Global Information Assurance Certification Paper

Securing Your Home Network - A Users Guide
Christopher Edward Stanfield
Date 09/23/2002

Abstract

This paper will explain the need and the how to for securing a home network with high-speed Internet access. It will explain what to do after a broadband high speed internet connection has been installed to a home network. This paper will also include definitions of some common technical terms to this process easer to understand. Furthermore an explanation will be provided of hardware firewall routers and software firewalls to present a clear understanding of the differences between and how to operate each. The Microsoft Windows update utility will also be covered in regards to it function and how a home network can benefit from its installation. Additionally included is an anti-virus software review to help understand the benefits of using each product and which one might be useful to in a home network situation. Finally, a system hardened with some of the products mentioned in this paper will be analyzed by penetration tests from various web sites to measure the security reinforcement discussed in this paper. By the end of this paper, the process of securing a home network should be more familiar and can easily be implemented.

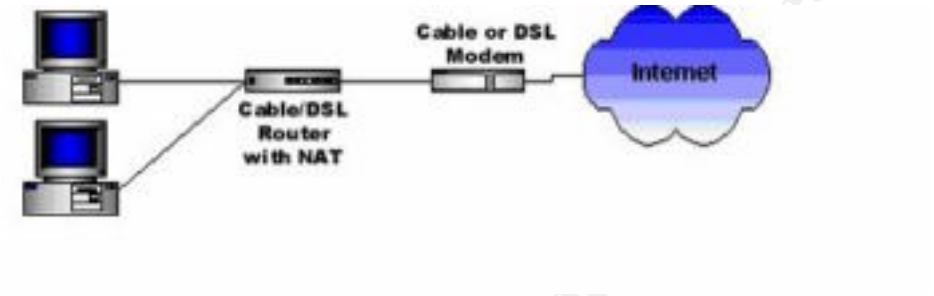
Introduction

In the beginning of 2002 Broadband reached over 30 million subscribers and is expected to reach as many as 117 million by 2004.[1] With identity theft on the rise the need for network security in the home is no longer an option but a method of protection and survival. Per Robert L. Hummel at CNN, “Hackers don't just target national security organizations for cyber attacks. They want your tax returns, network passwords, or bank account numbers.”[2] My first experience with a high-speed home internet connection was in 1999 when I subscribed to a DSL provider. I then installed PC Anywhere, a remote access program to connect to multiple computer systems via a network without having to be physically present at each computer system. I was appalled upon my realization that I could access nine separate Windows 98 home systems. Each of these systems also had PC Anywhere installed for the purpose of friendly communication with other computers. However this software also allowed any external or unfriendly system to connect to a home computer at the same time. I sat there in disbelief and proceeded to uninstall PC Anywhere. The security breaches to my private information that this software presented was threatening enough to convince me to research and learn to harden and secure my home network.

[1] Greenspan, Robyn “Broadband Future Is Bright “cyberatlas.internet 14, August 2002
[2] Hummel, Robert L. “How It Works: Personal Firewalls.” PC WORLD: 05 June 2000.

Background Information and Definitions

NAT (Network Address Translation) is found on most hardware routers/firewalls. The technical people at www.homenethelp.com have provided a clear explanation of how NAT works. “NAT is an acronym for Network Address Translation. It is a commonly used IP translation and mapping technology. To home networkers like you, it is a technology that allows your home network to share Internet access. Using a device or piece of software that implements NAT allows an entire home network to share a single Internet connection over a single IP address. A single cable mode, DSL modem, or even 56k modem could connect all the computers in your home to the Internet simultaneously. Additionally, NAT keeps your home network fairly secure from hackers.”



