10 ways to reduce enterprise security risk

Time is money and when it comes to small and medium businesses, they lack both. Therefore security experts shared tips to mitigate the risk of information security when using small resources.

Time is money and when it comes to small and medium businesses, they lack both. Therefore security experts shared tips to mitigate the risk of information security when using small resources.

What is the best method to ensure safety for small and medium enterprises?

Unlike large businesses that are capable of hiring IT professionals, security in small companies often requires only one 'multi-tasking' person. This method requires the greatest security automation especially for high-level hazards, so a small group can truly effectively protect the entire organization.

Unlike large businesses, small and medium enterprises only spend a few employees working on information security; Many companies rely entirely on advisers or suppliers. On average, small and medium enterprises also spend quite a lot of capital to cope with security issues. CJ Desai, director of sales management at Symantec, said, "Many typical small businesses have come to us and said they spent between 3 and 5% of their IT budget on security." Byrester research comparison, an average enterprise spends 8% of its budget on information security.

From the suggested numbers, many small and medium enterprises have cut investments into security. According to a study by the Small Business Technology Institute, one of the five small companies (less than 100 employees) has not been adequately protected, most of them have no secret police, and many The company only plans to deal after many attacks have occurred. Today small and medium enterprises as well as large businesses can be attacked or targeted by many threats.

Provide a list of threats, as well as the scarcity of time and resources . small and medium-sized businesses need to outline a plan to deal with the security risks currently faced. , using available human resources, time and resources to minimize threats.

Security experts have shared 10 tips to help make the program much faster and cheaper.

1. Defense automatically targets malware

The first idea for prevention for small and medium businesses is to lock and eliminate viruses, worms, spyware and other malicious software including Trojan downloaders and Keylogger software at both endpoints and gateways. . Next, deploy anti-malware software and filtering software for e-mail ports, prevent malware and spam (spam that usually carries malware) to the user's computer. To solve this problem many small and medium enterprises have equipped the 'effective management' tool to run multiple security technologies on the same device.

The one-way gateway defenses will no longer be suitable. As Randy Abrams, technical training director at ESET is also a security software vendor, " *If you shoot too many bullets at the same time, there will definitely be a few passes through.* " . So choose and install the appropriate anti-virus software for every laptop, desktop, server and mobile device. Each program includes a personal firewall that prevents intrusion on the server. The advantages of single devices are easy to control and upgrade.

Use administrative rights on the computer to prevent users from disconnecting security measures, " *so that employees cannot turn off the firewall if the IM doesn't work* " Teixeira Ron, executive director of the National Security Alliance Cyber ??(NCSA) said.

Also take advantage of prevention techniques: Turn off all computers at night. Not only does this prevent the attack during a break, but when the user restarts the computer ' *the operating system can restart and check the entire system* .'

2. Quickly have patches

An effective security program will ensure that the operating system and applications are corrected, without timely patches the entire computer can be 'destroyed'. Therefore, it is always necessary to quickly update the latest bug fixes for servers and computers on the network .

What motivated quickly? " *If asked a year ago, I would say that quarterly updates are very good, but now consider monthly movements, especially when there are more suppliers - not just Microsoft - regularly has monthly patches,* "said Webroot's Gerhard Eschelbeck. However, an effective error correction plan also offers many options: "You can't patch all the errors, you have to depend on the facts." Therefore, external resources - such as the SANS '20 list of Internet security attack targets' - are to determine which vulnerabilities are vulnerable to attack.

In addition, automatically patch as much as possible. Small stores - most of them use Windows - can guarantee regular updates. Small and medium businesses mostly use specialized error management software, increasing the time needed to fix errors on large numbers of computers.

3. Password: should not be taken lightly

Today many accesses require a password. Therefore ' *make sure that all employees have effectively used passwords at any part, using multi-factor authentication technology; Believe it or not, employees in small businesses especially like to use their username and password, so hackers have no trouble finding out* . ' Indeed - dictionary attacks quickly use thousands of words to guess passwords.

Here is a good solution: Users should avoid using actual words, and instead use the first letter of each word.

4. Definition of 'Safe operation'

Which activities are acceptable? While " *you can identify which activities are acceptable when you see them directly* ," but unexpected companies can easily demand this in a operational or legal way, unless they are recorded. paper.

