Security Protection

Protect the security of the application, mainly is for safety protective measures established by a specific application server (such as Web servers, database servers, FTP servers, etc.). It is independent of the network of any other security measures. Although some protective measures may be an alternative or overlap of a network security services, such as the encryption the Web browser and the Web server make to the payment settlement information packets on the network in the application layer, are all through the IP encryption, many applications have their specific security requirements. Cryptology is the kernel technology in the field of information security, it has extensive commercial prospect in many fields. Database security theories and technology not only is an important research field of database theory, but also is an important research field of information security.

The requirements for safety of application layer are very stringent and complex; therefore tend to be more in the application layer instead of various security measures in the network layer.

While the network layer security still has its specific position, People can't totally rely on it to solve the security of corporate information system. Application layer security business can include authentication, access control, confidentiality, data integrity, non-repudiation, Web security, security such as EDI and Internet payment applications.

Now information hiding technology has already had widespread application in multimedia information copyright protection and information security etc. The application of some other security techniques about the technical protection is researched, including Virus Prevention, Firewall, and Virtual Private Network etc. Common web attacks protection - detecting common web application security attacks. The application maintains safety and security with multiple layers of password protection. The invasion detection system is one kind of initiative protection network resources network security system, in recent years, we obtained extensive research and the application. With the application and spread of the classification protection, Network Security Vulnerability Scanning should consider the efficiency and the function expansion. Through the security testing, the security protection system would satisfy requirement of system, and the whole Web application would be protected effectively.

2.3 System Security Protection

System security protection is to point to Safety protection from the angle of the whole information system. It related with the network hardware platform, operating system, application software and so on. The safety strategy contains the following steps:

2.3.1 In the Software Installed, Check and Confirm the Unknown Security Vulnerabilities.

Network security assessment is a complex system engineering. Most of current security evaluation tools are only used to scan and detect the security vulnerabilities of network system. Old systems that haven't been upgraded are likely to have security vulnerabilities that attackers can exploit. Hackers look for computers with security vulnerabilities and infect them in advance of an attack. The administrator discovers, examines, reports and proposes fixes for system security vulnerabilities and misconfigurations. Propose a security vulnerabilities detection model which use static analysis and dynamic verification strategy. The method should be well integrated with conformance testing to cover some known protocol security vulnerabilities, and has the ability to reveal potential problems. Summarize common classes of security vulnerabilities and their taxonomy at the code level. Secure programs must minimize privileges so that any bugs are less likely to be become security

vulnerabilities.

2.3.2 Combined with Technology and Management, Make the System a Minimum Transmission Risk.

(1) Allow communication through many authentication

In view of some reasons, the authors first address one major security problem of multicast communication: source authentication. One of the main challenges of securing multicast communication is source authentication. It is therefore critical to provide sound security mechanisms for multicast communication. Client needs shared session key between itself and the authentication services for the future communication with authentication services. An authenticated key agreement protocol is used to provide authentication in communication systems, and produces a short-time key that can encrypt the transferred information. It is designed to provide strong authentication and encrypted communication for client-server applications by using secret-key cryptography. Assign a unique User ID and Password between WebSphere Business Integration Connect companies to increase the security and authentication level of communication. In addition, the two sides also reached an agreement on protection of varieties of plants, co-operation, authentication service, communication and plan.

As the foundation of Grid communicating security, research on the authentication and key agreement mechanism is one of the hot topics. With the development of Internet and communication technology, image authentication has been under active study in recent years. It has features as follows: identity authentication, changeable communication key, secure against active and passive attack. The principal parts of the scheme include application server access authentication, database server access authentication, secure communication, and administrator attack prevention. The type of channel that you select influences the authentication, authorization, secure communication, and performance characteristics of your solution. The model not only realizes key management, encrypted communication, digital signature and identity authentication, but also is fit for network system with real time and large data transfer. Authentication, authorization, and secure communication features provided by IIS and ASP.NET are immediately available. ASP.NET and IIS authentication, authorization, and secure communication features are available to remote objects that are hosted in ASP.NET. The C/S communication security is supported by the certificate authentication mechanism. The automatic recognition and parameter estimation techniques of communication signals can be utilized in the authentication and spectrum management for radio signals.

