Small businesses how to fight hackers?

Hackers can crash websites, destroy data and may have other bad behaviors for your corporate network ...

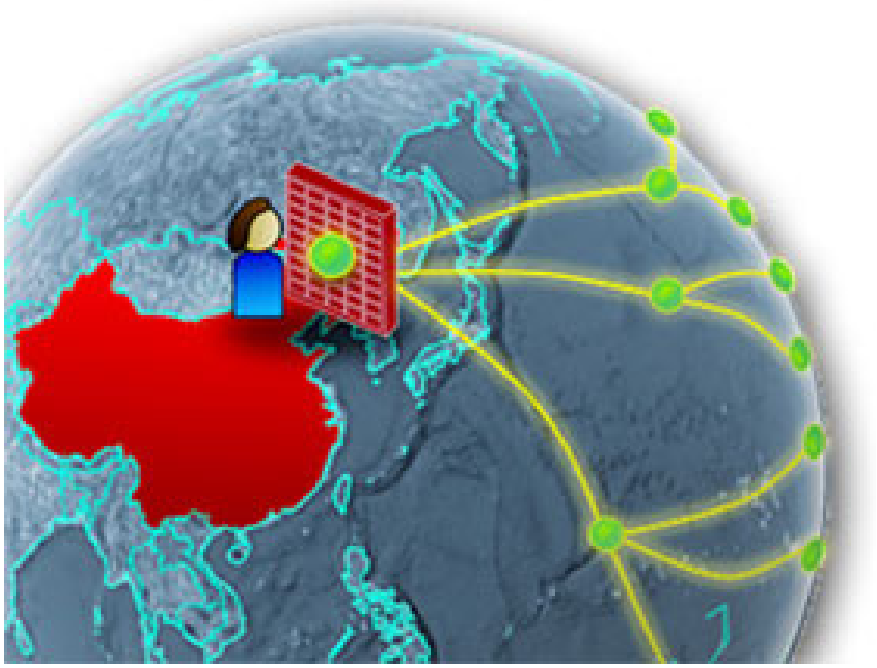
Hackers can crash websites, destroy data and may have other bad behaviors for your enterprise network. All possibilities are possible, and usually the defense capacity of small business networks is not enough to resist in this case.

Attack target

Hackers are always looking at the enterprise network, and only small businesses get enough. Gartner estimates that about 25% of small businesses worldwide were attacked in 2008, up 15% from five years ago. ' *Small businesses are increasingly becoming hackers* ' *targets* ,' said Adam Hils, an analyst with Gartner's network security strategy. According to Adam Hils, part of this reason is because the network of small and medium enterprises is more likely to break into. Stolen items are mainly customer information, and they will be sold on the black market.

However, over time, the nature of common attacks also changes, mainly towards Web surfers or checkmail. In addition, ' *innocent* ' users are also tricked into accessing websites controlled by hackers. Then their computer will be installed with malware to turn the PC into a part of the ghost computer network controlled by hackers. This computer network (often called a **botnet**) will be used to intentionally attack targeted targets, such as a business's computer network. Users often do not know about these activities, they happen quietly. In addition, users are also attacked by hackers using phishing methods (**phishing**) to steal passwords and login information to bank accounts.

Starting from basic



Today, the concept of just protecting the network with simple firewall software is almost no more. The general trend of businesses is that the more employees work outside, they need remote access devices into enterprise computer systems. The gap also followed that up. It could be vulnerabilities from laptops, PDAs, portable hard drives, or even mobile devices themselves to access the network. Typically, desktops and laptops are more secure, and smartphones and PDAs are not used even though they are also used to access corporate networks. However, security is not always a complex technical issue. You can increase the security of the system by simply updating antivirus software, or installing patches for other software running on the system. You should also remove simple and easy-to-guess passwords. As recommended by security experts, to ensure the safety of an important system, you should use a complex password that is made up of 26 characters or more of words, preferably a sentence Say something that you remember, of course you should combine numbers and upper and lowercase letters. Also, every 3 - 6 months, you should change your password once.

To protect the Internet, **you can use a security package that has anti-virus, anti-malware, combined with intrusion detection capabilities, and in some cases even needs E-mail filtering capability of virus** . Those software packages should also be equipped with ' *whitelist* ' initialization applications (secure web addresses). If employees work outside, you also need to make sure they access the corporate network through a virtual private network (VPN). You can also specify website addresses that employees are only allowed to access during business hours.

According to IDC, nearly 60% of small businesses rely on traditional firewall systems. Meanwhile, newer firewall systems often have more functions, they often use a combination of hardware and software to enhance protection. These firewalls also act as a gateway, helping to control data coming into the enterprise network. Many multi-function firewalls also have a detection tool, which helps detect vulnerabilities, or malicious code. They will warn administrators about those risks. CheckPoint, Symantec, SonicWall, WatchGuard, and Zscaler firewalls also have a ' *whitelist* ', which helps businesses minimize the risk of only allowing outside employees to access one certain websites via VPN.

Software updates

Once you have a strong security system, you need to set rules to ensure that your employees do not ' *accidentally* ' destroy the network. Need to set the rules but must avoid causing difficulties for employees, especially to create conditions for them to perform the work in the best way. According to Adam Hils, the most reasonable way is to allow open access to the web, but restrict access to social networking sites during working hours. If you have access, do not disclose your address, password, or any customer information to unknown sources.

' *Excessive* ' anti-virus software will definitely not be safe for you. Some security packages will automatically update, but others require users to activate the process. In most cases, you need to ask your employees to update your security software once a week. In addition, other software applications on the system need to be **updated regularly, especially QuickTime, Internet Explorer, Flash, and ActiveX** . These very common and important applications are often the target of hackers.