“NAT acts as an interpreter between two networks. In the case of a home network, it sits between the Internet and your home network. The Internet is considered the ‘public’ side and your home network is considered the ‘private’ side. When a computer in the private side request data from the public side (the internet), the NAT device will open a little conduit between your computer and the destination computer. When the public computer returns results from the request, it is passed back through the NAT device to the requesting computer.” [3]

A firewall is exactly as is sounds it is a wall of protection that can be either hardware or software. Firewalls will allow you to access the Internet but will keep intruders (hackers) out. The two most popular choices for Internet security is to install either a hardware or software based firewall. Michelle Von Wald and Nir Zuk, CTO of One Secure give another example of a firewall’s primary function. “A firewall is hardware, software, or a combination of the two that prevents unauthorized access to or from a private network.” Think of it as Internet customs and immigration. The firewall is the agent that checks each item entering or leaving the network. Each item must pass the right criteria in order to make it through. So a hacker attempting to enter the network of California with a Florida orange would be stopped at the border.”[4]

DHCP (Dynamic Host Configuration Protocol) is also used in conjunction with hardware routers running NAT. Here is a brief explanation of DHCP from “A

[3] “NAT Basics” Homenethelp: 5 Feb 2001
[4] Wald, Michelle Von and Zuk, Nir “Firewalls Explained” Techtv 22 April 2002

protocol that provides a means to dynamically allocate IP addresses to computers on a local area network. The system administrator assigns a range of IP addresses to DHCP and each client computer on the LAN has its TCP/IP software configured to request an IP address from the DHCP server. The request and grant process uses a lease concept with a controllable time period." [5] Otherwise IP addresses are statically assigned to a computer system to access the network. Therefore it is easy to see the security scenarios involved with DHCP. Simply by obtaining a "lease" could give an unfriendly system access to an entire network.

Routers and Firewalls

Next this paper will examine the many different firewall solutions currently out on the security market for home network uses. Remember the hardware-based firewalls are installed between the Cable/DSL modem and the home computers. The hardware firewalls have from one to eight ports on each allowing multiple systems to use a single Internet connection. Software firewalls run on the computer as an application and do not provide any routing services as their hardware counterparts. Even though it is very safe behind a hardware firewall or router, it is best to use a combination of hardware routers and software firewall applications on the home computer. Simply explained, this extra step just adds another layer of security on a home network which makes it more difficult or longer to penetrate.

Hardware Routers

The first firewall to be discussed is the Linksys BEFSR41.[6] This unit uses NAT firewall and routing services, it will also assign private IP addresses via DHCP. Out of the box, this unit is very user friendly for most people to install. The default configuration will allow most people to simply connect the unit properly to home network, install the necessary drivers (supporting software) and then the firewall will be operational. Furthermore, this unit's manufacturer provides a user-friendly web interface through Internet Explorer to change the default password and/or make any other custom configuration changes to the router. This unit also comes with four 10/100 LAN network ports, allowing four separate systems to utilize a single internet connection. A comparable and equally efficient router to the above example is the Netgear RP114.[7] It also uses NAT firewall and routing services, and will assign private IP addresses via DHCP. It also has four 10/100 LAN network ports for multiple systems to utilize one connection. It also has a friendly web interface to customize the default settings. Both routers fall in the same price range (about $99 -$150) and have virtually the same futures. The outside appearance is a little different, the Netgear being more compact than the

[5] Denis Howe The Free On-line Dictionary of Computing: 05 Sept 2002
[6] "Linksys BEFSR41" Linksys: 05 Sept 2002
[7] "Netgear RP114" Netgear: 05 Sept 2002

Linksys. Either one of these hardware routers would make an excellent start to securing a home network.

Software Firewalls

Software firewalls are an application that resides on the computer's operating system and protects it from outside intruders. An outside intruder would be any person, application, or computer not physically sitting at or connected to the home computer attempting to gain unauthorized access to the private network. Software firewalls are not as secure as hardware firewalls alone as each can be manipulated by possible operating system deficiencies. Again having a software firewall installed on every system in a home that touches the network and or the Internet is an added layer of security and well worth the little effort it takes to install. There are many companies that sell software firewalls currently on the market.

