Email Information Security of Enterprise based on Big Data

Ying Wu

Shanghai University of Political Science and Law, Shanghai, China

wuying@shupl.edu.cn

Abstract. The era of big data, more and more huge amounts of data, the value of data is becoming more and higher. The loss of any data will give users bring huge losses. So the enterprise internal email system security is paid attention to by the large number of enterprise managers. This article focuses on the enterprise mail information security problem, through to the enterprise mail in use process safety hazards and the analysis of the potential safety hazard, put forward the basic idea of how to ensure enterprise Email information security.

Keywords: Email Information Security; security risk; security policy; Big Data.

1. Introduction

In the era of big data, information data is particularly important, convenient to express their wishes, each other can respond fast and convenient, gives the negotiations as convenient. Email is to be able to the tool of fast information transmission and exchange, it is the world's only one word class communication exchange protocol, Email as a foundation for the Internet application, now is the important tool of corporate communications synergy.

According to a report by the China Internet network information center, the proportion of the enterprise to use email reached 89%, 37% enterprise Internet marketing using email marketing, so to speak, today's corporate office has been inseparable from the email. But for a long time, about phishing email, mail fraud, mail the leak problems such as frequent, not only the economic losses to the enterprises and individuals, serious and even a threat to national security. So safety problem has become one of the enterprise security problem that nots allow to ignore.

2. Security threats facing the enterprise mail

2.1 Use malicious monitoring software, lead to leak sensitive information

Malicious monitoring software is not really a Trojan or virus, but it is much more difficult than Trojan horse or virus prevention; These malicious monitoring software, which could come in quietly to your system, and can in the case of your unconscious, the system of privacy information is sent to the system. Once malicious monitoring software “visit” your system, then your system will be subject to security threats.

2.2 Phishing by putting on a Trojan

The so-called "phishing" refers to is when your account has a problem, someone will let you by sending the authenticity of a user name and password to verify your identity to solve the problem. Looks like really, but it's not, it is a means to steal user information. Sometimes ask for information of the place may let you link to a fake site, so the user on high alert.

2.3 Financial fraud to mail through the web fake

So-called fake web, is to use Email to lure users to imitate a real enterprise website, enticing for fraudulent activities such as they enter the credit card number.

In fake email on the page, the sender pretend to be a real company email address, use "please update credit card information" looks very normal words to lure victims. If don't understand web counterfeit, even very carefully, will use email as is really come from the company. Then click on a real to link, it is hard to figure out were drawn to a looks really fake website page.

2.4 Let email system failure denial of service, so that we can’t carry out normal office

Denial of service is to show through to the server sends a large number of spam or interfere with the way of information, cause the server are unable to offer the normal user services.

Constantly released a loophole in the notification, the email system vulnerabilities are the most common. Hackers often use Email system, combined with simple tools can achieve attack, the user can't normal email.

2.5 Steal the email account, to attack other systems

Now most people have Alipay, online banking, QQ, and other financial and chat software, if say the hackers into your email account, the personal information that you will definitely be leaked, serious is that the money is transferred.

3. Enterprise mail safety hazard analysis

The above five aspects to enterprise mail behind security threat, highlighting the current Email three problems: one is the email protocol is an open, email itself is expressly transmission, to the sender identity at the same time the lack of effective authentication; Second, mail system adopts the plaintext storage, library off risky, improper mail system configuration, failed to timely upgrades, patches, mail system loophole; The third is the question of users use habits, many users with weak password Email and often don't make changes, often can open the file without detection and many users in the system is not effective antivirus software installation or to update antivirus software doesn't.

Now to mail some of the latest development trend of information security to draw the following analysis:

(1)Email is becoming more and more targeted attack

Over the years, hackers have understood the use of email for personal attacks, through access to the victim's trust as the means, improve the attack success probability. But penetration with other forms of advanced persistent threats and hidden malicious software, will be targeted attack level to a new level, and the situation is not optimistic.

(2)More and more common senior malware

Network crime has always been to rely on email as a PDF file, transmitting infection, .Exe files, and other malicious attachment tool, this way of attack has not been changed. But the change is additional malicious software technical complexity. Although a large number of reports have demonstrated the overall number of spam level decreased, but the number of emails with malicious code is more and more.

(3)Identify new target data value

Once upon a time, fishing the attacker to get the user login credentials with the credit card information, such intent continues today, but today the target range is more extensive, including to steal a large amount of data, including intellectual property, such as product design and the source of this information. Pick up the mail of malicious software can not only avoid detection has higher information theft ability at the same time, quietly into a variety of classification system server and will eventually move company or organization is the most sensitive information. And a focal point in such a way as before, the mail gateway is a very important information and key chain, by Internet crime group use the most direct way.

4. The idea of ensuring the security of mail information in Enterprises

Enterprise mail should be said to be the core of enterprise security, Email security issues related to enterprise security two aspects, one is to get the core of the enterprise's secret, that is, two is to undermine the production of enterprises. Mail and everyone have a relationship, and the competitiveness of each enterprise is closely related to the protection of the security of the message is the core issue. Below we discuss from two aspects of the development of security policy and Email security encryption methods.

