ABOUT SECURING ECONOMICAL APPLICATION ON OUR SYSTEM BY PROTECTING OUR COMPUTER FROM INTRUDERS

SORIN MIHAIL SAV *

ABSTRACT: *Computer security is one of the most important issues in the computer world. With the number of viruses and other malicious software that prey on exploits in the Windows operating system increasing, we need to take preventative measures to make sure that our computer does not become infected. The days of only having to worry about e-mail attachments and documents on a floppy disk are over. Nowadays, viruses or worms actively seek out computers to infect without the computer user even doing anything. Once a virus or worm has gained entry to a system, the invaded computer can turn into a virus distribution centre. Often, the computer sends copies of the virus to all of the people in its address book. Even worse, the infected computer may begin to scan a block of IP addresses (that is, computer addresses) to try to find more machines that it can infect.*

KEY WORDS: *Port, Exploit, Firewall, DCOM, Wireless Network*

1. INTRODUCTION

If our computer is not protecting its connection to the Web, it is at increased risk of becoming infected. So how do you protect our Internet connection? That topic is what this whole paper is about. We'll learn how to test our computer and see how vulnerable it actually is. Then, we'll find out how we can use firewalls to build a "brick wall" around our computer. You'll also learn how to turn off some unnecessary services to lower the risk of infection even further. We'll discover how we can secure wireless network connections, as they are growing so much in popularity.

Once we have our computer locked down from the outside, some connections to our computer may still be open, which we do not want to close down. Remote connections need to have certain ports open on our computer so that we can connect remotely to our computer. If we want to share files with other computers on our local network, then we'll want to leave the Client for Microsoft Networks unblocked. However, when we have openings in our computer's security, we leave us vulnerable,

* *Lecturer, Ph.D. Student, University of Petroşani, Romania, savsorinmihail@yahoo.co.uk*

allowing users to get in. To help combat that vulnerability, we'll learn about ways to use the various user accounts settings to assign complex passwords and permissions to users.

2. HOW VULNERABLE IS OUR SYSTEM?

Our computers are a vault of important information. We could have sensitive data on our computer that you do not want the whole world to see. Data such as family photos, personal documents, and financial information can be found on almost everyone's computer. If a virus or an attacker connected to our computer remotely and gained access, that intruder could wipe out years of work and memories as well as steal sensitive personal information. This paper will show us how to test our computer and find out how vulnerable it really is. To do this, we'll be using a nifty online utility to test our Internet security. Then, proper security update procedures will be examined, so we can see if we are really doing what we should to ensure a secure PC.

Testing our internet security. Ports are the gateways inside your computer. When a computer program wants to communicate with a remote computer, it makes a connection to the remote computer with a port, with which it can then talk to the computer. Each computer has thousands of ports - 65,535 to be exact. The different ports of a computer can be thought of as a bunch of different mailboxes. When a program wants to send data to a remote computer, it sends it to a specific port (mailbox) number. Then, provided that a program is on the remote computer that is set up to receive data at a particular port (mailbox), the remote computer can then work with the data that it was sent. Theoretically, nothing is wrong with this scenario. In the real world, however, programs don't always work this way. Programs are not perfect, nor are they always efficient. Sometimes, they are sent data that they are not programmed to receive, which causes all kinds of program errors, including errors that can allow a remote attacker to connect and run commands on our computer.

The technical name for data sent to a program that results in problems is exploit. Because of errors in programs and the exploitation of the errors, we need to protect your computer. Even though we may have all the latest security patches installed, our computer will not be protected forever. It is just a matter of time before someone figures out a new exploit and it starts to spread. Only after the fact is the patch usually developed and distributed. So how do we protect us from future attacks? It is actually a very simple concept. There are a lot of open ports (mailboxes) on our computer that just don't really need to be open to the outside world. Why not close all ports except for one or two you absolutely need so that exploits can no longer get through because they never have a chance to connect to your computer?