Enter security policies and procedures. " *Users will not know what to do right and wrong, so there are mandatory and restrictive policies,* " Abrams said. In fact, regulations tell employees what they are required to do (change passwords every 30 days) or be banned from doing so (see unhealthy websites).

5. Practical application

To truly maximize safety in the shortest amount of time, part of the "usable" policy prohibits the installation of illegal software on computers. " *Then it is imperative and guaranteed to use only the software for business needs* ."

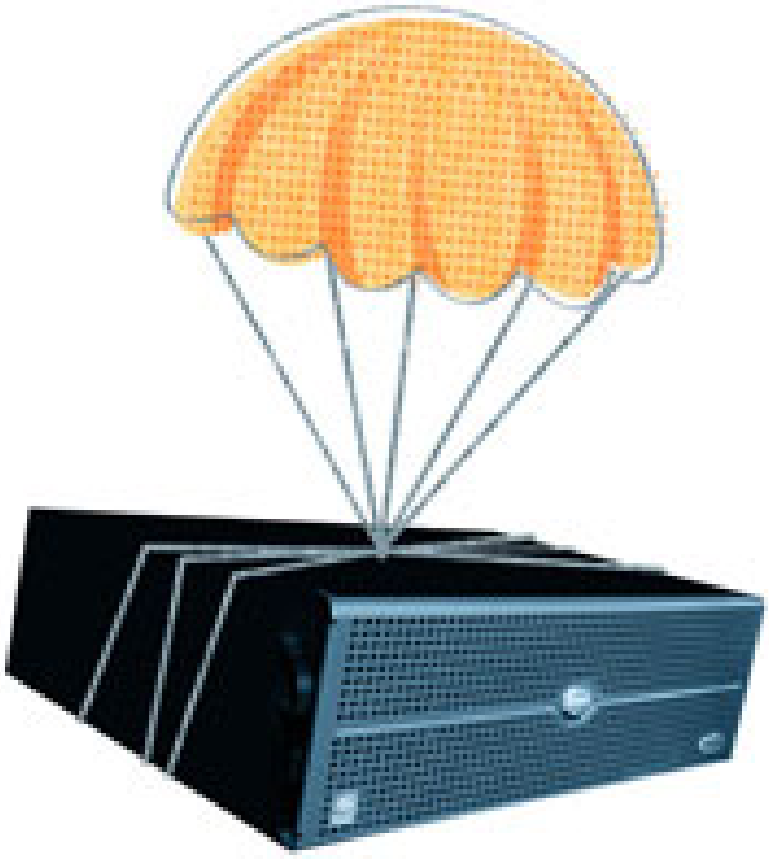
This is an approach to improving safety and saving time because using illegal software will create security holes and need more time to fix errors. Also, if the computer is infected with malware it will be very difficult to eradicate the root. It is much faster to clean up and redo a computer with a standard ghost without the need to install additional applications.

6. Don't get stuck, plan

When something goes wrong, with a sense of security, does an employee know what to do? " *When no one IT staff supports 24 hours a day - this is common in small and medium businesses - employees need a method of handling, at least from coordination and communication* " Webroot's Eschelbeck .

This issue requires time to plan for consideration, admittedly this is a rare typical luxury luxury in the model of small and medium enterprises. Even so " *there is an emergency response plan: anticipate a successful attack and know what to do when it happens* " Abrams advised. In the end, who should employees call when their security software has been infected with malware?

When planning an emergency situation, understand the requirements. For example, if a company stores personal customer information in it, it will ask the company to warn all employees when it finds that information is lost, stolen or the system is compromised.



7. Create backup habits (backup)

Data loss, storms, destructive software, cable breakdowns, damaged hard drives, electric explosions, strike workers and even malware: no problem does not affect data integrity. unless the data is regularly backed up updated. Of course everyone must know how to back up data regularly. Therefore, IT staff must guide every employee to ensure the safety of company data.

An automatic backup software can be used and ensure backup results are stored in a safe location to be ready against attacks. Or more easily and automatically than deploying an automated online backup service, though this way is not always less expensive.

