10 common network security design errors

In this article, I will show you some common errors and their consequences that can cause compromise for your network and put the company at risk.

Network Administration - It can be said that network security is one of the most important functions of IT. However, sometimes we come across some organizations that overlook the simple but very necessary security design operations. So what are the mistakes that these companies make, in this article we will show you some of the common errors and their consequences that can cause compromise for your network as well as the The company is in high risk.

1. Set up but then forget

The first error we want to show you is planning. It relates to what we can describe through the phrase ' *set but then forget* '. This is what happens when organizations are dedicated to protecting their networks and forgetting to review security plans. The threats to security often change quickly so your security architecture needs to be changed accordingly. The best way to do this is to reassess the security needs of the company on a given basis.

2. Open too many firewall ports as needed

We all know that opening multiple ports too much will be harmful, but sometimes opening the port is unavoidable. For example, get a Microsoft Office Communications Server 2007 R2 server. If you are planning to provide external access, then some ports need to be opened. In addition, OCS 2007 R2 assigns a wide range of

dynamic ports. So what do security administrators need to do in this case?

One of the best solutions is to use a **reverse proxy** (such as Microsoft's ForeFront Threat Management Gateway). A reverse proxy will stand between the Internet and the server requesting multiple open ports. When there is no need to open ports, a reverse proxy can block and filter requests, then transfer them to the server they are intended to send. This will hide the server from the outside world and help protect your network from malicious code requirements.

3. Over-capacity operation

With the current state of the world economy slowing down, the pressure on existing server resources is increasing. A server may have to configure multiple applications as well as multiple application roles. While this approach is not bad, there is a problem that we need to know is that as the size of the application code increases, the risk of exploiting vulnerabilities increases.

Using only a dedicated server for an application is impractical, you need to care about which applications or application roles should be configured on a separate server. For example, to minimize this, an Exchange 2007 server requires up to three server roles (hub transport, client access, and mailbox server). Although you can host all three roles on the same server, you should avoid doing so if you provide Outlook Web Access to external users. Client Access Server role will be effective for IIS in configuring Outlook Web Access. Therefore, if you put the client access server role on the same server as your hub transport and mailbox server roles, you will probably expose your mailbox database on the Internet.

4. Ignore workstations

Someone asked, what is the biggest threat to network security. Our answer here is **workstations** . We can see a lot of organization holes in network security but in fact neglect their workstations. Unless the workstations are completely protected, no user (or malicious websites) can still install unauthorized software without your knowledge.

5. Failure to use SSL encryption where necessary

A website needs to use SSL encryption at any time to protect sensitive information that users are entering, such as usernames and passwords or credit card numbers. However, many organizations still make inappropriate decisions in the process of protecting their portals. The security error here is the insecure content on a secure website. When this happens, users will receive a prompt asking if they want to display both secure and unsafe content. This problem will make the user have a habit of allowing Internet Explorer to provide insecure content.

A less aware but typical problem is that organizations often fail to encrypt important pages within their websites. In our opinion, any page that provides important information, security advice or contact information needs SSL encryption. However, that does not mean that these pages are particularly sensitive, which means that the certificate used by the encryption process will protect the user who is accessing a valid website instead of a page that someone has set up as part of a phishing scheme.

6. The use of self-signed certificates

Because some organizations completely ignore the importance of SSL encryption, Microsoft has grouped self-signed certificates with some of their products. In this way, the web interface can be used to encrypt SSL even though the organization still does not have their own certificate.

While self-signed certificates fix some problems, they are not an alternative to a valid SSL certificate issued by authentic authentication agencies. The main purpose of self-signed certificates is intended to help improve the security of the product until an administrator can protect it. Indeed, a self-signed certificate can provide SSL encryption, but users will receive warning messages in their browser because their computers do not trust these certificates. In addition, some SSL-based web services (such as ActiveSync) are not compatible with self-signed certificates because of reliability issues.

7. Excess status for security records

Although log events are very important in the network, if too much is recorded, it is a different story and can be harmful to your network. Too many records can lead to difficulties or it can be said that the security events you are interested in cannot be identified. Instead of having to try all things, how can you focus on really meaningful events.

8. Random group of virtual servers

Virtual servers are often grouped on configuration servers due to their performance issues. For example, a high-level virtual server can be paired on a server with a low-level virtual server. From a performance standpoint, this is a pretty good way, but this may be a bad idea for security.

It's best to use dedicated virtual hosts for any Internet virtual server. If you have three virtual servers that provide services to Internet users, you might consider grouping these servers on the same virtual host, but not for infrastructure servers (for example, as domain controllers) on the host.

Following this approach will provide protection so your network can resist leaking attacks. A leak attack is the way a hacker attacks a virtual machine and takes control of the host. No one has yet to figure out how to make a real-world leak attack, but it may appear in the next day or two.

9. Set member servers in DMZ

If you can avoid this, don't put any member server in your DMZ. Because if compromised, the member server can disclose information about your Active Directory.

10. Depends on users in installing updates

Another common mistake mentioned in this article is depending on the user in deploying security patches. There are some recent network deployments using WSUS to patch workstations in their networks. However, many of these deployments rely on users clicking on the option to install the latest updates. The problem here is that users know that every time they upgrade, their computer has to restart. Therefore, some people will not upgrade. To overcome this drawback, we should use a patch management solution to push patches automatically, regardless of the user's choice in this regard.