Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

Frederick M. Heyn
GSEC Practical Assignment Version 1.2d

Batten Down the Net Hatches:
Making your 24x7 home access to the Internet as secure as possible.

Protecting your home PC or home network against the vandals of the Internet is not a task to be taken lightly. Like your home, you need to make sure that the security for your home computer systems has several layers. Rather than employing just one or two security measures you should actually employ as many as possible. If you really think about home protection, people usually do several things to ward off criminals. Steps generally taken for home security are the following: leaving lights on at the front and back doors at night, locking all windows and doors (some even take an extra measure and deadbolt the doors), installing motion detector lights on the back and sides of the house, putting indoor lights on timers, installing a home security system and last but not least, getting a dog. These are all things that should be implemented either as a whole or with some variation, but employing only one of these measures alone would be foolhardy.

If you implemented all these measures burglars would more than likely skip your house and move on to a more vulnerable and less protected target. It is this defense in depth approach that needs to be applied by those connecting to the Internet with a 24x7 DSL or Cable connection. Implementing a defense in depth requires several measures to be taken, for example, installing a router/firewall, installing an anti-virus, installing a personal firewall, employing good password practices and last but not least, performing backups. Implementing all these measures would increase your chances that would-be hackers pass you over for more open and vulnerable targets. Enforcing only one of these measures alone, as in home protection, would be foolhardy in the sense that you would have a false sense of security. While you might have covered one possibly security breach, you are leaving several other gaps wide open for exploitation.

The first piece of hardware you will get with your DSL or Cable Internet connection is the modem. One thing you should do is to find the manufacturer of the device and go to their web site and find out any information on the modem itself. If there are any patches for it make sure you download them and update your modem. Hackers are notorious for finding the security weaknesses of hardware and exploiting them. Try and stay on top of hardware updates as best as you can, check manufacturers sites periodically.

One hardware device you need to consider purchasing for a 24x7 Internet DSL/Cable connection is a DSL/Cable router. A router provides you with a first line of perimeter defense. Routers allow you to connect several systems on your home network to gain access to the Internet. Your DSL or Cable modem connection to the Internet is then attached to the DSL/Cable router and from there you can either connect to several machines directly from the router, depending on the number of ports the router has, or plug the router into a hub and distribute the Internet connection through it. All of the DSL/Cable routers I found on the Internet (Linksys BEFSR41, Netgear RT314 and Asante FR3004) provide numerous utilities to

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

make your 24x7 Internet connection safer and better to manage at a low cost. A DSL/Cable router costs anywhere from $90 to $175, with the cheaper routers generally having only one fast Ethernet port while the more expensive routers usually have four fast Ethernet ports. One model, the Asante FR3004LC, also includes a com port to connect to a modem as a backup when your broadband connection goes down as well as a parallel port for the router to act as a print server.

Every DSL/Cable router I found provided DHCP services that will allow you to assign up to 253-255 IP addresses automatically for your home network. The most important service provided by all of the DSL/Cable routers I found was network address translation (NAT). The basic purpose of NAT is to multiplex traffic from the internal network and present it to the Internet as if it was coming from a single computer having only one IP address. By providing a natural packet filter and router with NAT, the router is essentially acting as a firewall. Other configurations these DSL/Cable routers have include the ability to block internal users' access to the Internet, the ability to configure the router through your networked PC's web browser and some provide the ability of remote administration over the Internet.

After viewing all three of the above mentioned DSL/Cable routers, one stands above the rest, that's the Asante FR3004 series routers. While they all provide what every household needs for security of the home network on the Internet, the Asante router offers two extra security features that will benefit your defense in depth strategy. The first is the ability to log intrusion detection attempts. This will show you how much your Internet connection is being scanned, allowing connections on demand and logins & logouts. The ability to view that sort of information gives you a way in which you can keep track of attacks and possible exploits by hackers. Better to be informed of a possible break-in rather than be left in the dark thinking you're totally safe. The second feature that the Asante router has is the ability to open ports on-demand to accommodate popular applications, while the other routers have the ports always open. Having these popular ports open all the time only invites knowledgeable hackers to exploit the router firewall and gain access to your home network. Whatever router you get make sure you periodically go on-line and check and see if there's any new updates for your router. If you find that there is a new update make sure you employ it immediately. Hackers routinely find ways to take advantage of security holes in routers so manufacturers develop fixes for these security breaches and post the updates on their web sites.