How do we close ports and protect our computer? We use a firewall. To give you an idea of how open our computer really is to the outside world, I recommend that we use one of the various online security screening tests that attempt to probe our computer to find weaknesses. The following is a list of sites that I feel does a good job of letting us know how open our computer really is:

- *Symantec Security Check*: http://security.symantec.com
- *Sygate Online Services*: http://scan.sygate.com/

3. UPDATING OUR COMPUTER

Because programs are not perfect, they require updating. Windows XP is a great operating system; however, no operating system is perfect. In order to keep our machine secure and free of the latest exploits, we must update our computer regularly. Visiting the Windows Update Web site (www.WindowsUpdate.com) once every few months is not going to result in a secure, up-to-date computer. Microsoft releases security updates monthly and emergency security updates whenever they are needed. The only way to stay on top of these updates is to check Windows Update daily, subscribe to the Microsoft Security Newsletter, or enable automatic updates.

3.1. Windows update

Microsoft's Windows Update Web site offers an easy way to view all of the updates that are available for our computer. Microsoft releases both critical and features updates that update various software apps and add interesting new features to Windows XP. For example, critical updates fix major security concerns, such as the widespread exploit for Windows XP known as the W32.Blaster.Worm worm. This worm spread to other computers by using a vulnerability in a component of Windows known as RPC (remote procedure call). To fix the security hole, Microsoft released a critical patch that fixed the security hole. Feature updates update bugs and add new features to common Windows applications such as Windows Movie Maker. Using the Windows Update Web site is very easy too. Just key in www.WindowsUpdate.com in your Web browser Address window, click Go, and we'll be there in no time.

3.2. Security newsletter

The Microsoft Security Newsletter is a great way to keep informed about all of the latest security patches that Microsoft releases. Receive an e-mail in our inbox every time Microsoft releases a critical security patch. If you are a home user, visit www.microsoft.com/security/security_bulletins/alerts2.asp for more information on the newsletter. On that page, Microsoft also offers a more technical version of the Microsoft Security Newsletter that will not only notify us of a critical security patch, but will also explain the full vulnerability. If you are an IT professional and want to know exactly what the patch is for, the technical version is for you.

Microsoft TechNet also offers a monthly newsletter that offers security news and advice. This is another great newsletter to subscribe to. It was primarily intended for IT professionals, but home users may also find it useful if they are interested in a more technical approach.

Visit www.microsoft.com/technet/security/secnews/newsletter.htm for a copy of the latest newsletter, as well as information on how to subscribe.

3.3. Automatic updates

Windows XP has a great Automatic Updates service. With the release of Service Pack 3, that service is now even better. With the ability to set a specific time every day to check and install new updates, we now can schedule a time for our computer to automatically check for and apply updates so that we will not have to visit the Windows Update Web site manually. By turning on Automatic Updates is a great way to make sure our computer is up-to-date. However, it is a good idea to visit the Windows Update Web site every few months to make sure that Automatic Updates is still working. If it is, then we should not see any critical updates available when you visit the Web site.

Working with the Automatic Update settings is not a difficult task. Just right-click the My Computer icon located in the Start panel or on our desktop and select Properties. Then, click the Automatic Updates tab and specify the setting that we want, and click OK to save your changes. Users also have the ability to turn off Automatic Updates by selecting the last option on the Automatic Update tab. We should have to be crazy to do this unless we plan on checking the Windows update Web sites daily or subscribing to the Microsoft Security Newsletter. The Automatic Updates service does not consume a lot of system resources. The resources that it does consume are well worth it because of the invaluable service that Automatic Updates provides.

4. FIREWALLS

We now know that our computer is vulnerable to viruses and attackers from the Internet. We also know that one way to help fight those attackers is to block access to our computer on all of the different ports, which can be gateways into our computer. How exactly to block all the ports? Use a firewall. A firewall is a special application that acts like a brick wall that is protecting all of the ports on our computer. When a remote computer attempts to access a computer on which a firewall has been installed, which is blocking the port on which the remote machine is trying to connect, it will not be able to connect and the data that was sent will be ignored and discarded.

