Discussion on Information Security of Enterprise Network

Xiaorui Liang

Aobaota Operation Area, No.7 Oil Production Plant, Daqing Oilfield Co., Ltd., China.

Abstract. With the rapid development of computer information technology, the number of computers and application systems in enterprise networks gradually increases, and the security threats enterprise networks face become more and more prominent. This paper explains the hidden dangers and problems the information of oil production plants face, and establishes a good information security system through secret-related document protection, network boundary access control, deployment of anti-virus software, and patch distribution, and creates a good and secure enterprise information operation environment.

Keywords: enterprise network, information, information security.

1. Introduction

With the networking and globalization of computers, information has become one of the important resources for enterprise competition; however, commercial hackers, viruses, malicious attacks, etc. will cause great harm and loss to enterprises. The enterprises face huge losses caused by virus raging, hacker intrusion, leaking and stealing, only continue to implement overall solutions of information security, and then can ensure the security of using the network to obtain and deliver information.

2. Hidden Dangers and Problems Information of Oil Production Plants Face

In recent years, oil production plants have continued to carry out information construction, network coverage area has expanded year by year, and application systems are more and more, so far, there are more than 50 self-built systems and more than 2,000 network clients have been built, and the hidden dangers and problems information faces is getting more and more.

2.1 Weak Password Phenomenon are Still Repeated

Weak passwords generally refer to passwords that are easily guessed by someone else or cracked by cracking tool. These include passwords that only contain simple numbers and letters, such as "123", "abc", birthday, hand-free telephone, and mobile number and so on.

Because such passwords are easily cracked by others, resulting in information leakage, remote control, etc., so that the user's computers face risk.

2.2 High-risk Vulnerability Fix Abilities are Generally Lacking

High-risk vulnerability is a kind of vulnerability with the highest level of risk, which is easily exploited by hackers, and causes the computer to be remotely controlled. Because the oilfield company does not have unified vulnerability fix software, all units generally lack high-risk vulnerability emergency response mechanisms and vulnerability fix abilities.

At the same time, the group information security operation center has paid more and more attention to system vulnerabilities recently, and regularly tested the intranet of China National Petroleum Corporation through vulnerability scanning software and manual checking and so on. For example, the oil production plant receives information security vulnerability rectification notice some time ago, its vulnerabilities include Bar Mitzvah vulnerability, IIS remote code execution vulnerability, IIS write permission vulnerability, and the above vulnerabilities cannot be found even if 360 security guard vulnerability scans are used.

2.3 Privately Build Internet Export are Serious

The group company's information management measures and previous network security conferences banned the construction of Internet export, virtual private network (VPN), wireless networks and satellite communication systems on the intranet, private exports have expanded the intranet's attack on the Internet, provide an attack channel and reduce the overall security level of the enterprise network.

Even if the same computer is installed with two network cards for switching or using a secondary agent to link to the Internet, it will leave a record in the computer and is discovered by the information security department of the oilfield company.

2.4 Network Security Operation and Maintenance Ability is Weak

All units generally lack network security full-time personnel; the equipment operation and maintenance personnel' network security ability is insufficient, does not fully and clearly grasp assets, and lack basic network security inspection tools. Some units even have zombie servers, and no one maintains for a long time, which causes major security hidden trouble.

2.5 IP Address Management is Confused

In the divided IP segment, the IP address has a one-to-one corresponding relation with the computer. However, some units do not clearly assign IP addresses, and there is a lack of corresponding relation between IP addresses and computers, there are phenomena where IP address arbitrarily change and occupy the Internet authority IP, causes computer users to have IP conflict or cannot access the enterprise network.

2.6 Self-built System Lacks Security Protection

Self-built information systems generally lack protection means in application layer, hackers can easily use the database command (SQL) inject form, cross-site scripting attacks and other application layer vulnerabilities to obtain server control.

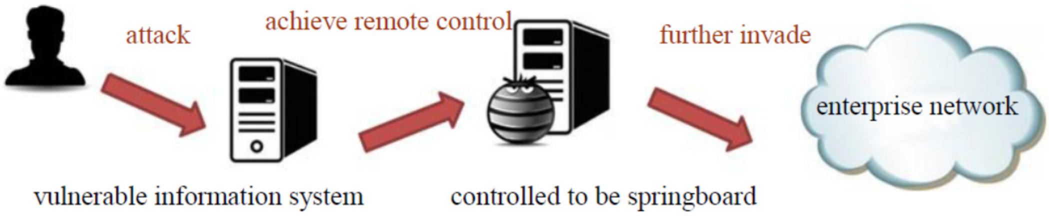

Fig 1. Self-built information systems

2.7 The Confidential Consciousness is Not Strong

The confidential consciousness of confidential documents and computers is not strong; inadvertently use the network to send confidential documents, it is easy to cause leakage risk, for example, use email or FTP to send confidential documents and so on.

