10 tips to help Windows security

Security risks are increasing in large and small business environments. Here are 10 simple tips that may help you.

TipsMake.com - **Security risks are increasing in large and small business environments. Network security is always very important, and this issue is even higher in today's era. This is definitely a top priority in any organization. Here are 10 simple tips that may help you.**

1: Minimize attack ground whenever possible

One of the first steps to take to 'reinforce' a computer is to minimize its attack surface. The more code running on the machine, the more likely the code is exploited. So you should remove all unimportant parts of the operating system and unused applications.

2: Only use reputable applications

For today's market, users tend to use free, heavily discounted or open source applications. Although it is undeniable the importance and utility of these applications in offices and personal use, it is still important to conduct a small study before using these applications. Some free or low-cost applications are designed to serve

users, other applications designed to steal users' personal information or track their browsing habits.

3: Use a regular user account if possible

As a good habit, administrators should use regular user accounts when possible. If malware infection occurs, often malware also has the same rights as the person who is logged in. So, make sure that the malware can cause even more vandalism if the user has admin rights.

4: Create multiple Administrator accounts

In the previous section, we discussed the importance of using a regular user account whenever possible and only using the Admin account when you need to perform an action that requires permission. manager. However, this does not mean that you should use the Administrator account.

If there are multiple Administrators in the company, you should create an Administrator account for each person. Therefore, when a manager action is taken, you will definitely know who made it. For example, if you have an Administrator named John Doe, you should create 2 accounts for this user. One is a regular account for daily use, and the other is a management account that is used only when needed. These 2 accounts can be named JohnDoe and Admin-JohnDoe respectively.

5: Do not write too much audit

Although creating policy audit to record daily events can be very helpful, there is one problem you should remember: something too much is not good. When you perform too many audit records, audit files will take up quite a bit of space. This leads to a situation where you can hardly find the record you want. So, instead of recording all the facts, it's better to focus only on important events.

6: Take advantage of local security policies

Using Active Directory based on policy group settings does not disable the need for local security policy settings. Remember that group policy settings are used only when someone signs in with a domain account. They will do nothing if someone logs on to the computer using a local account. Local security policies can help protect your computer against using local accounts.

7: Review the firewall configuration

You should use fiewall on the outer ring of the network and on each machine in the network. However, this is not enough. You should also review the firewall's exception port list to ensure that only important ports are still open.

The focus is often placed on ports used by the Windows operating system. However, you should also check any firewall rule that accepts ports 1433 and 1434. These ports are used for remote monitoring and connection to the SQL server. They are hackers' favorite targets.

8: Isolation of services

Whenever possible, you should configure the server for them to perform a specific task. In this way, if a server is attacked, the hacker will only be able to gain access to a certain set of services. We recognize that financial pressure often forces organizations to run multiple roles on their servers. In such cases, you can upgrade security without spending money using virtualization. In a virtualized environment, Microsoft allows you to deploy multiple virtual machines running Windows Server 2008 R2 operating systems with only one license server.

9: Apply timeline security patches

You should regularly check the patches before applying them to the server. However, some organizations still have the habit of ignoring the inspection process. Surely we cannot deny the importance of ensuring the stability of the server, but you still have to balance the need to check with security needs.

Every time Microsoft releases a security patch, this patch is designed to target a certain vulnerability. This means hackers are sure to know this vulnerability and will look for deployment options while the patch for the vulnerability has not yet been applied.

10: Take advantage of the Security Configuration Wizard

The Security Configuration Wizard allows you to create XML-based security policies that can be applied to your server. These policies are used to activate services, configure settings, and set firewall rules. However, keep in mind that policies created by the Security Configuration Wizard are not the same as policies created from security templates (using .INF files). Additionally, you cannot use policy groups to deploy the policy Security Configuration Wizard.