Global Information Assurance Certification Paper

SOHO Security Best Practices

Lisa Yeo

November 29, 2000

With the proliferation of fast Internet connections like DSL and cable, more small offices and home users are connecting 24x7 to the Internet. Many of these new users don't understand the threat they are now under. In the past, corporate IT departments worried about the safety of information stored on computers, but what happens when there is no corporate IT department? It is up to you, the small business owner, to know the risk and take appropriate action to minimize it.

So, what are the threats of connecting to the Internet? The most highly publicized threat is that of viruses. The specific delivery mechanisms of viruses, worms and Trojan horses vary, but the Internet provides a very effective medium for their propagation today.

Macro viruses spread through shared files, something that email has made very simple and effective to do. Worms such as Melissa automatically send email to address book entries, and new virus delivery methods are being explored even now.

The threat doesn't end at virus infections though. If it did, a good, regularly updated AV product would be all you need. Beyond the threat of virus infection lies that of intrusion.

The goal of an intruder can take many forms. A compromised system could be used as a platform to compromise a more enticing host (say, NASA), or as an agent in a distributed denial of service (DDOS) attack. The attacker could simply steal or corrupt information from the compromised system—financial data, proprietary business information, customer files.

So, what is a small business person, or home user, to do in the face of such threats? The first step is to evaluate the risk to your business of any given threat. If someone compromises your computer and steals business information, what is the impact on your business? If a virus deletes all your data, will you be able to carry on? If your customers find out that your computer(s) have been compromised, will they be nervous that their confidential information has been stolen? Would you be legally liable if your system is used in an attack against another host?

In your assessment, remember to include items such as power failures, hardware failures, theft of equipment and so on. These are all things you need to protect your data from to ensure the continued operation of your business. In fact, you may already have assessed some of the risks to your business and only need to look at the new threats posed by Internet accessibility.

Based on the risk assessment, you can begin developing your security policy. This document will lay out the risks as you perceive them and define the steps you plan to take to minimize these risks.

A security policy defines such things as when backups will be performed, where the backups will be stored, how long backups are kept. You could have policies governing the restoration of files—who can decide when a file is to be restored? The file's owner? A manager? Anyone? Policies are also used to lay the ground rules for Internet access, email usage, conditions for encrypting data even.

Details on writing a security policy can be found by checking the resources listed at the end of this paper.

While you are performing your risk assessment and writing your security policy, there are some immediate steps you can take. These initial steps will not affect the functionality of your systems and will provide reasonable protection. It is not recommended that you stop after implementing these first measures, though.

Install anti-virus software

This step is simple, non-invasive and the payback can be enormous—simply ask anyone that has ever tried to recover from a destructive virus.

Anti-virus protection, however, is more than just installing software. It requires an on-going commitment to safe computing practice. Anti-virus signature definitions need to be updated, regardless of the anti-virus software package you choose to install. Many can automatically update, but you need to be aware of the need to update and check that you in fact have the current definitions.

Further, you need to scan files before you open them. Most scanners provide on access scanning, but that is not always enough. It is wise to be wary of all email attachments, even if they come from someone you know, and scan before opening them. Schedule regular scans of your entire system. Change the default scan settings to include all files, not just certain types.

Perform regular backups

If your system is compromised, by virus or attacker, you can use a backup to restore your system, especially your data. Backups are important even without the threats posed by the Internet. They help protect against hardware failures or other catastrophes.

It is wise to keep several copies of your backups rather than immediately writing over the last one. Sometimes attackers will place programs on compromised systems to allow them a backdoor in if the original hole is fixed. When restoring after a compromise, you want to be able to restore from a 'clean' backup, one that definitely doesn't include any files that may have been left, and that may require using an older backup.

Be sure to test restoring from your backups. You want to know that you will be able to restore in an emergency.

The following steps should wait until you have created your security policy. The policy will define what risks you intend to protect against and should lay the groundwork for further modifications to your systems.

Install firewall software

Firewall software is designed to block certain types of traffic based on user defined criteria. There are many products that make configuration simple and straight forward; a handy feature if you're not interested in spending your life configuring firewall rules. For more information on selecting the firewall product that's right for you, see the resources listed at the end of this paper.

You will use your security policy when choosing your firewall software and to direct your configuration choices. Of course, if you don't have a security policy, your firewall rules become your policy, but it is a much weaker approach.

Use strong passwords

This step is especially important if you choose to enable file sharing on your systems. It is often necessary to share files in a networked office environment, and requiring user authentication is the only way to secure access to those shared files. However, if user passwords are easy to guess or crack, then user authentication just provides a false sense of security.

Common guidelines for strong passwords include:

- At least eight characters long
- Mixture of upper and lower case letters
- Contains at least one number
- Contains non-alphanumeric characters (like >,&?)