BlackICE PC Protection

BlackICE PC Protection is very easy to install "out-of-the-box" and provides firewall protection along with application protection. It reports the attacks in an easy to read layout and by clicking the advice button you can instantly bring up a web site explaining the alert to you in plain English and will give you links on how to report the incident in question. Included in the reports is statistics on attempted attacks, identity (IP address) of intruders. This software also secures both high speed and wireless Internet connections. BlackICE furthermore offers application protection. It can be set to stop a destructive application from running and will warn you if any new programs are trying to start on your system. The application protection can seem a little annoying at times but it is a nice new layer of protection. BlackICE PC Protection estimated cost is about $39.95 for a single user license that has a support time duration of one year.[8]

Zone Alarm

Zone Alarm comes in three different flavors the free version and the two versions that you can buy. The free version of Zone Alarm comes with standard firewall protection and that is it. Of course that is better than nothing, especially for free. The first retail version is called Zone Alarm Pro 3.0 it comes with the standard firewall plus it can also do internet ad blocking, cookie control, "who is" Hacker tracker, and you can completely customize the firewall settings and controls. If you are not sure about moving from the free version to the retail it comes with a 30-day trial to try it out. This version runs about $49.95, which is more than BlackICE, but you are getting 2 years of updates instead of only one. The final version that they sell is Zone Alarm Pro 3.0 with Pest Patrol. The only difference is that it will scan your system for spy ware, hacker tools and Trojans. The other difference is that it will also monitor quarantine or destroy malicious files. This is

[8] "BlackICE PC Protection" Internet security systems: 05 Sept 2002

a great deal considering currently they are charging the same price $49.95 with the added features.[9]

Tiny Personal Firewall

Tiny Personal Firewall is another software firewall solution that we will look at. Tiny Personal Firewall created by tiny software is another great solution for securing the home network. Tiny Personal Firewall software includes statefull packet inspection desktop firewall protection. It will also protect you against viruses like worms, Trojans and malicious code from starting on your system. It reports and malicious activities through its GUI interface making upstanding the attacks that you are receiving easy to understand. This is very similar to the functions of Black ICE. Tiny Personal Firewall runs $39.95 but of course there is always a free version that you can try out first.[10]

Windows Update

Windows could be one of the most important steps you can take to secure your computers on your home network. Windows Update is the tool that Microsoft uses to send you the desperately needed patches and updates to keep your system secure and safe. Windows update can be triggered manually by opening an Internet Explorer browser window and choosing from the top bar Tools and then Windows Update. This will take you to Microsoft's windows update web site. Accept any download windows from Microsoft, as they will pull down the needed software so that you can update your system. You will then be prompted to have Microsoft scan your system. After the scan completes you will be presented with download options from the critical, Windows OS (Your version of Windows) and Driver updates. Make sure you always check and download all critical updates by clicking on the critical updates link in the upper left corner of your screen. The critical updates fix major hole in windows security and will help keep hackers and virus out of you computer. All the other updates are optional and you can read through them and decide for yourself if they are need on your system. If this seems a little difficult to do weekly or even daily then you should consider using the automatic update client the newest version as of this writing, can be downloaded here. [11]
http://www.microsoft.com/Windows2000/downloads/recommended/susclient/download.asp

Here are the configuring instructions from Microsoft web site after you have completed the download of the file.

- Select your language from the drop-down list at the top of the page.
- Click Go.
- Click the link under Download.

[9] "Zone Alarm Pro" Smarter Security: 05 Sept 2002
[10] "Tiny Personal Firewall" Tiny Software: 05 Sept 2002
[11] "Windows Update" Microsoft: 05 Sept 2002

- Do one of the following:
- To start the installation immediately, click Open or Run this program from its current location.
- To copy the download to your computer for installation at a later time, click Save or Save this program to disk.
- Click OK.
- How to use
- To set your preferences for automatic updating, follow these steps:
- Click Start, click Settings, and then click Control Panel.
- Double-click Automatic Updates.
- Select the notification method you prefer.
- If you are running Windows XP, then you will chose the System icon in the control panel and click the Automatic Updates tab to configure your computer system. You can configure it to run at any time night or day.

