

Small Business Network Security 101

October, 2008

Brought to you by:



Introduction

What you don't know about Internet security threats may hurt your business.

With broadband usage quickly becoming a standard in the business world and network security hazards on the rise, small businesses without a dedicated IT team are faced with the great challenge of protecting their networks from threats. However, in order to meet this challenge, small businesses must first face a greater challenge: understanding and acknowledging the threats.

The purpose of this document is to provide small business owners, network administrators, and security solution providers with a better understanding of small business security needs and to outline the actions that can be taken to ensure the online and offline safety of small business networks and their data.

Why Are Small Businesses Vulnerable?

Don't say "It won't happen to my business" before you know the actual odds.

Perhaps the greatest threat to small business networks is the owners' false sense of security and their lack of proficiency in protecting their networks. Very often, small business owners push network security issues down the priority list in favor of more pressing matters, and in many cases, network security is not a concern at all.

To better understand the severity of this phenomenon, consider the following research results:

- According a survey conveyed by the National Cyber Security Alliance, "More than 30% of those polled by the National Cyber Security Alliance (NCSA) think they'll take a bolt of lightning through the chest before they see their computers violated in an Internet attack."¹
- The SANS/Internet Storm Center publishes a statistic reporting the average time a "clean" (un-patched and undefended) system can be connected to the Internet before being attacked or scanned. Recent data indicated an average of 20-25 minutes.²

New threats continue to emerge every day, and "lightning" can strike, whether in the form of lowered productivity due to spam, or priceless information such as customer credit card numbers that end up in the wrong hands.

According to a Yankee Group study, 40% of small businesses rank computer security breaches as an important issue, but nearly half defer security upgrades due to cost concerns³. Many others wave off network security concerns, claiming that the size of the company and its insignificance in the market will deter hackers from targeting the network. This is a very misguided approach. Strict regulations such as the Sarbanes-Oxley Act require enterprises to invest more in information security. Enterprises are aware of various security threats and often employ in-house specialists to defend their networks from various threats.

¹ Poll: Lightning strike more likely than breach - http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1011092,00.html

² Survival Time History - <http://isc.sans.org/survivalhistory.php>

³ The State of SMB and Mid-Market Enterprise Security - http://www.yankeegroup.com/yg_research/SMB/Audio%20Conference/SMB-14402/SMB-14402pdf.pdf

Companies with large networks own complex firewall and intrusion prevention systems that are regularly updated and maintained. Small businesses cannot be expected to have manpower, money, or time to invest in maintaining an enterprise-scale network security system. However, this does not mean they should ignore security threats.

A good example of the vulnerability of small networks in comparison to enterprises is the effect of the My.Doom worm (released in January 2004). According to the Internet Security Alliance data, one out of three small businesses was affected, while only one out of six enterprises was affected.⁴

It is not always personal. As you will learn later, most attacks and security threats are aimed at the general public and not directed at any specific company or network. A hacker can run a software program that scans networks and IP ranges, looking for potential weaknesses. When such weaknesses are found, the hacker can take over the machines or infect them, in order to use them as a “zombie army” in larger scale attacks.

But why ME?!

What Happens If I Do Get Hacked?

How much does it cost to be a victim?

According to a survey conducted by the Small Business Technology Institute⁵, 56% of small businesses experienced at least one security incident during 2005; however, less than 30% percent increased security spending during that time. Could you be one of those businesses? Are you aware of the damage a severe attack could inflict on your business?

Think of what would happen if a computer containing important business data was physically stolen, and the data was not backed up.

A severe cyber-attack is no less harmful than physical theft of valuable data.

How much would a new machine cost?

How much irreplaceable data would be lost?

How much would this data loss cost your company?

Can you afford the financial costs, downtime, and hassle?

Each business is different in both vulnerability and risk. The questions above can assist you in beginning to assess the potential damage of an attack on your network. However, there are other threats beyond hacker attacks and loss of information. Know them, and protect yourself.

