Global Information Assurance Certification Paper

Protecting Your Company from the Small Office or Networked Home Office

Kevin Zimmer

February 12, 2001

With the growing popularity of “always on” 24 x 7 high speed Internet access like cable and DSL modems, more and more people are working from or taking work home. Most users are unaware of the possible problems they can cause if the are not prepared to protect themselves or the companies they work for. These users are responsible for protecting their own personal data and the data of their companies when they bring work home. So, why are you at greater risk now with the use of cable or DSL modems? First of all when you hear the term "always-on" we mean just that. Unless you turn your computer off or disconnect your DSL or cable modem connection, your computer is now exposed in cyber-world with the same potential for being scanned and attacked as the corporations, military, and government organizations.

What are the possible threats to your PC or data? The most common or well-known threat is the virus, worm or trojan. The transport method of a virus, worm or trojan may vary but the Internet is a haven for these. Viruses do not damage hardware; they only affect programs, corrupting or destroy data when the infected program(s) are run. The one exception is the new breed of macro viruses that infect Word and Excel documents. Macro viruses are spread by sharing files and have become very easy to do by the use of email.

Another problem is the intrusion from a hacker or cracker. The goal of an intrusion is to compromise your system. The intruder will try to steal or damage your data to the point where it is now no use to you. They can also use the compromised system to act as an agent to perform denial of service attacks (DOS).

To help prevent these types of threats you must weigh the risks to you and your company. If an intruder compromises your computer and steals or damages the data, what is the ultimate effect on you and your company? Can you recover if a virus destroys your data? Are you liable if your compromised system is used to DOS?

During your risk assessment you need to be aware of the things that are a risk to you and your company. These things can range anywhere from an intrusion, theft, power loss, viruses and acts of nature. You need to protect yourself from these so you have no interruption in your day to day business. Based on your assessment you can start writing your security policy. A good security policy will define what security is, what type of security you need or should apply and define some roles.

What is Security? There are two types of security. The first type of security is physical security. Physical security can range anywhere from a security guard or “trusted” employee to guard something, a locked door, a swipe key card or finger print scanner. The presence of physical security helps deter an intruder.

The second security type is logical security. Logical security means a written corporate or personnel policy that outlines the standards, responsibilities, enforcement and sometimes exceptions the company wants you to follow as an employee.

These policies should also reflect the company's stance on how to deal with Internet access, email, phone calls, general security and any security violations. These policies should let the employees know what they are responsible for, their accountability and the consequences they face when they go against these policies.

Anti-Virus and Backup Software

Some simple and easy lines on defense that can be taken right away are installing backup software for daily backups and installing virus-scanning software. Installing anti-virus software is fairly easy, painless and the benefits are gigantic. Schedule regular scans of all of your computer systems. Keep your anti-virus data definitions and utilities current. There are thousands of virus variations. If your anti-virus software doesn't have the latest virus definitions a new or old virus could sneak through, no matter how often you scan.

If a virus or hacker compromises your system can you recover your data? It is very important that you do regular backups. Backups will help you even if a virus or hacker does compromise your system. It is important to keep backups for a long period of time and not write over the last backup. You want to be able to restore from a "clean" backup. Hackers can leave programs or files that will allow them to enter through a back door that they may have left behind. As long as you keep your backups for awhile, you can always restore lost or corrupted files due to hardware failures or other problems. Make sure to test your backups by restoring from your backup media. You want to make sure restoration is possible in an emergency.

Firewall Software

Another line of defense is using a firewall. Firewall software is intended to block certain types of traffic based on a defined rule or criteria. Your security policy should help you pick a firewall solution and define your rules. One way to test your firewall is to visit http://grc.com and use Shields Up!

You want to use a software package that you can custom tailor to each user's needs. ZoneAlarm is probably the easiest-to-use firewall software you will find. Each facet of the program is clearly separated, and the information is cleanly presented to prevent confusion. ZoneAlarm offers only three security levels; they should handle most small office needs

"Basic firewalls ignore any unsolicited data connection. It's like having call block on your telephone. You can call out and talk to anyone you want without being interrupted. Some firewalls let you screen the connections selectively to allow your computers to work as a server to the outside world. This enables you to keep a Web server or FTP server in your office that the world can get to without paying for a hosting service."

Passwords

A good security policy will help you with security. Some examples are the use of stronger passwords, password protected screen savers on unattended logged in terminals, controlled access and disabling terminated or resigned employee user accounts. Stronger passwords should be used especially if you have file and print sharing enabled. File and print sharing are enabled when you want to share files between other computers or users. You should enable password for these shares to help prevent unessecary access. If your passwords are easy to guess, this can defeat the purpose of using password on your shares.

Some best practices for passwords include:

- 7 – 8 character in length. 8 are preferred.
- Minimum of one number.
- Minimum of two alpha.
- Non-alphanumeric characters i.e. /*.$#.
- Upper case and lower case letters.