Depending on the way the firewall is configured, when data is sent to a blocked port on our computer, the firewall will either respond to where the data was sent from with a message that the port is closed or it will do nothing, giving our computer a stealth presence. Most firewall applications are set up by default to run in a stealth mode, which will provide the maximum amount of protection. Any remote computer trying to connect or send data to our computer with a firewall installed running in stealth mode will think that our computer has gone offline because it is not getting any response. Firewalls can be a very powerful security device. Windows XP benefits greatly from a firewall because it can lower, if not completely eliminate, the chance that your computer will be compromised.

Using the windows firewall. Windows XP has included a firewall - specifically, Internet Connection Firewall (IFC) software - since the product was first shipped. Although the firewall has not been turned on by default, it has always been there. The original firewall was a basic one-way firewall that would block incoming

traffic from the Web. One feature allowed users to open up ports so that they could still use remote applications.

This way, a user could protect all of the ports on the computer except one or two that they had set to remain open so that they could use a program such as remote desktop to connect to their computer from a different location. The new version of the firewall included as part of Service Pack 3 has a bunch of new features that makes use of a firewall even easier while the protection it provides to our computer remains the same.

5. DISABLING UNNEEDED SERVICES

Windows XP includes a lot of extra services and features that most users just do not use and have no reason to have running. Now, I am going to show you some services that we should disable that will make our computer more secure.

5.1. Disabling remote desktop connection

The Remote Desktop feature of Windows XP is a great way to be able to access our computer when we are away from the office or home. However, if we have poor computer security, the Remote Desktop also is a great way for anyone to be able to access and control our whole computer. Remote Desktop is a very risky application to leave exposed to the world. Its security relies solely on our account password, which for most users is easy to guess. If we do not use Remote Desktop, then it would be a good idea to disable the feature.

5.2. Disabling messenger service

Microsoft has included a service in the last few versions of Windows that allows system administrators to send pop-up messages to all computers on a local network. This service can be an invaluable resource for administrators who want to get the word out about some upcoming server maintenance. For example, end users would see a message pop up on their screen that notifies them that the workgroup file server will be inaccessible for the next hour while routine maintenance is performed.

This is a great service - when it is used correctly. Unfortunately, the Messenger Service has been abused. Just because any user can send messages to the entire workgroup doesn’t mean that she or he should. This capability is sometimes not a good thing. Users that are part of large local area network, such as just about every Internet user, can send out a mass message to all users in the same subnet. As you can imagine, some users that know how to use the service have started to abuse it by sending spam to all the users in their same subnet. Nowadays, we may get spam not only in our inbox but also in a pop-up window that could appear at any time.

The Messenger Service, just like any other service or program that is accessible to the outside world, increases our security risk. Although there is currently not an exploit for the Messenger Service that allows remote users to execute

commands on our computer, who knows what the future will hold? To be safe, it is best to just disable this service. We'll also be cutting down on a new type of spam.

5.3. Disabling universal Plug and Play

Universal Plug and Play (UPnP) is kind of like an expanded version of the old Plug and Play hardware support. Many years ago, when we should buy a new soundcard, we should have to going to run at. Then Plug and Play technology came around and automated that whole process so that the user did not have to worry about managing interrupt and address numbers any more. Now there is Universal Plug and Play, which expands the easy install concepts of the original Plug and Play to a whole new class of devices. Universal Plug and Play can not only detect local devices such as hardware (the original version), but it can also detect external hardware such as printers across the network or other PCs' shared drives.

Universal Plug and Play, theoretically, is a great idea. It gives you the ability to easily add and control devices such as a printer across your local network, an MP3 player, a television, lighting devices, and so on. Universal Plug and Play can be thought of as a way to make all of the different electronic devices in our home, or local network, work together. However, there are very few devices, other than remote printers and file shares that take advantage of the new protocol. Universal Plug and Play will play a big role in our computing lives in the future, but not yet.

Universal Plug and Play also presents a security risk for our computer. It continuously scans our local network, which could be a network that is open to the world, for new devices and negotiates new connections. Just as with the Messenger Service, with Universal Plug and Play the surface exposure of our computer is increased, which increases the risk that our computer could become attacked and infected. Unlike with the Messenger Service, with Universal Plug and Play a flaw has been found in the service and has already been exploited. Microsoft was forced to release a critical security patch to fix Universal Plug and Play so that users' computers would no longer be vulnerable.