⁴ “Common Sense Guide to Cyber Security for Small Business” – <http://www.isalliance.org>

⁵ <http://www.sbtechnologyinstitute.org/mi/research/security.htm>

What Are the Threats?

Know your enemy.

Like any technology, Internet security threats are changing and evolving at all times. Hackers adjust their methods and develop them to take advantage of both technological vulnerabilities and psychological weaknesses of employees. Some current threats are:

Security Holes or Vulnerabilities. These are “bugs” in operating systems and software that can be exploited by hackers. When a vulnerability is discovered, the race begins: hackers hurry to develop *exploits*, which are pieces of code that use the vulnerability to penetrate or disable a program or a whole network, before the software developer releases a patch to close the hole. According to the US-CERT organization, there was a 38% increase in vulnerabilities over the previous year⁶. Examining these findings, it seems that it is not the number of available exploits that has been increasing, but rather the competition over finding the exploits. Anyone can join the race, from private companies with commercial motives to private hackers trying to win respect for finding new, severe, and surprising vulnerabilities before everybody else.

Direct Attack. Direct attacks are not unique to enterprises; they can occur in the small business world as well. A disgruntled worker, a very unhappy customer, or a competitor with network knowledge can try to hack into the network with different intentions. According to a Gartner study, only 20% of SMBs consider internal hackers to be a top security issue⁷, while in fact the recent CSI/FBI Computer Crime and Security Survey states that internal attacks occur almost as often as external attacks⁸. Many SMB networks are not adequately protected and leave confidential information exposed and vulnerable to hacker invasions.

There are many motives, from simple curiosity to data theft, that may lead a hacker to come knocking on your office network door – and that door may be wide open. Unused physical LAN ports in the office may also present a threat to corporate network security. As businesses grow and expand their networks, conference and server rooms, as well as unoccupied rooms, are often equipped with LAN ports that are constantly open to intruders of any kind, exposing the corporate network to information theft and abuse of network resources. The existence of these potential security breaches, which are nearly impossible to track in real-time, presents network administrators with a difficult, time-consuming challenge.

Viruses. Although viruses are less common nowadays, they can – and often do – cause damage to computer systems. Commonly confused with worms, viruses often spread over email and recently over instant messaging networks, by disguising themselves as legitimate attachments. The user activates the code unknowingly, thus infecting their system with the virus. Viruses often use the victim’s address book to email themselves to other mailboxes.

⁶ <http://www.securityfocus.com/news/11367/1>

⁷ The State Of Security In SMBs And Enterprises – Gartner, September 21, 2005.

⁸ CSI/FBI Computer Crime And Security Survey - http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf

Viruses can range from merely annoying to dangerously destructive, and they are still widespread: 83% of responders to the CSI/FBI Computer Crime And Security Survey detected viruses on their computers⁹. These statistics reflect the fact that most people who have antivirus software installed on their computers tend to postpone downloading antivirus updates and often do not bother updating the antivirus definitions at all¹⁰.

Worms. Similar to viruses and much more common are computer worms. Unlike viruses, which infect programs and files, worms do not attach themselves to any other software and are self-sustained. Worms often propagate themselves using an infected system's file transmission capabilities, and may increase network traffic dramatically in the process. Other possible effects of a worm include deletion of files, emailing of files from the infected computer, and so on. More recently, hackers have designed worms to be multi-headed, so that their payload includes other executables. The most infamous worm is My.Doom, which, along with its variants, caused several billion dollars worth of damage to businesses, ISPs, and home users.

Trojan Horses. These are software programs that capture passwords and other personal information, and which can also allow an unauthorized remote user to gain access to the system where the Trojan is installed. To protect against damage by Trojan horses, it is necessary to use a firewall with strict control for outgoing traffic.

