10 ways to protect data in businesses

In this article, I will show you what to do to secure the data for your company.

Network administration **- Many organizations focus on protecting against external attacks, but ignore even more dangerous dangers: data theft by someone inside the company. This is an important perspective that needs to be addressed in security.**

Hackers who attack "take down" networks often receive a lot of attention, so companies are often concerned with protecting against these threats. However, if your organization only focuses on this type of security, it is similar to putting all the effort into preventing an attacker from attacking the company but forgetting to care about the thief. hiding at the back door and "stealing" all the precious assets.
Unfortunately, security precautions used to prevent DoS attacks, viruses, worms, and other attacks do not seem to be able to solve the more insidious problem: stealing company data for the item. Spy target or other purposes. Exposure of trade secrets to a competitor or the release of private company information to the media, in some cases, can cause a lot of loss compared to the time of suspension. dynamics of machines.

In this article, I will show you what to do to secure the data for your company.

1. Implement the principle of minimum privilege and establish policies for recording

There are two opposing philosophies from which you can set network access policies. First, the policy is ' *open all* ', assuming that all data is available to everyone unless you need to restrict access. Second, the ' *minimum privilege* ' policy, works on the assumption that all data is limited to a maximum before each user unless they are given access. The latter is like the ' *need to know* ' policy of government intelligence centers: Unless users have an urgent need to access a specific file, they will not be able to access it.

One thing to clarify is that **employees should not copy important information or take it home, or email outside the internal network without permission** . However, unless such policies are set in paper documents and signed by employees to confirm, otherwise it is difficult to force your users to implement those policies well. Unwritten rules will be very difficult to enforce.

Policies also need to be specific and there are examples of what is prohibited. Employees may not understand if they are not explicitly explained, such as emailing a company document in the name attached to someone outside the network (or even to their own account at home) will violate the policy of copying the document to USB and talking about it outside of its company.

In addition, expressing policy should be clear in order to express the prohibition not only with the examples you give.

2. Set up access privileges and authentication

It is not possible to depend only on policies to protect your data. Tell the staff what they should not do, this way will prevent someone from making mistakes due to negligence. The implementation of technical policies will strip away their choice of whether to comply or not. So the first step in data protection is to set appropriate privileges for files and folders. It should be noted that data on Windows networks should be stored under NTFS-formatted drives to be able to use NTFS privileges with sharing privileges. The drive's NTFS format will have more details than the sharing privilege and applies to users accessing data on the local computer as well as over the network.

While enforcing the minimum privilege principle, it is necessary to allow users the lowest level of privilege possible so that they can perform their tasks. For example, grant ' *Read Only* ' privileges to prevent users from changing important data files.

You can also set up a file or directory validation action that contains sensitive data so you can know who accessed it and when. In this regard, you can learn more about object access authentication mechanisms on Windows Server here.

There are also many third-party authentication solutions that you can use to verify file access in storage sites:

- NTP Software File Auditor
- Blue Lance LT Auditor +
- isdecisions FileAudit for Windows

3. Use encryption

Another advantage for storing data on NTFS-formatted devices is the ability to use Encrypting File System (EFS) encryption. EFS is supported in Windows 2000 and recent operating systems, it can prevent users from

opening data files even with NTFS privileges. In Windows XP / 2003 and recent operating systems, encrypted folders can be shared with other users by assigning them certain privileges through the encryption dialog.

But there is still a path in which data can be stolen, losing the entire computer, especially if it is laptop computers. In Vista and Windows 7 Enterprise versions, Ultimate, you can use the entire disk encryption function to protect data in case of a computer loss.

In addition to the features that come with Microsoft operating systems, you can choose alternative software from third parties such as:

- PGP Whole Disk Encryption
- Check Point Full Disk Encryption Software Blade

See page 2

4. Enforcement of rights management

Some data theft can be prevented by using the above methods to keep unnecessary people from accessing that data. But what if theft comes from people you need to give access to? You can use the Windows Rights Management Services (RMS) and Information Rights Management (IRM) features in many Office 2003 and Office 2007 versions to prevent users from forwarding, copying, or misusing e-mail and financial communications. Office (Word, Excel and PowerPoint files) that you send to them.

5. Limit the use of external storage devices

One of the most common ways to bring data out of an organization is to copy it to external storage devices. Today's USB drives are very cheap and easy to hide, and their storage capacity is increasing. Users can also copy data files to iPod or MP3 player devices, or to CDs and DVDs using a burner. To avoid this kind of data loss, you need to permanently restrict the installation of USB devices by removing all physical ports or plugging them in with a certain compound. In addition to the above physical measures, you can use the software to disable the use of external devices on personal computers or the entire network.

In Vista, you can restrict the use of external devices (such as USB or CD / DVD burner) via Group Policy. You can also refer to third-party products, such as Portable Storage Control (PSC) of GFI, for example.

6. Good control of laptops

Another way that users can take away important data files in your organization is to connect to your local network using a laptop or handheld device, copy files to its hard drive, then take the computer away. other places. To avoid this situation, you need to maintain strict control over the use of computers connected to the LAN, not only remotely but also plugged directly into the hub or switch in your network.

IPsec can be used to prevent computers that are not domain members from connecting to the file server and other computers on the LAN.

7. Set up guidelines for content sent

Firewalls can block traffic and do not send in or out of the network. They can also allow certain traffic to leave the network. Your data can be sent outside or it can be sent to a virtual door via email, peer-to-peer file sharing, etc. You can set up a firewall to lock out some types of outgoing protocols. , such as those used by P2P software.

It is possible to set up a mail server so that it blocks the sending of outgoing attachments. In addition, you can block content sent by keywords using content filtering devices, software or services such as:

- Microsoft ForeFront technologies
- McAfee's MX Logic
- GFI Mail Security
- Google's Postini

8. Control wireless communication

Although it is possible to block the sending of certain data using firewalls or filtering systems, there are still people who can connect a company laptop to another wireless network. Or still someone can access the Internet using a mobile phone as a modem. To prevent these vulnerabilities, you need to strictly control nearby wireless networks, and, if possible, enforce their signal blocking measures appropriately.

9. Remote access control

Users may not necessarily be in the company to get your company data. With the popularity of remote communication and work on the road, they can fully access the corporate network through many remote access techniques.

10. Need to know the latest methods of data theft

Keep in mind that your data may be taken in different forms. Users can print out a document and take it out of the company, or a thief can steal printed documents from trash cans if they haven't been trimmed. Even if technology is implemented such as rights management to prevent copying and printing of documents, there are people who can use screen capture techniques or even sit and copy information manually. . Know all the ways you can take away your important data, from which you can take steps to protect against them.