5.4. Disabling remote registry access

The System Registry is one of the most important parts of the operating system. It's where all of the system settings and configuration data is stored. If we do not know what we are doing and we just start editing entries found in the System Registry, we can render our computer useless. So, protecting our computer's registry is very important.

Included with Windows XP Professional (not Windows XP Home) is a service that allows users with administrative privileges to connect our computer's registry and edit it. Having this service enabled and running is just way too big a security risk. The vast majority of computer users have little or no use for this service. Why would we even want to give anyone a chance at trying to break into one of the most critical parts of the operating system? Disabling this service is a snap. Now we have knocked off yet another unneeded service from your computer.

5.5. Disable DCOM support

The Distributed Component Object Model, or DCOM, is yet another feature that was built into Windows that has caused a great deal of problems. Sure, it provides an acceptable programming interface for programmers who are trying to write network apps, but there are better ways to do that than to use a DCOM.

DCOM has presented quite a few problems in terms of security. Exploits have been discovered for it that has allowed an Internet worm to spread to hundreds of thousands of Windows machines worldwide. Additionally, a very small number of applications actually use DCOM. Home and professional PC users probably will never even use an application that uses DCOM. So why is it on your computer?

DCOM was one of Microsoft's attempts to please software developers. However, this attempt has clearly failed, and yet they still include it. The only thing that it has given to operating systems such as Windows XP is headlines in the newspapers about how some worm exploited it and has now infected thousands of PCs. Disabling the Distributed Component Object Model is a good idea for most computing users.

6. WIRELESS NETWORKS

Wireless networks are growing in popularity because of the ease of installation and the terrific benefits that they offer. Nothing beats the ability to take our laptop and not have to worry about plugging into the network to do our work. The added freedom of a wireless network is very pleasing. Nevertheless, many people do not realize how insecure most wireless networks actually are. To fully understand this, we must realize how exactly a wireless network works. Basically, wireless connections are made up of a base station and a client adapter. The wireless base station broadcasts all of the data to the clients in a circle around the base station, as do the client's adapters.

This creates a large area over which information is broadcast. If we care about the security of our computer and personal information such as credit card numbers, we must configure our wireless base station to encrypt the data that it sends. Otherwise, just about anyone can connect to our wireless network and gain access behind our firewall to all of our unprotected computers. Additionally, users can sniff the wireless traffic and see exactly what we are sending back and forth. It really is amazing how many people leave encryption turned off on their wireless base stations. Securing our wireless base station/access point is very important.

6.1. Using WEP for secure communication

Wired Equivalent Privacy, or WEP, is the first security standard for wireless networks. The basic concept for WEP security is to encrypt the data that is sent back and forth between the access point and the client adapter. This is done using various degrees of encryption strength. A special key, known as the encryption key, is used by computers to connect to a WEP-protected wireless network. This allows the client computer's adapter to be able to decrypt and also send encrypted messages in the same

language as the base station. This standard sounds like a great way to secure a wireless network. However, it presents some flaws. The largest one is that the whole system relies on just one key. If someone's laptop is stolen that is part of a corporate network, the encryption key must be changed for the base station and for all of the other computers using the wireless connection. This change is necessary because the current encryption key could be easily extracted from the system settings. Additionally, someone can potentially derive the encryption key by carefully analyzing the data they intercepted. If you have a wireless base station, I highly recommend that you enable WEP to protect your home. Setting up WEP is different on every set of hardware. Setting up WEP will greatly increase the security of our wireless network. Even though there are some flaws, it is much better than using no protection at all. It has the same effect as a car alarm.