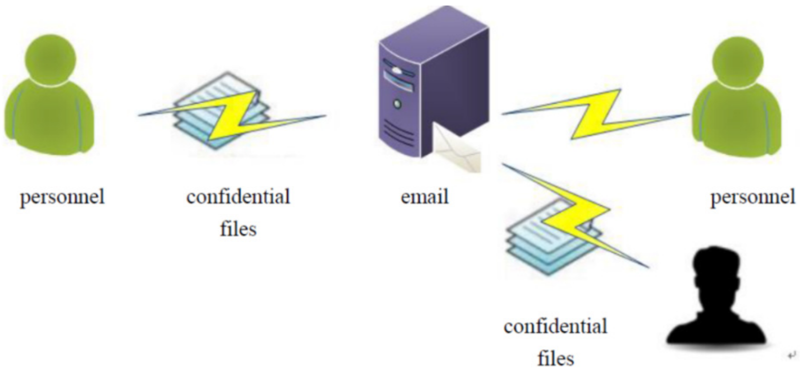

Fig 2. Use email or FTP to send confidential documents

3. Information Security Solution of Enterprise Network

In allusion to the hidden dangers and problems the above-mentioned oil plant information face, a relatively secure enterprise network information security network is established through three parts, namely network firewall, core switch and client terminal.

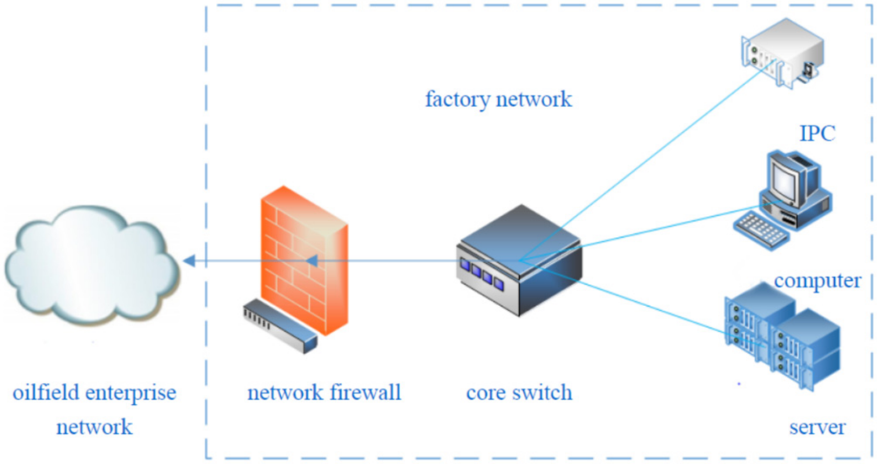

Fig 3. A relatively secure enterprise network information security network

3.1 Deploy Network Firewall

The hardware firewall is used to guarantee security of local area network. The firewall is similar to partition wall that prevents fire from spreading in a building, which monitors access channels between trusted network (equivalent to local area network) and untrusted network (equivalent to an wide area network), and it prevents the danger of wide area networks from spreading to the local area network, it acts on the entrance of the protected area, not only provides protection against network layer attacks, provides security protection based on access control policy, but also provides various intelligent analysis and management tools, and it fully protect the local area network. The hardware firewall can also provide various network management monitoring methods to help network administrators complete network security management.

The main security features of the hardware firewall are as follows:

1) ASPF (Application Specific Packet Filter) is packet filtering for the application layer, namely message filtering based on status. ASPF can detect protocol session information in application layer that attempts to pass through the firewall, and prevent data packets that do not conform to the rule from passing through.

2) The attack defense function of the firewall can detect various types of network attacks and take corresponding measures to protect the local area network from malicious attacks, and ensure the normal operation of the local area network and system.

3) The firewall provides real-time network traffic analysis function, which not only monitors data traffic, but also can detects connection initiation condition between internal and wide area networks, find abnormal traffic generated by attacks and network worms in time, notify the network administrator to handle them. And the abnormal traffic is blocked in time by the address dynamic isolation technology (address blacklist), thereby avoiding congestion of the network bandwidth by the junk traffic.

4) The firewall protects the address security of the local area network in various ways, prevent attacks from the local area network and protect the local area network security. Including MAC and IP address binding, ARP cheat check, and ARP reverse query.

5) The firewall provides the access control function for the application protocol, analyzes the application layer protocol, and provides HTTP Internet address filtering and web content filtering through the HTTP protocol filtering provided by the firewall, which can effectively manage the behavior of employees on the Internet, improve the working efficiency, save export bandwidth,

ensure normal data traffic, and shield various "junk" information, thus ensuring the "green environment" of the local area network.

6) Through filtering and controlling of SMTP mail, firewall ensures no leakage of information in the enterprise. Moreover, it is possible to prevent the spread of emails carrying illegal content and virus programs by controlling the content of the mail. Its security features include: email address filtering, email subject filtering, and email content filtering.

