Security in difficult economic times

When new servers or computers are allowed to be invested, security is another cost that causes you a headache. However, what if you can protect your network with your network computer without spending much money?

TipsMake.com - **For many people, security is like our search for dentists - you have to do this and this and it doesn't mean we like or are willing to go to such places.** One of the main problems with IT security is money. When new servers or computers are allowed to be invested, security is another cost that causes you a headache. However, what if you can protect your network with your network computer without spending much money?

Of course, well-known companies like General Motors and JP Morgan Chase Bank cannot do this cheaply, but small and medium-sized businesses - as well as individual users - can choose from a variety of code tools. Open source and free software to protect your network and your computer are safe in a tight economy.

Protect the outer ring

Firewall is the most important requirement when deploying any network. Firewall is the gatekeeper of the network - blocking illegal traffic into the internal network, and limiting traffic to and from the network based on the rules you have set up. Think of it as if you locked out of your home or corporate network.

Clean up the old desktop computer that you have used for a long time and take advantage of it - it can run firewall software. SmoothWall Express is an open source firewall based on Linux. This software has advanced features and the ability to protect the outer ring, can run on any computer with at least 128 MB RAM.

Smoothwall Express is simply designed so that any individual user can use it, even if they don't have any Linux experience. This software can run effectively on most hardware (although they are outdated with today's standards) as well as provide intuitive management and configuration through a browser-based console.

Smoothwall Express supports local area networks, wireless networks and even areas known as technology experts called DMZ (demilitarized zone). This software performs all the basic functions of a firewall - port forwarding, outbound filtering, blocking bad IP addresses - as well as providing special features and possible network traffic parameters at a given link. network interface or an IP address.

Network monitoring

Filtering the network traffic allowed to enter or exit the network in the outer ring is one thing. However, you should also monitor traffic within the network to look for suspicious and malicious activities. An intrusion detection or intrusion detection system (IDS / IPS) will help you do this. Besides, when talking about IDS (intrusion detection), Snort is the application you need.

Snort combines management based on signs of threats (such as virus definition in antivirus software) with management based on suspicious activity detection to find potential hazards. With millions of downloads and 300,000 registered users worldwide, Snort is the most widely deployed intrusion detection system in the world.

This software is available for both Linux and Windows operating systems.

Snort is a good example of the benefits of an automated open source community. As new malware and new attack skills are discovered, rules need to be created and applied to Snort to help IDS detect and identify them. However, thanks to the great contributions of the Snort user community, the rules are always updated.

While Snort can run on any computer, Smoothwall Express firewall also includes an IDS function with integrated support for Snort rules. If you've installed a Smoothwall firewall, you can simply use Snort rules to detect without having to install Snort separately.

Computer protection

Even if the external ring is locked, and the local network has been actively monitored, some threats can still be spread through network computers. A firewall and IDS system are still not enough to replace anti-malware software, and you should install this software on each local machine.

Currently, there are many free anti-malware applications available on the market, but users are still "indifferent" to use them. Businesses seem to be charged in most cases. Even so, Microsoft has made the idea of ??turning free Microsoft Security Essentials software for small businesses that can run over 10 computers.

Later, Microsoft automatically added Security Essentials to unprotected computers via its Microsoft Update Service. So even businesses with more than 10 computers running Windows operating systems are still actively protected by Microsoft.

Check the weak strength of the password

Do you use password policy in the office? If not, use immediately. However, we will provide you with a little secret about the use of password policies - the security that appears on paper does not mean that users cannot find a way to avoid their purpose. Users can follow the terms in the password policy but create an open password that is vulnerable to attack.

If you want to test the strength of the password policy you are using, or just want to make sure that users do not weaken your network's security with a weak password, try cracking them yourself.

Tools like John the Ripper or Cain and Abel will use dictionary methods, shallow attacks and hybrid methods to crack passwords. The dictionary attack will try all possible passwords from a dictionary database, while the exhausted attack will try all possible character combinations. The hybrid method will combine both methods for password cracking, such as "p @ ssw0rd" - this word is based on a word in the dictionary but some characters are replaced by special characters.

Based on the test results, you can edit the entire password policy to make it more secure, or simply identify some accounts with weak passwords and then work separately with each person to remind them to use stronger passwords.

Not only that, such tools are not only useful in small business environments - try them on your home personal computer and see how good your passwords are.

Risk management

In order to fill the gap and strengthen the 'defense' of the network and computer, you must first know what the weakness is. Vulnerability scanning can be an effective tool when it comes to where you might be at risk and how dangerous it is. From there, you can manage risks and fill holes or apply a secondary security method to reduce risks.

Nessus has become the gold standard for vulnerability scanning. At one point, this tool was provided free to users, but now it is a commercial product. Nessus software is free to download, but it can be used to pay for Nessus feed (providing tests and audits that Nessus needs for network exploration). Professional Feed costs you $ 1200 a year.

Although not automatic, the Nessus 2 tool is still an open source and forms 'backbone' for free tools like OpenVAS. They may not be as automatic or famous as the Nessus software, but if the IT admin can't stand the $ 1200 fee each year, they can be used, at least to see what they can do.

Individual users can view the Microsoft Baseline Security Analyzer. This free tool from Microsoft will scan your Windows-based computer and find out about the security configuration and missing security updates on your computer system.

Protecting the network and the computer with free, open-source tools can effectively bring bits to the same level as expensive security software and services. Open source tools may not be as sophisticated as commercial software but they work well and are not difficult to argue because they are free.