6.2. Using WPA for a more secure wireless connection

Wi-Fi Protected Access, or WPA, is a new, improved security standard for wireless connections. WPA has addressed the weaknesses of WEP; it was developed to create a viable alternative to WEP that is more secure than that standard. The fundamentals are the same between the standards, but WPA has improved some of the various mechanisms that plagued WEP. For example, encryption keys are now dynamic and change often automatically. Additionally, the complexity of the encryption key has also been increased to help fight off users who try to derive a key from data that they capture. One of the largest improvements in WPA is the addition of authentication to the wireless connection. Now, users have to have the right encryption settings, as well as a valid username and password, to gain access to the network. This new standard is just starting to gain momentum. Microsoft has released a special patch for Windows XP that adds this new standard to Windows.

However, installing the patch will not allow us to use this new standard. Just as with WEP, WPA is programmed into the firmware of the hardware components. In order to use WPA, we must have hardware that specifically supports it. Currently, only a few companies offer base stations and wireless adapters that support this new method of security. However, that will change in time. The next time you are considering purchasing a wireless base station and adapter, do some research and pick one that supports WPA to ensure that your wireless communications will not be decrypted and your privacy is secure.

7. CONTROLLING ACCESS TO YOUR COMPUTER

So far, we have spent a lot of time locking down our computer. We have closed down ports and have removed unused services from our computer. The next step to secure our computer is to reinforce the main entry point, the logon. No matter what we do to secure your computer, it all comes down to our security at the user level. If we have no password on our account and have a computer that is not protected by a firewall and other devices, then we are at huge risk of being attacked. Managing user

accounts is very important with Windows XP because the accounts are the keys into the system.

7.1. Managing user accounts

Windows XP includes the same old account manager found in Windows 2000. This easy-to-use and straight forward interface can be found in the Local User and Group Management interface. There are various "good" security practices that you can follow to make your computer practically invincible to many attackers.

Assign a password and rename the guest account. Windows XP includes a guest account that is disabled by default. However, at some time, this account may be enabled by an application. If you have Windows XP Professional, I recommend that you disable this account using. Just in case it becomes enabled again, I recommend that you rename the guest account and also assign it a password.

Clearing the last user logged on. If you are using the classic logon screen, every time a user logs into your computer, its username is stored, and that name is displayed the next time the classic logon screen is displayed. This can be a nice feature, but it also can be a feature that causes a security problem. Knowing a user's username is half the battle of breaking into a computer. If you have sensitive information on your computer, I suggest that you hide the last user logged on.

Disable and rename the administrator account. The Administrator account is the most important account on the computer. Users should not be using the computer under the Administrator account. That just is not a good security practice for anyone that is running Windows XP Professional and has sensitive data on their computer. I like to disable my Administrator account and rename it, so that anyone trying to get in with that account and at that privilege level will not be able to.

7.2. Make sure that every account on our computer has a complex password

All of the accounts on our computer should have a complex password associated with them if our computer is ever exposed to the Internet. Passwords such as easy-to-remember words and key combinations like "asdf" just do not cut it. A complex password is a password that is at least seven characters long and consists of uppercase and lowercase letters as well as numbers or other symbols. SRm3D8&8 is an example of a complex password. Something like that is impossible to guess and will take quite some time for a brute-force technique to crack. Using complex passwords on all of our accounts might not be easy at first, but after a while they will grow on us and we'll have no problem remembering them.

8. SUMMARY

This paper has shown us how to test a how to see, how vulnerable our computer is to attacks and how to protect it by using firewalls and lowering our computer's exposure to the world by disabling unneeded services. We have learned how to secure our wireless networks and how to strengthen our account security.

REFERENCES:

[1]. Beaver, K.; Davis, P.T. - *Hacking Wireless Network*, Wiley Publishing, Inc, 2005
[2]. Herrmann, S.D. - *A Practical Guide to - Security Engineering and Information Assurance*, Auerbach Publications, A CRC Press Company Boca Raton, London, New York, Washington, D.C., 2005
[3]. http://helpdeskgeek.com/how-to/change-boot-order-xp-vista/
[4]. http://www.theeldergeek.com/disk_defragmenter_utility.htm
[5]. http://docs.sun.com/app/docs/doc/819-6990/gdxqy?a=view
[6]. http://www.freepatentsonline.com/y2006/0039563.html
[7]. http://support.microsoft.com/kb/314837A