Anti-virus programs have been around for quite some time and the majority of people who own computers have and use these important programs, Norton Anti-Virus or McAffee Virus Scan being the most popular. However, without proper maintenance of an anti-virus program you can find yourself in trouble fast. The world of computer viruses parallels the world of biological viruses in that they are constantly changing on a daily basis. Viruses are constantly being created and developed by Internet deviants to try and wreak havoc on a monumental worldwide scale. The first step to combat this threat is to make sure you scan for viruses on a regular basis. Anti-virus programs have an option so that you can have it scan for viruses automatically. Just scanning for viruses won't totally keep you protected though, you need to make sure your anti-virus definitions are as up to date as possible. You can do this by either allowing the anti-virus program to automatically update the signature definitions or you can go on-line and download and update the definitions manually.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The irony about viruses is that you, the owner(or user) of the computer, are more than likely the person who will allow a virus into your home network environment. The two ways for computer viruses to infect your home systems are by sneaker net and through e-mail attachments. Sneaker net is when you bring home virus tainted floppies, zip disks and burned CDs from work or school and don't scan them before you use them. The next virus threat is e-mail attachments. Attachments sent by anyone, either known or unknown, should all be suspected of being contaminated with viruses. I know this sounds drastic but the "ILOVEYOU" virus was spread by using the infected systems own e-mail contact list of friends and associates. Once the virus infected the system it would then send out the infected document to others on the e-mail list. Moral of the story is to trust no one.

Once you receive a document through e-mail, detach it immediately. Do not launch(open) it. Save it to a directory and then scan it. You also want to make sure your virus definitions are the most recent. If you hear about a virus spreading across the Internet you should immediately go on-line and get the latest virus definitions. Make sure the virus definitions include a fix for the virus you have heard about, if it doesn't wait for the manufacturer of your anti-virus program to come out with one. It is worth it to wait, and they usually come out with a fix the same day a virus is reported. Protecting your home PC network will require all those in your household who use it to practice these measures. If you have kids in school you especially need to ingrain these security practices against anti-viruses into their heads. Mimicking the spread of biological viruses in the real world, schools are the one of the biggest breading grounds for computer viruses.

Personal firewall software turns your home system into a low-end firewall. Sure it takes up hard drive space and memory on your system but the added security is necessary. I found two free personal firewall packages Zone Alarm v2.1.44 from Zone Labs and Freedom v2.0 from Freedom.net. They both provide a firewall and a wealth of other free security features. For a price tag of $40 to $50 you can upgrade those programs and add even more advanced security features. Two other popular firewall programs in the same price range include McAfee Firewall and Norton Personal Firewall. I found that not all offer the exact same features so you must view each one and pick the one that meets your security needs. You might find that you need more than just one personal firewall program, which is fine since more than one program will only add to your defense in depth.

Rather than go through and tell the slight differences of each program I will list some of the important security options that they offer. Other than the obvious firewall feature, the security options are as follows: AutoBlock of malicious systems that scan your computer, Form Filler to speed up online registrations and transactions, Cookie Manager to help prevent sites from tracking your activities, Keyword Alert prevents personal information from leaving your computer and Alert logging feature to log and report all attempts to access your computer from the internet. Whichever one you choose, make sure you keep the software up to date.