Following these best practices formula for a password can be easy to follow but difficult to remember when it comes time to login. A common thing for users to do is write the password down somewhere. To avoid witting your password down, try using a sentence and then use the first letter of each word. i.e. A41a14a! "All for one and one for all!"

Pillars of Security

Confidentiality, integrity and availability are three pillars of security. Confidentiality consists of keeping information private or secret. Integrity ensures the data has not been altered or deleted by anyone other than the intended user(s). Availability is having information available when needed and in a usable form; meaning undamaged, unaltered or not deleted. Without using these three pillars it is hard for other companies to rely or trust your company.

Security Cycle

The following are three cycles to follow when following a good security model. These cycles along with the three pillars of security will help you prevent an intrusion. The first cycle is prevention. Prevention is what is done to keep unpleasant events from happening. This can consist of written security policies, employee awareness, virus scanning, daily backups and network monitoring. Detection is the next line of defense if your prevention fails. You need to be able to determine the damage and take the proper actions to correct the problems. Detection has several shapes, but typically involves some kind of monitoring or alerting function. The most important and final cycle is response. You need to act quickly and respond in a timely manner when you detect a security problem.

You need to find out what went wrong, correct the problem and try to find out the point of penetration if you expect to avoid the security breach in the future. You must remember that this is an ongoing cycle that must be done to help keep hackers from causing damage or other problems for you and your company.

Patches

Installing patches for operating systems or software packages can be a risky task. Some of these patches can effect other programs that are functioning today to stop working. A good practice to follow is to have a complete backup of the system before you apply a patch. These patches are available through the software vendors and are put out there because there is a possible problem with their software.

Disable

Disabling unnecessary services or protocols is a good practice also. Keep only the protocols that you need to connect to network. This will limit what an intruder can use to access your system. Try to eliminate the file and print sharing so you are not as vulnerable to malicious port scans.

Summary

In summary, things to remember when working from home or taking work home and connecting to the Internet:

You must weigh the risks to you and your company:

- Perform your risk assessment
  - If an intruder compromises your computer and steals or damages the data, what is the ultimate effect on you and your company? Can you recover if a virus destroys your data? Are you liable if your compromised system is used to DOS?
- Create your policy based off of your risk assessment
  - Based on your assessment you can start writing your security policy. A good security policy will define what security is, what type of security you need or should apply and define some roles.

Some simple and easy lines of defense that can be taken right away:

- Install anti-virus scanning software.
  - Keep data definition files current.
- Perform daily backups of all critical data.
  - You need to keep backups for long period of time, so you can restore if you lose or corrupted a file(s). You want to be able to restore from a "clean " backup.

- Install firewall software.
- Installing critical software patches.
  - Remember to have a backup of the system you are working on in case the patch(s) cause problem(s).
- Use stronger passwords on shares.
- Remove or disable unnecessary protocols.
- Remove file and print sharing.

Keep in mind the three pillars of security:
- Confidentiality
- Integrity
- Availability

Follow the three cycles of security to help reduce the chance of an intrusion:
- Prevention
- Detection
- Response

You must always remember that security is an ongoing cycle that must be done to help prevent hackers from causing damage or other problems for you and your company. There are new threats everyday and new tools to help catch these threats.

Resources

Sans
http://www.sans.org/infosecFAQ/index.htm

Anti-Virus Software
http://www.nai.com
http://www.symantic.com
http://www.cai.com/products

Backup Software
http://www.cai.com/products
http://www.veritas.com

Firewall Software
http://zonealarm.com
http://www.networkice.com/

Testing Firewall
https://grc.com/x/ne.dll?bh0bkyd2

Security Policies
http://sans.org/infosecFAQ/policy.htm

Risk Assessments
http://sans.org/infosecFAQ/risk.htm

Software Updates
http://windowsupdate.microsoft.com
http://www.microsoft.com/technet/security/current.asp

References

1. Yeo, Lisa. "SOHO Security Best Practices." November 21, 2000. URL: http://www.sans.org/infosecFAQ/homeoffice/SOHO.htm

2. Bigelow, Stephen. "Virus Verities" Practicing Safe Computing. July 01, 1997. URL: http://www.computeruser.com/magazine/national/1513/cadv1513.html

3. Zimmer, Kevin. "What Is Security?" Kickstart Practical. January 2000.

4. McPherson, James. "Network security for the small office." Aug 3, 2000. URL: http://www.microsoft.com/technet/security/current.asp

5. Livingston, Brian. "Self-replicating virus exploits the File and Printer Sharing flaws of Windows networks." Apr. 7, 2000 URL: http://www.infoworld.com/articles/op/xml/00/04/10/000410oplivingston.xml

6. Zenkin, Denis. "Protecting Your Workplace: 10 Anti-Virus Rules." February 5, 2001 URL: http://www.securityfocus.com/
7. Johnston, Mark. "DSL (Defending Someone's Lair) in the 'Always-On' World of High-Speed Internet from the Home." October 11, 2000 URL: http://www.sans.org/infosecFAQ/homeoffice/DSL_home.html