7) Anti-virus feature is an important feature of the firewall; it uses the virus database and detection engine provided by the built-in anti-virus software company, achieve virus detection and blocking of network traffic, thereby protecting the enterprise's business system from network viruses.

8) The firewall not only provides alarm ways such as system logs and log hosts, but also provides real-time email warning technology. Through the traffic analysis function, there are detailed network traffic analysis results in the email, which can provide administrators for network optimization. There are two ways to send an email; one is to send in real time, once the attack is detected, the email is sent to the specified email address, the other is to send the warning email periodically at the specified fixed daily time.

9) The log feature can save system messages or packet filtering actions in buffer zone or send them to the log host. The analysis and filing of log content enable administrators to check security vulnerabilities of firewall, when someone is trying to violate security policies, the type of network attack, and real-time log record can also be used to detect ongoing intrusions.

3.2 Core Switch

The core switch supports many routing protocols; its main function is to exchange data and route, similarly, some switches support firewall functions like ACL (Access Control List).

In allusion to the problem of network IP address theft in the enterprise network, the IP and MAC of the protected computer are bound on the core switch, so that users who steal IP cannot access the enterprise network; add some servers, industrial computers, computers and other devices to the ACL (Access Control List), only the specified network segment is allowed to access, and partial access control functions are achieved.

ACL can limit network traffic and improve network performance. For example, ACL can assign priority of packet based on the protocol of the packet.

ACL provide means of controlling communication traffic. For example, ACL can limit or simplify the length which route update information, thereby limiting communication traffic through network segment of the router.

ACL is the basic means to provide secure access to the network. ACL allows Host A to access the human resources network and reject access of host B.

ACL can determine which type of traffic is forwarded or blocked at the router port. For example, users can allow E-mail communication traffic to be routed and reject all Telnet communication traffic.

For example, a department requires only WWW function can be used, which can be achieved by ACL, for example, in order to the confidentiality of a department, it is not allowed to access the wide area network, and the wide area network is not allowed to access it, which can be achieved through ACL.

However, the specialized firewall products not only support ACL filtering way, but also defend against various network attacks, and can also carry out dynamic packet filtering, so the switch cannot replace the firewall.

3.3 Strengthen Information Security of Terminal Equipment

The terminal equipment such as servers, computers, and industrial personal computers, the following security measures are adopted:

1) Fix high-risk vulnerabilities

The computer or server is used to build system vulnerability scanning and fix software, download and fix system vulnerabilities for client computers in the enterprise network, such as 360 Security Enterprise Edition.

The vulnerability scanning software is deployed, periodically scan the whole network segment of the computer, and timely notify and modify the scanned high-risk vulnerability computer.

2) Set a strong password

Each terminal device's power-on password and various application systems need to set a strong password of more than 12 number, including numbers, letters, symbols, etc., such as "AppLe, 785364@Xxzx".

3) Deploy anti-virus system (SEP) and desktop security management system (VRV)

The anti-virus system specification is a top-down three-level architecture, which realizes the unified management and distribution of virus definition codes from the server to the client, and reduces the impact of computer viruses on desktop computers, the desktop security management system can realize the real name system of desktop computers, illegal connection and mobile storage management, and reinforce the system's protection abilities.

4) Identity management and unified authentication system

The identity management and unified authentication system are implemented, this system uses USBKEY and PIN code two authentication ways, implement unified security authentication of the user identity of important application systems, and ensure the security of system access.

5) Self-built system security protection

The virtualization layer is used to centrally deploy on the application layer of self-built system, the system data is saved in one or two databases, which is convenient for administrators to carry out security protection and fix vulnerability.

6) Execute confidential system

According to the confidential management requirements of the oilfield company, the confidential system is strictly implemented, and the most basic principle is followed: confidentiality is not online (any network), and not confidential on the Internet. Any confidential files cannot be transmitted over the network, including email, FTP services, etc.

4. Conclusion

With the continuous advancement of digital oil fields and office networks, the importance of information security system construction will become more prominent. With the continuous development of information security technology, the construction of information security system will also be a process of continuous improvement. This paper analyzes the hidden dangers and problems the information of oil production plants face, proposes solutions specifically, builds relatively secure enterprise network information security system, and promotes the development of enterprise information.

References

[1]. Yan Bin, Qu Junhua, Qi Linhai, Study of Construction of Network Information Security System of Electric Enterprise[J], Modern Electric Power, 2003, 1.

[2]. Wang Yu, Problems in the Enterprise Network Information Security and the Countermeasures[J], Journal of Hefei University of Technology (Natural Science), 2003, 1.

[3]. Sun Hongmei Jia Ruisheng, Technical Architecture of Enterprise Network Information Security under Big Data Background[J], Communications Technology, 2017, 2.

[4]. Lin Shixi, Lin Xiaodi, Establishment of Network Information Security Protection System in Power Enterprises[J], East China Electric Power, 2010, 5.

[5]. Peng Haishen, Research of Enterprise Network Information Security Based on WIFI[J], Bulletin of Science and Technology, 2012,8.