4.1 Security strategy

(1) To assess the role of Email in the organization

Enterprises have realized the importance of security, but it is still in use in the form of do not conform to the requirements of the safe Email system, you should understand in the enterprise use email the specific way and ensure the compliance with the existing risk tolerance. "You need to use email which task?" To Base on this consideration to protect the whole system including the application, the server and connection mechanism.

(2) To review management means

Email management strategy must be deeply rooted in the business system, and the only way to achieve this goal is to set a proper governance and execution mechanism, and has strong support from business leaders. One set of the governance body after a targeted adjustment helps to solve the difficult security situation, such as business executives used carelessly the rogue resources. And cross functional entity (such as legal, IT and human resources staff jointly build) are better able to explain the use of against compliance requirements resources what bring security risks, to ensure that the senior management team from the illegal practice, and at the same time inspire IT department to find the ideal security solutions.

(3) Develop acceptable and feasible policy

Management department also need to ensure that the management policy has the acceptability and feasibility, and for mobile, cloud computing, social networking and other important issues to adapt and update.

When companies sometimes use policy often don't consider the acceptable level of content, and it also ignores the training users follow these policies or remind them according to the policy to do this important work. Have the acceptable use policy should be updated every year and always adhere to the user friendly the core features. Customers need to clearly understand what behavior conforms to the requirements and what needs to be resolutely put an end to, it is more important to help them understand the reasons.

(4) The user training as the best weapon against phishing attacks

We should implement related training for users of phishing attacks. People are easily deceived by such way expressions, but also for yourself to receive the contents of the lack of proper guard.

4.2 Email security encryption method

(1) The use of symmetric encryption algorithm to encrypt Email

Symmetric encryption algorithm is applied earlier encryption algorithms, mature technology. In symmetric encryption algorithm and data sent will clear (raw data) and the encryption key after dealing with the special encryption algorithm together, make it become complex encryption cipher text to send out. The receiving party, after receipt of the cipher text to read the original, you will need to use encryption used keys and the same algorithm of inverse algorithm to decrypt the ciphertext to, to make it back into readable plaintext. In the symmetric encryption algorithm, and the key is only one, send receiving both use this key to encrypt and decrypt data, which requires the decrypting party must know in advance the encryption key. Symmetric encryption algorithm is characterized by openness, small amount of calculation, fast encryption, encryption, high efficiency. The downside is that both parties are using the same key, security is not guaranteed. To take advantage of symmetric cipher algorithm to encrypt Email, transmission, storage, exchange the password need to be solved. This type of email encryption system is rarely used.

(2) Use of PKI/CA authentication encryption to encrypt Email

PKI (Public Key Infrastructure) is a Public Key Infrastructure, CA (Certificate Authority) refers to the certification Authority. Working principle of PKI/CA is through the distribution and maintenance of a digital certificate to set up a trust network, in the same trust in the network by the user application to the digital certificate to complete the identity authentication and security processing. Registry is responsible for the audit certificate of the applicant's true identity, after approval, will be responsible for user information through the network authentication center, card processing by the certification center is responsible for the final system. Certificate shall be revoked, update, also is to be submitted by the registration agency certification center for processing. A typical, complete and effective CA system should be provided with at least the following parts: the public key cryptography certificate management; Blacklist of publishing and management; the key to backup and restore; Automatic update key; Key management; Support cross certification, etc. PKI/CA certification system is relatively mature, but also exists when applied to the systems designed to encrypt Emails key management complex, need to exchange key can decrypt add operation, such as the famous systems designed to encrypt Emails PGP encrypted is to use the encryption process. This encryption method is only applicable to enterprises, units and some high-end users, because the CA certificate for trouble, exchange and trival, so this Email encryption mode has been difficult to popularize.

(3) The IBC (SM9) encryption

The IBC (Identity - -based Cryptography identification password algorithm) is the password to emerging technology. In the id password system, each entity has a meaningful, only logo, the logo itself is the entity's public key. Without prior consultation with the password or exchange certificate. Can greatly reduce the traditional application and verification certificate system, easy to use. The algorithm in 2008 won the state password administration of commercial cipher algorithm models: SM9 (commercial cipher algorithm) no. 9.

Based on the IBC to achieve security authentication, users can use the cell phone number or Email address as id, easy to use, in the process of certification without any user name and password, safe and reliable. It works mainly adopts the Challenge/response mode of CHAP Authentication Protocol, referred to as "CHAP (Challenge Authentication Protocol). The agreement is based on signature challenge/response, can resist the Trojan, such as password dictionary attacks.

5. Conclusion

Mail system is an important link in network security, especially the spam has become a global problem, rely on purely technical means is not, or should be used in management and technology, with advanced technology as the foundation, in order to perfect the management system and laws and regulations as the basis, relying on coordination the cooperation of all operators and mail service providers, to regulate the mail subject of social activities, to achieve the ideal goal.

References

[1] Shi Jingwei. Enterprise web spam defense technologies and solutions. Financial Computer of China. 2013 (5).

[2] Zhang Lu. Network behavior recognition of anti-spam technology research [I]. Silicon Valley, 2010 (10).

[3] Li Xinjie. Spam behavior recognition technology research field. Computer Technology and Development, 2011 (10).

[4] Li Jie. Spam and anti-spam technology analysis [I]. Science and Technology of West China. 2010 (3).