Anti-Virus Software

Anti Virus Software is a very important step in keeping a home network secure. All of the firewalls in the world are not going to help when an E-mail is opened containing a virus that instance ran and infected the home computer. This is why an efficient Anti-Virus software application is highly needed and recommended. There are several Anti-virus products, however this paper will examine some to top and popular products currently available.

McAfee Antivirus

McAfee Antivirus 7.0 is a great product easy to install and easy to use. McAfee can be set up to pull down product updates as often as you like. The product will warn you if it detects a virus it will also scan you entire hard drive at times that you can set up in the console. McAfee offers a very user-friendly interface. From the interface you can schedule where and when to scan your hard disks. This has become increasingly important with the size of hard disks above the 100 gigabytes. It can take hours for a virus scanner to check the whole disk. An example would be you have a 100 gigabyte hard drive partitioned into a 25 gigabyte c:\ drive, 25 gigabyte d: drive 50 gigabyte e: drive. You could have McAfee start scanning your 25 gigabyte c: drive at midnight on Monday during sleeping hours, then schedule the d: and e: drives on Tuesday and Wednesday at midnight respectively. Scheduling scan jobs, such as suggested above, allows you to protect and check your system with out the inconvenience of performing scans during peek times to use your computer system. Through the user interface you can schedule DAT updates to take place. DAT updates are downloadable files that allow the McAfee software to have the most up to date virus signature files installed. In other words, after the download is completed, your system can detect and remove more viruses than before. At $49.95 McAfee offers a lot of bang for the buck. If the money seems too steep to out right buy the product. [12]

[12] "McAfee Anti-Virus" McAfee: 05 Sept 2002

Norton Antivirus 2003

Norton Antivirus 2003, by Symantec, is another great anti-virus product and is extremely similar to McAfee. It is a very configurable product. Scanning and updates can be set to a time when you are not at your computer like 12 am. You can also download product and virus signature updates. It will scan attachment in both Outlook and Outlook express. It can be installed on a computer that is already infected and clean it. Instructions are on how to clean a system are supplied with the product. Norton Antivirus is also very affordable at only $49.95. Norton and McAfee are both exceptional products, so it really ultimately depends on which of the products appeals the most to the user. I would highly recommend that you download the trial version of both products and test each before committing to a purchase.[13]

PC-cillin 2002

PC-cillin 2002 v9.02 is a lesser-known anti-virus product but that does not get the job done. PC-cillin scans your hard drives along with floppies and other media. Web site are scanned as you surf the Internet with little to no slowdown. Product and virus update can be completed through the software. PC-cillin will scan E-mail for malicious software and scripts. Not only is PC-ciliin 2002 great for detecting and destroying viruses. It also comes with its own personal firewall software. This makes the price of $40 for PC-cillin 2002 a great deal for the home user. As always there is a free trial version for you to try before you buy.[14]

McAfee Trial Version
http://download.com.com/3000-2239-8244960.html?tag=lst-0-1
Norton Trial Version
http://download.com.com/3000-2239-8079062.html?tag=lst-0-2
PC-cillin 2002
http://download.com.com/3001-2239-9649107.html

Testing home network security for vulnerabilities

Now for the true test, taking the knowledge from this paper and putting it into practical use. For this paper I will use my own experiences and tests to illustrate the testing process. In the past I have used both hardware firewalls and software ones. Basically every hardware firewall will always receive a great score on sites like www.dslreports.com. For this test I wanted to try the software side of firewalls. The equipment that I chose was an Intel Celeron 500, running Microsoft Windows 2000 server. I patched any security holes in Windows operating system on the box following the Windows patching instructions in this paper. This took a