DoS (Denial of Service) Attacks. This particular threat is valid if you run a Web server with a promotional or Web commerce site. The attack attempts to disable the server by flooding it with fake requests that overload the server. Very often, unable to mount this attack with a limited number of computers and bandwidth, the attacker will create an army of "zombie" machines, by infecting various networks with worms that allow the hacker to exploit the machines and their bandwidth for the attack. This is called a DDoS (Distributed Denial of Service). DoS has become a popular online criminal activity with hacker groups demanding protection money to keep them from ruining businesses. Companies that depend on online commerce are particularly vulnerable to this type of attack.

Spam. Though not officially defined as a security threat, spam can seriously damage productivity and represents a potential risk, due to the current rise of malicious software delivered by spam messages, as well as "phishing". Latest statistics by Symantec indicate that one in every 119 processed email messages is a "phishing" attempt¹¹. Phishing is a method used to acquire personal information such as passwords, bank account and credit card numbers, and more, through sophisticated email messages that claim to have come from a specific provider (eBay for example) and appear quite authentic to the unsuspecting recipient. Phishing is a serious economic threat, with an average cost of identity theft per victim of \$6,383 in 2006¹².

⁹ http://www.fbi.gov/page2/jan06/computer_crime_survey011806.htm

¹⁰ "Survey Reveals the Majority of U.S. Adult Computer Users Are Unprotected from Malware" -

http://www.eset.com/joomla/index.php?option=com_content&task=view&id=1553&Itemid=9

¹¹ http://investor.symantec.com/phoenix.zhtml?c=89422&p=irol-newsArticle_print&ID=843053&highlight=

¹² Javelin Strategy and Research - 2006 Identity Fraud Survey Report Consumer Version - <http://www.javelinstrategy.com/products/99DEBA/27/delivery.pdf>

Spyware and Malware. Spyware and malware is malicious code sometimes found in various freeware or shareware software, as well as in file sharing clients. It takes a toll on system performance and sends user data to the spyware creators. According to a Microsoft anti-malware team white paper, the MSRT (Microsoft Malicious Software Removal Tool) has removed 16 million instances of malicious software from 5.7 million unique Windows computers¹³.

Inappropriate or Illegal Content. Though not considered a security threat, inappropriate content can seriously damage employee productivity. Web sites with illegal content often contain files with viruses, worms, and Trojans horses embedded in the available downloads.

How Can I Protect Myself?

Don't wait for lightning to strike.

If you have read this far, you have passed the toughest challenge for small business network owners. You should now have a pretty clear picture of what the possible threats are and how they can harm your network. The next step is to evaluate the risks and allocate the resources:

Assess your needs and invest correctly. Consider the harm that could be caused if a competitor retrieved customer information. Think of the damage to your business that can be done by Web site downtime.

Don't go overboard, investing valuable time and money in resources you do not need. For example, a home-based business of three employees does not necessarily require web content filtering to avoid questionable content online.

Outsource whenever possible. DakotaPro offers managed security services for small as well as large networks. Check out what security management options we can provide. We can help as your network security consultant and also with network security service provisioning if you do not have dedicated IT staff.

¹³ The Windows Malicious Software Removal Tool: Progress Made, Trends Observed - <http://download.microsoft.com/download/5/6/d/56d20350-afc8-4051-a0df-677b28298912/MSRT%20-%20Progress%20Made%20Lessons%20Learned.pdf>

Ten Steps to a Secure Small Business Network

It's not as complicated as it may seem.

Not Just the Technology – Before you go out and shop for firewalls, antivirus software, and network security service providers, be sure to set the goal. Assess your needs, examine your current resources, and estimate the potential benefits of having a secure network.

1. **Awareness.** Perhaps one of the most important ingredients of a secure network is awareness. Familiarize yourself with various security threats. Be sure to check the availability of security updates and software patches. Increase awareness among your workers. Have them read this document, if necessary. Make sure they do not bring unprotected mobile devices into the network, that they do not open unexpected email attachments, and so on.
2. **Security Policy.** Technology is but a tool in the enforcement of certain rules that are meant to keep your data safe and your business running smoothly. A security policy should consist of various rules and behaviors, such as a password policy requiring users to have passwords that cannot be easily guessed or broken and firewall rules permitting specific traffic in and out of the network. It is highly recommended to consult with a network security specialist when compiling a security policy for an office with more than ten users. It is necessary to enforce the policy once it has been created, to ensure its effectiveness.