When you're in the confines of your own home, I'm sure you think that password protection doesn't apply to your home computer security. Guess what, it does! The use of passwords on important documents, databases and programs gives you added security in case someone has actually gotten through your home Internet firewalls. It's also a good practice just

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

in case your home is broken into and your PC is stolen or if your laptop is lost or stolen. This doesn't mean that someone won't be able to crack your password once they have your PC in their possession, but if you employ an intensive password naming convention it will dramatically increase your odds that they won't, or at least lose interest in trying. A good secure password should contain more than 8 characters, use upper and lower case letters, include several numbers and non-alphanumeric characters. Some non-alphanumeric characters are the following: ~, !,@, #, $, %, ^, &, *, (,), _, and +, just to name a few. Employing these measures as well as not using traditional words found in the dictionary will help to better secure your passwords. It's not a guarantee but it is yet another hurdle in your defense in depth security for anyone trying to break in and find out your private information to misuse.

For those that have file and print sharing enabled on your home networked systems, make sure you enable that function for only a folder you want to share rather than the whole hard drive. That way if someone does break into your home network the initial damage can remain a minimum. Along with a good password naming convention you should employ the practice of changing your passwords on a regular basis. Changing them every three months is a good practice, that's what large networked businesses usually employ, but some might think this to be too much for home security. If you do anything, make sure you change them at least once or even twice a year. Keeping it the same forever only allows the possibility of someone accessing your information to increase, because given enough time and accessibility, they will eventually be able to crack your password.

Another security option to employ is the use of file encryption software. The software cost ranges anywhere from $20-$60. CenturionSoft Steganos Security Suite, Network Associates PGP Personal Privacy and Panda Software Panda Security are just a few of the software packages that provide software encryption. Encryption is yet another tool to use to thwart hackers who've broken into your home network or thieves if your computer is lost or stolen.

The final aspect of defense in depth for home security I am going to cover is backups. Backing up your system's operating system and data files is the most important security measure you can take. Think of backups like an insurance policy. If you go out and buy a new car with safety and security options like anti-lock brakes, airbags and an anti-theft device you wouldn't then take it out on the road without an insurance policy covering it. If you did, just one accident could put a major dent in your pocketbook. You want to make sure that if you somehow damage or lose your investment, you can then either restore it so that it's as good as new or replace it. Backups, like insurance, help to make sure that unplanned incidents like a hard drive crash or a virus infection make the overall damage more bearable. When I speak of damage in these types of computer events I am ultimately talking about time and effort it took create the data lost or install and configure the lost operating system.

Having to re-install an operating system can take hours. Just installing the operating system usually isn't the end of the process. You then usually need to configure and tweak device drivers of the hardware you have in order to make the operating system run properly. This process can take even longer than installing the operating system because you might have to go out to the Internet and search for the proper device drivers and download them. Sometimes the

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

device drivers you install do more harm than good, causing you to have to go back to ground zero. How do you go about making this process smooth and easy? The answer is a program from Symantec called Ghost. Basically you use this program by copying an image of your hard drive or partition to another source, be it another local hard drive, CD-Rom or network drive. The imaging process usually takes no more than 20 minutes, depending on how much data you have on the system.

One important time to use this program is when you first purchase or build your system and get the operating system running on it for the first time. If something goes wrong with the system you will always have a recovery image to get back to square one. If you are building a system and make an image before installing software or drivers you're not sure of, you can always get back within a few minutes rather than starting from ground zero by rebuilding the operating system. If you do this and get a final version before you start creating data, which will become dated rather quickly, make a final image and mark it appropriately. Catalog on paper, or electronically, and keep copies of all updates, drivers and software you installed after that point so that you will be able to update the image if you wanted to, or if you in fact had a catastrophic event. Ghost is compatible with Windows 95, 98, 2000 and Millennium Edition, support Microsoft PC file systems: FAT 16, FAT 32 and NTFS, supports Linux ext2 file system, creates images to CDR/RW drives, and clones from PC to PC using parallel, USB or network IP connections. Files can even be added to previously created images.

