Small Business Network Security 101

By Ilana Nijnik

info@sofaware.com

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 and network administrators with a better understanding of security needs and to outline the actions that can be taken to ensure the safety of 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 20-30 minutes. [2]

[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

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.

Many small business owners 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. 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.[3]

But why ME?!

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.

What Happens If I Do Get Hacked?

How much does it cost to be a victim?

According to a Gartner study[4], 40% of small businesses that use the Internet for more than email will be successfully attacked by the end of 2005. More than half of the businesses attacked will not even know it. 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.

[3] "Common Sense Guide to Cyber Security for Small Business" – http://www.isalliance.org

[4] "SMBs Show Preference for Security Services" – Gartner.

- 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?

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

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.

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.
- **Direct Attack.** Though less common in the small business world, direct attacks do exist. A disgruntled worker, a very unhappy customer, or a competitor with network knowledge can try to hack into the network with different intentions. From simple curiosity to data theft, many reasons can cause a hacker to come knocking on your office network door.
- **Viruses.** Though less common nowadays and often confused with worms, viruses are pieces of executable code that can do damage to a computer system. 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. Viruses can range from merely annoying to dangerously destructive.
- **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”. 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.
- **Spyware.** Spyware 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.
- **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 content filtering to avoid questionable content online.
- **Outsource whenever possible**. Many ISPs offer security services for small as well as large networks. Check what security management options then can provide. Network security consultants as well as companies dedicated to network security service provisioning can be very helpful if you do not have an IT staff.

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, antiviruses, and network security service providers, be sure to set the goal. Asses 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. **Firewall**[5]**.** 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 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 email messages are scanned for viruses while they are being downloaded 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.

[5] To read more about firewalls, visit the SofaWare Web site – How Do Firewalls Work?

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 Antispyware.** 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 antispyware 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 Security and Remote Access Solution

The Safe@Office 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 and IPSec VPN capabilities with customization options and ease of use, Safe@Office delivers a cost-effective solution for offices with three to seventy-five 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 Internet Security Appliance Features

Safe@Office network and remote access security appliances are high-performance, hardware-based platforms that provide advanced firewall protection and support a wide variety of security services from Email Antivirus to Dynamic DNS. All Safe@Office appliances include the following features:

- **Stateful Packet Inspection Firewall.** Safe@Office appliances are equipped with best-of–breed, patented firewall technology from Check Point Software Technologies, the same technology used by 97% 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.
- **Internet Connection Sharing and IP Address Management.** All Safe@Office appliances include built-in NAT (Network Address Translation) and DHCP (Dynamic Host Configuration Protocol) features to allow seamless integration with an existing network and connection sharing between multiple stations.
- **Easy Management and Simple Configuration.** Safe@Office appliances provide you with a wide range of management options, both local and remote, to provide all users with the configurability they require. Locally, the Safe@Office can be managed via a Web-based interface that incorporates easy-to-understand wizards and options. For extended configuration options, advanced users can configure the appliance directly via the command line, using SSH. Remotely, the Safe@Office appliance can be configured via HTTPS or secure SSH, when these remote access options are enabled. For increased security, you can configure the Safe@Office appliance to allow administrator access only from specified IP addresses, over VPN, or from local machines. Safe@Office appliances can be centrally managed by the SofaWare Security Management Portal (SMP) to receive customized security policies, additional services, and advanced logging 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.

Safe@Office Solution for Any Office

Safe@Office appliances are available in a variety of feature sets and user numbers to suit your business. All Safe@Office appliances can be subscribed to advanced security and productivity services such as Email Antivirus, Antispam, Web Filtering, Dynamic DNS, managed VPN and security policy, and advanced security logging.

Safe@Office 100/200 Series

Safe@Office 100/200 series appliances protect your computers and data from hackers and reduce network downtime, so you can focus on running your business.

Designed specifically for the needs of the small to medium business, Safe@Office 100/200 series appliances provide easy-to-use, Stateful Inspection firewall protection, while supporting Remote Access and Site-to-Site VPNs. Safe@Office 100/200 offers exceptional firewall and VPN throughput, allowing employees in remote locations to securely and easily access resources that reside on the company network (such as email), enhancing both efficiency and comfort.

Safe@Office 400W Series

The Safe@Office 400W series wireless security appliance is an advanced, fully integrated wireless access point, delivering top performance and comprehensive wireless security in a single plug-and-play solution.

Specifically designed to meet the needs of the small business, Safe@Office 400W is simple to install and manage, allowing your business to become fully secured and wireless in minutes.

Safe@Office 400W keeps your information secret from unauthorized intruders by using mature IPSec technology to encrypt all wireless transmissions. Your network will also be fully protected against external Internet attacks by the world-class Check Point firewall.

For increased productivity, Safe@Office 400W also supports secure remote access and the creation of VPN networks, enabling remote branches and on-the-road employees to remain securely connected to office resources at all times.

For more information on Safe@Office solutions please visit the Safe@Office homepage at http://www.safeatoffice.com, and use the automatic product selector to choose the right solution for your business. If you have any questions, please feel free to use our live chat service to speak with a Safe@Office security expert. If you are interested in posting this document on your Web page or any other media, please contact marketing@sofaware.com .