The Basics

The following three resources are a must for any single computer or network connected to the Internet.

3. **Firewall¹⁴.** A firewall acts as the security guard between your network and the Internet. Software firewalls that are installed directly on the computer are required in cases where the machine leaves the office, or where it is the only computer in the business. Hardware firewalls installed on firewall-dedicated machines are required in networks comprised of a number of computers.

Firewalls differ from one another: some provide in-depth firewall protection and additional security services, while others simply provide Internet connection sharing with NAT translation, allowing only very basic protection. The main purpose of a firewall is to keep out unwanted traffic, such as a computer worm attempting to infect computers with a specific vulnerability. Note that some firewalls can also be used to block specified outgoing traffic, such as file sharing programs, and to block specified incoming traffic, such as instant messengers or any other service the firewall administrator chooses to block.

Many hardware firewalls offer additional services such as email antivirus and antispam filtering, content filtering, and secure wireless access point (AP) options. When selecting a firewall, define the requirements of your business. Many firewall vendors provide customizable firewalls

¹⁴ To read more about firewalls, visit the SofaWare Web site – [How Do Firewalls Work?](#)

with pricing depending on the range of services you select. If you can, get technical assistance from a local network security service provider.

4. **Antivirus.** Antivirus (AV) software is used to scan files on the computer on which it is installed, files that are downloaded to the computer, and of course email. In addition to implementing AV solutions on each machine, it is important to have an AV gateway: a local or remote machine where traffic is scanned for viruses before it is transferred to the client computer. It is crucial to keep the antivirus software updated at all times, as new viruses are found almost every day. Do not forget that simply having the software is not enough. Schedule an automatic scan if possible. If not, then set a reminder to ensure that you and other office employees run the scan on their computers periodically.

An antivirus gateway installed at the entrance to the network can provide a first line of defense against the latest threats by using automatic updates thus preventing viruses from reaching network computers that do not have the latest virus definitions or patches installed.

5. **Patches and Updates.** Microsoft and other software vendors provide updates that are meant to fix bugs and patch potential security holes in their software. Make sure you regularly check for updates. You can even decide on a specific day (once in two weeks is usually enough) on which to remind yourself and your employees to run the software updates or check the software manufacturer Web site for any updates that may be available.

Disaster Recovery

Be prepared if something goes wrong. Beyond network security issues, there are many more things that can disable your network or leave it vulnerable.

6. **Backup.** Always backup information. The more important the information is, the more copies of it you should have available. Make sure not to leave it lying around or misplace it. Create a backup policy to back the data up regularly. If possible, encrypt sensitive information and always keep a non-rewritable copy (CD-ROM) of the files in a safe location. It is also recommended to back up firewall, email, and Internet configuration settings to enable quick access to these settings in case of a failure.
7. **ISP and/or Gateway Failover.** For businesses that are dependant on Internet connectivity, it is crucial to have a backup Internet connection and a backup firewall/gateway to preserve connectivity and production in the event that your primary Internet connection goes offline or the main firewall/gateway malfunctions. Several firewall gateways offer smooth and automated failover and ISP backup options. If temporary connectivity loss means potential profit loss, be sure to have failover options.

Annoyances

Spam and spyware are not only annoying, but they can be quite dangerous to your network security and, of course, productivity. Another threat to productivity is sites with questionable content, as well as file sharing software.