[13] "Norton Anti-Virus 2003" Symantec: 05 Sept 2002
[14] "PC-cillin 2002" Trend Micro: 05 Sept 2002

while Windows 2k has been out a while and there has been a great number of security patches to fix the security holes in the Operating System. After many downloads and reboots the patching was complete. I then loaded the firewall software. For this test I chose the Black Ice product. I chose this not because it was better than any of the other products out there but I really like its interface and find it very easy to configure. The newest version of Black ICE performs both firewall and application protection. So at the end of the install Black ICE creates a baseline image of what current applications on the hard disk look like. The reason behind this is if you happen to accidentally run a hackers program from either web, IRC, E-mail or any other means. Black ICE will see this happening and will temporally stop the program from running while it checks with you via a pop up box forcing you to decide if you mean to have that program running. From that point you can terminate the program or accept it so it does not prompt you again. I am running NAT (Network Address Translation) on my Windows 2000 box this is the same way that a Linksys or Netgear router would use to route the network traffic through a Broadband connection. Now don't feel bad if you think using another computer to do nothing but run NAT and Firewall software seem like a big waste. I constantly have friends and family come up to me and ask, "What is the cheapest way to securely route their home network traffic through a DSL or Broadband connection". I always point them towards a Linksys or Netgear hardware router setup like I discussed earlier in this paper.

The Test

There are many ways of doing testing the newly created system. My preferred method of testing is using web sites like www.dslreports.com. Port scanning from your friend's house is not recommended as you could get his and your accounts shut down if the ISP notices what you are doing. A safer way of port scanning would be to pull the system in question off of your Internet connection and scan it on your private LAN. I started off by going to www.dslreports.com and choosing the system scan from the tools area. Here are the results.[15]

DSLreports PORT SCAN results page

Key:

OPEN PORT	a port or ports appear to offer a possibly vulnerable service All services should be closed unless you require them to be open
CLOSED PORT	a port or ports are responding that they are closed A software or hardware firewall may provide you even higher security
FILTERED PORT	The port is silent to basic open-port requests This port or port range was like a black hole - no response was returned.

Further resources

- Security forum
- Premium IP monitoring with 'constant-scan'®
- Security for Cable/DSL networks

[15] DSL Reports Port scan" DSL Reports: 18 Sept 2002

Your IP Address	
Conclusion: Healthy Setup! We could detect nothing interesting on any of the default ports on your IP address. Your computer appears to be a hard target. Well done!	
ALL TCP FILTERED	No response (open or closed) to an open request was received.
ALL UDP FILTERED	No response (open or closed) to an open request was received.

As you can see they gave this a healthy setup! These are the results that are great to see from this kind of web site. The results show that if any of the ports were open they were being filtered so no response from them was received. Let's look at a few more. Next I went to Shields Up https://grc.com/x/ne.dll?bh0bkyd2 website and had them run a port scan on me. Here are the results from that scan.[16]

Your computer at IP:

XXX.XXX.XXX.XXX

Is being 'NanoProbed'. Please stand by. . .

Total elapsed testing time: 9.986 seconds
(See "NanoProbe" box below.)

Port	Service	Status	Security Implications
21	FTP	Stealth!	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
23	Telnet	Stealth!	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
25	SMTP	Stealth!	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
79	Finger	Stealth!	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
110	POP3	Stealth!	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
113	IDENT	Stealth!	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
135	RPC	Stealth!	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
139	NetBIOS	Stealth!	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
143	IMAP	Stealth!	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
443	HTTPS	Stealth!	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
445	MSFT DS	Stealth!	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!

[16] Gibson, Steve "ShieldsUP!!" Gibson Research Corporation: 18 Sept 2002

5000	UPnP	Stealth!	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!

Shields UP gave the test system excellent marks during this test also. This is great but remember no system is hack proof but the results given from these web site shows that even though this system may not be hack proof it is very well protected. Let's take a look at this same system with the firewall shut off.

DSLreports PORT SCAN results page

Key:

OPEN PORT	a port or ports appear to offer a possibly vulnerable service All services should be closed unless you require them to be open
CLOSED PORT	a port or ports are responding that they are closed A software or hardware firewall may provide you even higher security
FILTERED PORT	The port is silent to basic open-port requests This port or port range was like a black hole - no response was returned.