(2) For all access to the data must be audited to strict safety management system users

Computerized accounting and E-business data are widely used by many companies. The production data are audited in compliance with the procedure set forth within the testing facility. Aiming at the storage modes of production data of the audited units, several different network-based audit methods are brought forward. Administrator's requests are also accurately audited at the remote data source under his own identity. The prototype of LSSAS in network based on B/S& C/S mixing mode can be designed and implemented, and the log data collected by prototype system in the applied environment can be analyzed and audited.

(3) Do strict safety management to system users

① Cancel the set of users access to the network

Many times, the network administrator for convenient management, tend to focus on a group of user authorization, it improves the efficiency of network management, but also to the network security poses a potential threat, because some Trojans will secretly will create their own user account, to access higher group of users, then the Trojan program can easily obtain illegal attack power. In view of this, we need an important host in the system or server system, cancel the set of users access to the network.

② Set the appropriate permissions for the new user

If some trusted new users need to access the local server system through the network, so we need to create a new user alone in a server system, and for the new user set the appropriate access rights.

③ Make a particular user has permissions

In order to facilitate the management of the network, we often need through the network, remote control of important host system in LAN; however, open the remote control function, easy to the server or host system poses a security threat. In view of this, we should follow the following steps, remote control permissions to specific users trust worthy.

④ Force a network user authentication

Many times, the network administrator in the remote management operation, convenience, without setting up a remote login password, later in their remote control operation, it does not require network authentication, can directly login into the LAN server system, it was evident that the server system is very dangerous. In order to ensure the safety of remote control, we need to think of a way to force the network user authentication.

⑤ Monitoring user account login status

In order to prevent illegal user login server system secretly, some operating system adds a new monitoring user account login, the clever use of this function; we can find the potential security risks, to ensure stable operation of the server system can always.

(4) Establish detailed security audit log to detect and track intrusion attack.

Information system log is an important source of information for real-time monitoring system and the analysis of network events. Information system audit

body, should strengthen the application and innovation of audit evidence acquisition method based on log analysis, and effective implementation of security audit of information system by the log audit as the dominant. Functional requirements of security audit system based on log perspective, can use the information system security audit model, and using COBIT theory, in order to log oriented information system security audit risk control idea: rational planning of recognition and log mining, strengthen the whole process of audit information system security; the effective implementation of mining and evaluation of log, science confirm the material misstatement risks related to the security of information system; strengthen the audit of network platform.

2.4 The Strict Safety Management

The managers of the enterprise should establish the corresponding network security management measures, strengthen internal management, and improve the overall awareness of network security.

2.5 To Strengthen The Staff's Information Security Training

In the corporate office, if employees often have some Computer operations not related with work, it would affect both the network speed and system security. therefore, Throughout management in the corporate office information system, the human factor is the most important. So we must strengthen the safety training of computer users.

CONCLUSIONS

Information security is a new mode in the corporate office, we should make full use of network platform, at the same time, we also want to do a good job of protection, to avoid appear all sorts of internal computer information security problems.

REFERENCES

A Road Map for Digital Forensic Research. (2001). *Digital Forensic Research Workshop*.

Vicka Coreyet (November & December 2002). Network Forensics Analysis. *IEEE Internet Computing*.

ISO/IEC 17799 (2005). *Information technology-Code of practice for information security management*.

ISO/IEC 17799. (2005). *Information technology - Security techniques - Code of practice for information security management* (2nd ed.).

ISO/IEC 17799. (2002). *Information technology-Code of practice for information security management*.

ISO/IEC TR 13335-2. (1997). *Guidelines for the management of IT Security Part 2:Managing and Planning IT Security*.

ISO/IEC TR 13335-4. (1999). *Guidelines for the management of IT Security Part 4:Selection of Safeguards*.

ISO/IEC 15408. (1998). *Information technology-Security techniques-Evaluation Criteria for IT Security-Part 1: Introduction and general model*.

ISO/IEC TR 18044. (2004). Information technology-Security techniques-Information security incident management.

NIST SP800-18 (1998). Guide for Developing Security Plans for Information Technology Systems.

NIST SP800-30. (July, 2002). Risk Management Guide for Information Technology Systems.