8. **Antispam and Anti-spyware.** Spam filtering can be implemented on the mail server, on the firewall/gateway, or on the machine receiving the messages. Most antispam software uses various filters and blacklists to attempt to eliminate spam without deleting legitimate emails. In small networks with few mailboxes, you may consider locally set antispam software, but in larger networks with more users, you may want to use spam scanning on the firewall/gateway. Spyware can be removed by using anti-spyware software on the local machine. You may want to include this in your weekly or bi-weekly routine of updates and scans, and scan your network computers for spyware, as well as viruses and worms.
9. **Blocking Specific Sites, IM Clients, and File Sharing Programs.** The best way to deal with questionable sites online, IM conversations during work hours, and bandwidth-wasting file sharing is to enforce their exclusion on the gateway. Some firewalls allow you to select specific services to which access should be blocked and to filter Web sites by address and/or by category.

Improving Productivity Safely

Access your office network whenever you need it wherever you need it – safely.

10. **Remote Access VPN and Site-to-Site VPN.** Virtual private network (VPN) technology allows you to connect two or more networks in a private connection, creating a tunnel of encrypted data between the two points. This technology was adopted to replace expensive private networks (such as frame relay) with increasing popular and available broadband Internet connections. VPNs provide privacy and encryption for the data as it is transferred over the Internet. This is especially useful if you have two or more branches in your business or would like to access your office network remotely. For example, your sales representative does not have to carry confidential information on his laptop when visiting abroad. All he has to do is connect to the Internet and access the data in the office through a secure connection. Numerous security appliances offer VPN server and endpoint capabilities. If accessing your office network increases productivity, or if you have been accessing your office network without using a *secure VPN*, you should select a gateway appliance that offers this feature.

Check Point® Safe@Office® Small Business UTM Solution

The Safe@Office UTM appliance delivers a modular small business security solution that can be tailored to any small business network and its requirements. By combining enterprise-level Stateful Inspection firewall protection, network gateway antivirus and IPSec VPN capabilities with customization options and ease of use, Safe@Office delivers a cost-effective solution for offices with three to one hundred users.

No security expert is required for appliance installation and configuration, as wizard-driven setup options allow simple and quick customization of the firewall and VPN settings to match the company security policy.

Safe@Office Solution for Any Office

The Safe@Office 500 is a fully-integrated stateful inspection firewall, intrusion prevention, VPN and antivirus gateway, specifically designed to meet the needs of small businesses of various sizes.



Employing Check Point's Firewall-1® and VPN-1® technology, Safe@Office 500 affords your network the same level of protection enjoyed by 98% of the Fortune 500 and allows you to extend your secure perimeter to include remote locations and traveling employees, so that you can stay secure and connected anywhere, anytime!

Safe@Office 500W includes an 802.11b/g access point, allowing your business the freedom of a wireless network, without compromising data security.

Safe@Office Internet Security Appliance Features

Safe@Office UTM appliances are high-performance, hardware-based platforms that provide advanced firewall and antivirus protection and support a wide variety of security services from Antivirus Updates to Dynamic DNS.

Stateful Packet Inspection Firewall. Safe@Office UTM appliances are equipped with best-of-breed, patented firewall technology from Check Point Software Technologies, the same technology used by 98% of the Fortune 500. The firewall protects your network from DoS attacks, IP spoofing, and TCP/IP-based attacks, without any need for configuration. The moment you connect your network to the Internet using the Safe@Office appliance, your network is protected: no setup is required on the LAN computers, and no expert is needed to configure the firewall settings.

Network Gateway Antivirus - Stateful inspection antivirus blocks viruses before they can enter the network, providing protection to all the PCs in your network, even if they do not have all the latest patches and updates installed. Using an antivirus at the gateway allows you to have a single point of control for blocking viruses before they enter your network. The antivirus policy setup provides a simple and quick way to define which communications should be scanned. By incorporating a gateway antivirus in parallel to the desktop antivirus, you can assure protection against zero-hour virus outbreaks and provide an additional layer of protection against new viruses in the wild.