Further resources

- Security forum
- Premium IP monitoring with 'constant-scan'®
- Security for Cable/DSL networks

Your IP Address	
Conclusion: Possible Problem! We did get information from scanning your ports; this information could encourage attackers to probe further. Do you know why you are advertising these services to the net? Perhaps installation of a firewall, or reconfiguration of your firewall to be more secure, would provide peace of mind.	
other TCP CLOSED	We *received a response* that this port was closed.
TCP 80 is OPEN	Advice for OS : any If this is your web server, then obviously you need it to be publicly accessible. General security tips for webservers are to be careful of any opportunity site visitors have to inject any form of HTML into your site, via bulletin boards or other active content, be careful cgi-bin or equivalent active scripts cannot be convinced via user input to misbehave, ensure that any web permission systems are working properly, ensure no directories are listable that you do not wish to be listable. Make sure the owner of the web server process is a user with no permission on the web server machine. Do not bury passwords anywhere in your web server tree, for example, in active scripts of any kind. Do not store data inside the web server tree where the web server could serve it to clients who guess or know the right filename. Ensure web server error logs are reviewed for strange activity.

TCP 135 is OPEN	We have no specific hints for this port number just yet. We are monitoring results though, and we add advice for port numbers that come up frequently.
TCP 137 is FILTERED	No response (open or closed) to an open request was received.
TCP 138 is FILTERED	No response (open or closed) to an open request was received.
TCP 139 is FILTERED	No response (open or closed) to an open request was received.
TCP 389 is OPEN	We have no specific hints for this port number just yet. We are monitoring results though, and we add advice for port numbers that come up frequently.
TCP 443 is OPEN	We have no specific hints for this port number just yet. We are monitoring results though, and we add advice for port numbers that come up frequently.
TCP 1002 is OPEN	We have no specific hints for this port number just yet. We are monitoring results though, and we add advice for port numbers that come up frequently.
TCP 1025 is OPEN	We have no specific hints for this port number just yet. We are monitoring results though, and we add advice for port numbers that come up frequently.
TCP 1026 is OPEN	We have no specific hints for this port number just yet. We are monitoring results though, and we add advice for port numbers that come up frequently.
TCP 1080 is FILTERED	No response (open or closed) to an open request was received.
ALL UDP FILTERED	No response (open or closed) to an open request was received.

Amazingly enough, make sure to examine the results as to what opened up after shutting the firewall software down. We went from a healthy setup up to a problem setup for our rating. Ports 80, 135, 389, 443, 1002, 1025 and 1026 are open for the world to see.

Your computer at IP:

XXX.XXX.XXX.XXX

Is being 'NanoProbed'. Please stand by. . .

Total elapsed testing time: 9.980 seconds
(See "NanoProbe" box below.)

Port	Service	Status	Security Implications
21	FTP	Closed	Your computer has responded that this port exists but is currently closed to connections.
23	Telnet	Closed	Your computer has responded that this port exists but is currently closed to connections.
25	SMTP	Closed	Your computer has responded that this port exists but is currently closed to connections.
79	Finger	Closed	Your computer has responded that this port exists but is currently closed to connections.
110	POP3	Closed	Your computer has responded that this port exists but is currently closed to connections.
113	IDENT	Closed	Your computer has responded that this port exists but is currently closed to connections.
135	RPC	OPEN!	(Remote Procedure Call) This impossible-to-close port appears in most Windows systems. Since many insecure Microsoft services use this port, it should never be left "open" to the outside world. Since it is impossible to close, you will need a personal firewall to block it from external access. Do it soon!
139	NetBIOS	Stealth!	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
143	IMAP	Closed	Your computer has responded that this port exists but is currently closed to connections.
443	HTTPS	OPEN!	The presence of this secure web port in your system implies that this system is establishing secure connections with web browsers. The number one reason for doing this is the transmission of credit card information. This implies that the successful intruder could access the web server's credit card database and score bigtime. This is a VERY bad port to have open unless you are actually conducting secure web commerce!
445	MSFT DS	Closed	Your computer has responded that this port exists but is currently closed to connections.
5000	UPnP	Closed	Your computer has responded that this port exists but is currently closed to connections.