8. Check: protection and protection program

" *If a virus detection program is loud, but no one around, is it really a virus?* " ESET Abrams asked. " *You have checked and understood the records but why were attacked? Because IDS is deflecting everything, you want to know the reason? Because the attacks are always changing until the attacker breaks in. inside.* "

Even small and medium-sized enterprises without an intrusion exploration system still use antivirus programs to monitor screen attacks, and also monitor server security settings. " *Hackers will change security settings to make it easier to come back, be aware that when there is a security change, that is the first sign of intrusion* ."

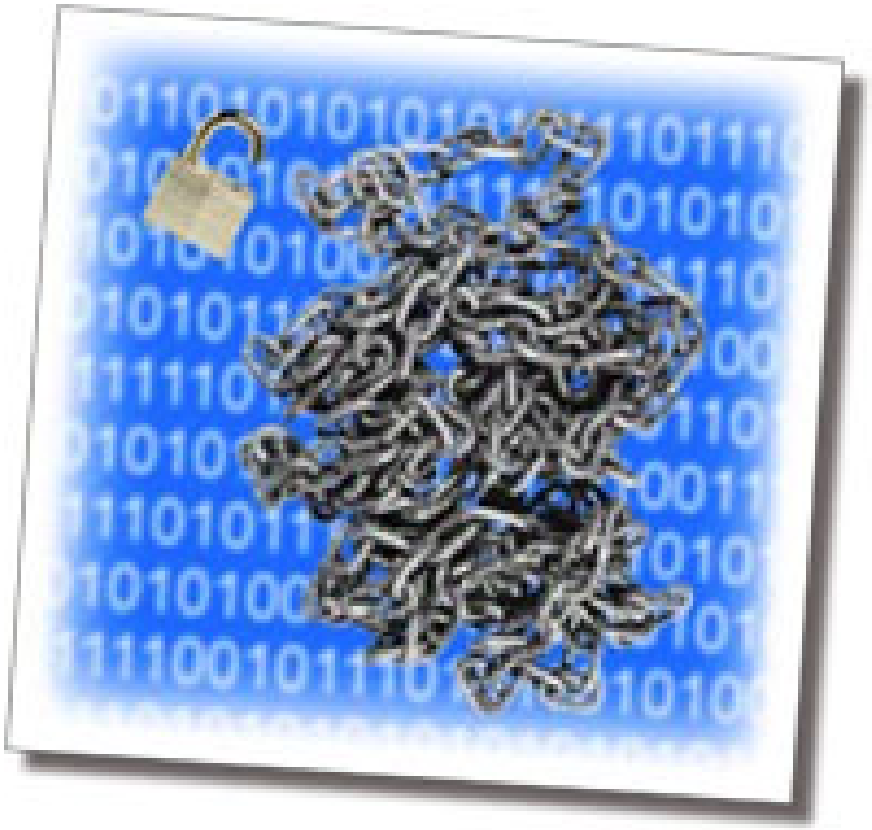
9. Security training: Be creative

For most companies, to be effective, they need to be mindful of people, processes and technology. " *But*

everyone ignored this problem, " Forrester researcher warned.

Always maintain a reliable security chapter. The best starting point is to have a short course so that new employees have basic skills: the help screen will not require a password; Watch out for free Wi-Fi spots because someone will be able to track all the media; use hotel computers or the internet at the airport to copy all data and attachments; Do not open any attachments in e-mail when you see suspicious signs.

This training is not expensive; Funny to say, this is a security approach.



Point out to users that today's major attacks are not caused by the Siberian war taking advantage of computer siege. This is a long-standing habit, a community-based technical attack. Indeed, why are you blocked when you have the right to demand for your needs? A recent example is the attack on the IRS phishing, which begins with an e-mail informing the IRS that it is building a customer reference. If the recipient clicks on the link, the Web page will ask for the name and phone number, promising to pay 80USD when certified by phone later. And so when the IRS needs a credit card number to send money. " *That's when they have useful information,* " Abrams said.

10. Encryption: Set and forget

What is the best way to protect information from loss, theft or misuse? With full-disk encryption software, hard drive data entry becomes difficult for those who do not have access. " *Laptops are lost and what you want is that no one can steal your computer and sell customer information on the Internet* ."

According to information security laws, if a company loses a machine with important information, but the data has been encrypted, it is not necessary to give notice. On average, the price of a data infringement notification

according to Ponemon institute is 182USD for each record (not counting customer units), entire disk encryption is very beneficial for finance.