Picking a password that meets such criteria and is easy to remember can often be difficult, so users write the password down. However, consider this idea to choose a password both easy to remember and hard to guess. Think of a sentence, then use the first letter of each word in that sentence, including punctuation to generate your password. For example, the password Cg4spi: corresponds to the phrase "Common guidelines for strong passwords include:". I know, it's only seven characters, but you get the idea.

Install Operating System/web browser patches & security updates

This can be a risky operation. Sometimes patches break other functionality that you need. It is often wise to perform a backup before applying patches, hot-fixes or security updates.

It is, however, important to be aware of necessary updates so that you can choose which ones will be necessary in your environment. If you are a Microsoft Windows user, you may want to subscribe to their security alert mail list to receive the latest security bulletins.

Specific steps for Windows platforms

Disable unnecessary protocols on Internet interface

Each network interface card (NIC) has protocols bound to it in Windows. By default, all installed protocols, such as TCP/IP, are bound to all NICs. It is unnecessary, even dangerous, to have NetBEUI/NetBIOS bound to the Internet interface. This protocol is used by Windows to aid in file and print sharing, among other things.

To disable unnecessary protocols on the external interface run the Network applet from Control Panel. The specific steps vary depending on the operating system, but for Windows 95, double click the external NIC and on the Bindings tab uncheck any protocols you wish to unbind. Typically, the only protocol you should need bound to the Internet interface is TCP/IP.

Disable file & printer sharing

If it is necessary to share files within the office, configure the security properties of your shares to require user authentication. You configure security for a share by right-clicking the share and choosing properties.

Disabling file and printer sharing is accomplished through the Network applet in the Control Panel.

Specific steps for Macintosh

Turn off file sharing

File sharing is turned off and on through control panel. If file sharing is necessary, disable the Guest account and ensure that only specified users with passwords have access. It is also good practice to place files to be shared in a folder and only share that folder, rather than sharing your entire hard drive.

In summary, the following points should be considered:

- Perform risk assessment
    - specific Internet risks to consider-intruder steals information (how will you know?), intruder alters information, intruder uses system to attack other hosts, virus destroys data, virus overloads mail system trying to send itself to others, etc.
- Create policy based on risk assessment
    - Things to consider include use of encrypted email, frequency of backups, testing of backups, backup storage rules, conditions for restoring files, AV update frequency, what type of file attachments are allowed in/out, how to react to a given threat, will you notify ISP of (attempted) intrusion

Take these steps now…you don't need to finish your risk assessment

- Perform regular backups
- Install anti-virus software

Platform independent steps

- Install firewall software
- Update AV and FW signatures (if applicable) regularly

- Use strong passwords
- install Operating System/web browser patches & security updates
- never run programs unless sure of authenticity

Windows platforms

- disable unnecessary protocols on internet interface
- disable file & printer sharing

Macintosh OS

- Turn off file sharing

Items for further consideration include using encryption to protect files stored on hard drives, limiting physical access to business systems (to prevent your children/spouse from accidentally corrupting data), encrypting sensitive email and installing an intrusion detection system. The value in precautions such as these really need to be assessed individually, especially against the possible usability implications.

The steps presented in this paper should provide immediate, adequate security for your Internet connected computers. It should be noted, though, that security is an on-going commitment. The threats change and tools need to be updated to meet these new challenges.

Resources

The SANS reading room (http://www.sans.org/infosecFAQ/index.htm) has many articles on topics ranging from writing security policies to legal issues to getting started in Information security.

Risk assessment

http://www.sans.org/infosecFAQ/risk.htm

Security policies

http://www.sans.org/infosecFAQ/policy.htm

Anti-virus software

http://www.networkcomputing.com/1106/1106ws2.html

Firewall software

http://www.pcnineoneone.com/howto/intsec.html

http://www.firewallguide.com/

Windows Security

http://www.microsoft.com/technet/security/current.asp

Macintosh Security

http://www.securemac.com

References

Siepmann, Frank. "SOHO Security Solutions". Network Computing. 3 Apr. 2000. URL: http://www.techweb.com/smallbiz/story/5_1.html. (5 Nov. 2000)

"Books and Advice". URL: http://www.cyberdefenders.com/booksandadvice.htm . (28 Nov. 2000)

Markus, Henry. "Internet Security Solutions for Home and SOHO:. PC911 – Friendly Computer Help in Plain English. 2000. URL: http://www.pcnineoneone.com/howto/intsec.html . (30 Oct. 2000)

Hallberg, Carl, Michael Pavlu. "Securing your Home Network". 18 July 2000. URL: http://securityportal.com/topnews/secure20000718.html . (5 Nov. 2000)

Raba, Nicholas. "Security Aspect: Macs and Cable Modems". 10 Feb. 2000. URL: http://www.securemac.com/Cmacscable.cfm . (28 Nov. 2000)