Well the results from Shields Up https://grc.com/x/ne.dll?bh0bkyd2 are interesting it only discovered two open ports. This is a prime example why you should always use more than one source to test your systems. As seen here they only found ports 135 and 443 open where DSL reports found both 135 and 443 open plus it discovered five more ports that were open.

Conclusion

In this paper we have learned a great deal about the steps needed to help secure your home network. We have gone through definitions of some highly used technical terms. Learned about hardware routers and what they can do for the home network. Understanding the software firewall and how it can be used in conjunction with its hardware firewall/router counterparts. You should have a

good understanding of anti-virus software and how it can better protect your system. The Microsoft update tool and its benefits have been explained. You have seen a test system configuration and test ran against it showing the benefits of securing your network. Over all you need to remember that no system is hack proof we can only use due diligence in putting up enough barriers to help keep intruders out. Saying that security is not my problem is what keeps infections like Nimda out in the wild. Security is everybody's responsibility so do your part. I always think of security as the club device that you can put on your cars steering wheel. Will it keep some one from stealing you car? No, but why should they try when the car parked next to yours does not have a club installed. Doing the basic parts of security, installing firewalls, anti-virus and Operating system updates is your club against hacker's virus's and other malicious code. Why should they hit your protected system when there are thousands yes thousands of vulnerable systems out there for the taking. Don't be scared be prepared!

References

1 Greenspan, Robyn “Broadband Future Is Bright “cyberatlas.internet 14, August 2002
URL:http://cyberatlas.internet.com/markets/broadband/article/0,,10099_1446801,00.html (08 Sept 2002)

2 Hummel, Robert L. “How It Works: Personal Firewalls.” PC WORLD: 05 June 2000.
URL:http://www.idg.net/crd_idgsearch_0.html?url=http://www.pcworld.com/resource/printable/article/0,aid,17012,00.asp (08 Sept.2002).

3 “NAT Basics” Homenethelp: 5 Feb 2001
URL: http://www.homenethelp.com/web/explain/about-NAT.asp (20 Aug 2002)

4 Wald, Michelle Von and Zuk, Nir “Firewalls Explained” Techtv 22 April 2002
URL:http://www.techtv.com/callforhelp/answerstips/story/0,24330,2436994,00.html (01 Aug 2002)

5 Denis Howe The Free On-line Dictionary of Computing:
URL: http://www.nightflight.com/foldoc-bin/foldoc.cgi?query=dhcp (05 Sept 2002)

6 “Linksys BEFSR41” Linksys:
URL: http://www.linksys.com/products/product.asp?grid=23&prid=20 (05 Sept 2002)

7 “Netgear RP114” Netgear:
URL: http://www.netgear.com/categories.asp?xrp=4&yrp=12 (05 Sept 2002)

8 “BlackICE PC Protection” Internet security systems:
URL :http://blackice.iss.net/product_pc_protection.php (05Sept 2002)

9 “Zone Alarm Pro” Smarter Security
URL: http://www.zonelabs.com/store/content/home.jsp (05 Sept 2002)

10 “Tiny Personal Firewall” Tiny Software:
URL:Http://www.tinysoftware.com/home/tiny2?s=1860533584552019034A0&la=EN&va=&pg=main (05 Sept 2002)

11 “Windows Update” Microsoft:
URL:http://www.microsoft.com/Windows2000/downloads/recommended/susclient/download.asp (05 Sept 2002)

12 “McAfee Anti-Virus” McAfee: URL: http://www.mcafee.com (05 Sept 2002)

13 “Norton Anti-Virus 2003” Symantec:
URL: http://www.symantec.com/nav/nav_9xnt (05 Sept 2002)

14 “PC-cillin 2002” Trend Micro:
URL: http://www.trendmicro.com/pc-cillin/products (05 Sept 2002)

15 “DSL Reports Port scan” DSL Reports:
URL: http://www.dslreports.com/scan (18 Sept 2002)

16 Gibson , Steve “ShieldsUP!!” Gibson Research Corporation:
URL: https://grc.com/x/ne.dll?bh0bkyd2 (18 Sept 2002)