The current Ghost program, version 6.5, provides numerous useful utilities to help you protect your valuable PC system. It has a utility that creates bootable diskettes that can include drivers for network cards, CD drives, writeable CD drives, and USB ports. Another important utility is Ghost Explorer that allows you to search files on an image created by Ghost and even extract files from that image. Basically this is a very cheap and easy way to have a backup of your system. The GDisk utility provides command-line partitioning with more functionality than FDISK. While many people think they can keep their PC systems from viruses, hackers and other catastrophic events, they're only fooling themselves. As long as you have a computer system and depend on it, you will have at least some sort of PC catastrophic event in your life. To what degree of the damage depends on the measures you take to combat hackers, viruses and hardware failure. Backups ultimately save you from all types of catastrophic events, depending upon how often you perform them. While Ghost is a great software package to do this, you might also want to consider detachable media like Zip or tape backup drives. Once you've picked your backup solution make sure that you get into a good backup routine that you follow religiously. You can perform backups daily, weekly or monthly. Decide on what best fits your needs depending on how much your data changes, but at least make sure you create and execute a routine to perform the backups.

Defense in depth is a practice that needs to be implemented as long as you have a 24x7 presence on the Internet, and it must always be updated. Hackers are constantly finding new ways to break into computer network systems. Your home Internet security must evolve with the times. Just going out and buying a router along with installing anti-virus and personal firewall programs won't keep you safe for long. You must maintain and bring up to date all hardware and software with the most recent update patches. Also stay up with current information in regard to Internet security, you can do this either on-line or by subscribing to PC security based

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

magazine. Last but not least, backup your operating system as well as your data regularly. Backups are your insurance policy when catastrophic events strike. They might seem monotonous and take up your time, but better to be safe than sorry. If you don't employ a good backup scheme now it will only take one disastrous event to make you start. Don't wait for that to happen, be proactive! Backups are as important in security as firewalls and complex password naming conventions. Always keep your eyes open to expand your Internet security defenses, never become complacent with your home network security otherwise you'll have your very own "date that will live in infamy."

References

URL: http://grc.com/su-firewalls.htm (5/2/01)
URL: http://www.asante.com/product/routers/fncable-dsl.htm (5/2/01)
URL: http://www.asante.com/product/routers/fncable-dsl.pdf (5/2/01)
URL: http://techinfo.asante.com/pdfs/Internet/fr3004ugrf.pdf (5/2/01)
URL: http://www.linksys.com/products/product.asp?prid=20&grid=5 (5/2/01)
URL: ftp://ftp.linksys.com/datasheet/befsr41ds.pdf (5/2/01)
URL: ftp://ftp.linksys.com/pdf/befsr41ug.pdf (5/2/01)
URL: http://www.netgear.com/product_view.asp?xrp=4&yrp=12&zrp=55 (5/2/01)
URL: http://www.netgear.com/pdf_docs/RT314.PS.FINAL.pdf (5/2/01)
URL: http://www.symantec.com/nav/nav_9xnt/ (5/2/01)
URL: http://www.symantec.com/nav/nav_9xnt/features.html (5/2/01)
URL: http://mcafeestore.beyond.com/Product/0,1057,3-18-SN101924,00.html (5/2/01)
URL: http://mcafeestore.beyond.com/Product/0,1057,3-18-MM106410,00.html (5/2/01)
URL: http://www.symantec.com/sabu/nis/npf/ (5/2/01)
URL: http://www.symantec.com/sabu/nis/npf/features.html (5/2/01)
URL: http://www.freedom.net/info/index.html?Session=da21e2cd2810fa41832676fc214f1eaf (5/2/01)
URL: http://www.zonealarm.com/products/za/moreinfo.html (5/2/01)
URL: http://www.symantec.com/sabu/ghost/ghost_personal/ (5/2/01)
URL: http://www.symantec.com/sabu/ghost/ghost_personal/features.html (5/2/01)
URL: http://www.centurionsoft.com/Steganos%203/index.htm (5/2/01)
URL: http://www.mcafee-at-home.com/products/pgp-personal-privacy/default.asp (5/2/01)
URL: http://www.pandasecurity.com/desktopsecurityinfo.htm (5/2/01)
Yeo, Lisa. "SOHO Security Best Practices". February 29, 2000. URL: http://www.sans.org/infosecFAQ/homeoffice/SOHO.htm (5/2/01)

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.