Secure Wi-Fi Networking and Hotspots. With small businesses increasingly adopting wireless technology to provide flexibility and lower networking costs, a secure and easy to set up solution is required. The



Safe@Office 500W appliance delivers advanced performance and comprehensive security in a single plug-and-play wireless solution. The Safe@Office 500W appliance supports both the older 802.11b and the latest 802.11g technologies, as well as the Super-G standard that allows reaching wireless network speeds of up to 108 Mbps. In addition, you can easily set up hotspots for your guests. For the strongest safeguards available, the Safe@Office appliance is the answer. It isolates and controls access to your wireless network to protect your data. You can segment the wireless network into separate, isolated zones, with different security policies, SSID, security settings, IP

network segment, and Quality of Service (QoS) settings. The appliance authenticates remote user identities using a variety of authentication standards including the new WPA2, ensuring that only authorized individuals have network access. In addition, it allows using mature, VPN (IPSec) technology to encrypt wireless communication, so that data cannot be viewed or corrupted during transmission.

VPN and Remote Desktop Capabilities. The Safe@Office appliance integrates Remote Access and Site-to-Site VPN capabilities to enable traveling employees and remote offices to securely access network resources. The Safe@Office appliance authenticates remote user identities to ensure that only authorized people have network access, and encrypts communications to ensure they are private and uncorrupted. Using L2TP clients (available in all Microsoft OS) or VPN-1® SecuRemote™ software on their laptops or PDAs, teleworkers and traveling employees can securely access email and other applications on the business network. The clientless Remote Desktop feature allows access to all active network computers, without need for initial setup. With the Safe@Office solution, your business offices can communicate securely with one another, and partners can access your extranet, all over low-cost public networks.

Advanced Connectivity and Traffic Management. More than just a security appliance, the Safe@Office appliance is a full-fledged network router, including a 4-port LAN switch, dedicated DMZ and Wireless interfaces, port-based and tag-based VLANs, and virtual access points (VAPs) in wireless models, enabling the creation of multiple firewall-separated network zones in the office network. The Safe@Office appliance supports advanced routing options such as static routing, source-based routing and OSPF dynamic routing. For an additional layer of security, the Safe@Office appliance allows you to protect your LAN through comprehensive Network Access Control (NAC) using the 802.1x standard. 802.1x port-based authentication reduces the risk of security breaches.

The Safe@Office appliance also includes Traffic Shaper, a comprehensive bandwidth management (QoS) system that enables the administrator to fully control the traffic flow, by assigning weighted priorities, limits, and guaranteed bandwidth for different types of traffic.

To ensure continued business productivity, the Safe@Office appliance can be configured to use a secondary Internet connection in the event that the primary connection goes offline. A cellular or dialup USB modem can be used for the primary or secondary connection.

Safe@Office users can protect their business from objectionable Web sites, using the SofaWare URL Filtering Module (UFM). When UFM is used, employees can access the Internet but are prevented from viewing certain Web sites. Thus the company's productivity is protected and the corporate network is not exposed to the dangers of spam and spyware.

Safe@Office ADSL models feature a built-in broadband modem, eliminating the complexity involved in the installation and maintenance of multiple hardware devices, while reducing the physical space dedicated to networking equipment.

Easy Management and Simple Configuration. The Safe@Office appliance's simple Web-based management enables you to secure your business in minutes. After accessing a setup wizard, you can select one of four pre-set firewall policies (high, medium, low, or block all), or create your own custom security policy. Either way, the Safe@Office setup wizard quickly takes you through the steps of policy creation. Your security rules are as flexible as your business needs dictate — and you can change them at any time and from any place – using a variety of remote management options.

Security Updates and Additional Services. Internet hazards, security standards, and technology are constantly developing. The Safe@Office solution can be customized for your office network and updated automatically with the latest security updates and new features.

For more information on DakotaPro Guardian Pro and Guardian Advantage Managed Security Solutions featuring Check Point Safe@Office Solutions, please go to our web site: <http://www.DakotPro.biz> or contact us at the address and telephone below:



4003 E Speedway Blvd, Suite 111

Tucson, AZ 85712

Office: 520.745.3900

Email: Sales@DakotaPro.biz