Global Information Assurance Certification Paper

COMPUTER SECURITY ESSENTIALS FOR THE HOMEFRONT

Michael J. Lukasz Assignment Version 1.3

Abstract

Much has been made of the everyday IT security threat of hackers, viruses and data pirating. The intrusions and subsequent destruction of data, downtime and lost capability translates into Millions of dollars in lost revenue. Technology tries to keep pace with the bad guys and IT professionals scramble to stay on track in an effort to thwart the endless attempts to crash the system.

This is what some read about in their IT journals or see on TV. The computer security war seems to be going on somewhere else. But what about the small networks online in rural America? How about the home PC in the den? Are there vulnerabilities? Are there computer security risks and should there be basic precautions. This paper addresses the often over-looked importance of computer security at small-businesses and at home.

The cost of IT Security in today=s environment

The issue of whether or not to implement some form of IT security at work and at home is often not a matter of to do or not to do, but more at what expense. Large business=s and corporations are often caught up in the bottom line and would very much like to minimize costs and expenditures and maybe Atake the risk@. In today=s environment, this is hardly an option anymore. IT security as an operating expense is now a reality. Even the federal government recognizes this reality as seen in budget allocations in recent times. AThe White House last week submitted to Congress an emergency supplemental request for fiscal 2002 that includes more than $36 million for various homeland security information technology programs@[1]

But there is no funding for your home PC/LAN or none for the small-business. While funding of this nature is clearly set aside for corporate America and the crowned jewels of the business world, the little guy is left to fend for themselves. Is it really that big of an issue? Is there a security threat out there than can be of substance or magnitude that would attract the hacker to attempt to infiltrate microuser territory? You bet there is. The very essence of Alack of security@ is a big enough red flag to begin with. While large corporations are beefing up security to keep the bad guys out, they must also maintain their systems to allow their customers and users in. If the hacker can not gain direct access directly to their target, they will most certainly attempt to do so by gaining access to a microuser node and disguising themselves as a friendly customer while they are actually a hacker on the prowl. This sort of ploy was displayed recently in the investigations that followed the carnage of 9/11. Small airports across the country

[1]Federal Computer Week, Volume 16, Number 8, March 25, 2002, pg. 6

were shutdown when it was realized that they served as a huge security hole to major airline hubs. Terrorists could have used them to gain access to critical transportation hubs. Additionally, they were used to gain knowledge regarding the aviation industry, protocol and security standards.
Much in this way, a hacker could gain access to a microuser who works for a large corporation. Many people bring their work home and could very easily place critical information on their machine. In this next section, we will look at the vulnerabilities of a home computer.

HOME COMPUTER SECURITY ESSENTIALS

Just how much risk is associated with having a home PC? Is there any? Questions such as these can be answered by performing a Arisk assessment@ on your system. It not as simple as one might think. There are many things to consider and not just do you have an internet connection. The most common misconception I have heard is the comment, AI=m not hooked up to the internet, so I am safe from any kind of digital catastrophe.@ While the internet is a common method for the hacker to utilize to wreak havoc on systems, it is not the only Athreat@ to the integrity of critical data.

Assessing your vulnerability and course of action

The first thing one must do is make an educated assessment of the actual threats which exist to the home/small-business user. Many families have at least one home computer and many of them are attached to the internet in one form or another. Log on security is often lax and/or non-existent at home for the sake of convenience and many Afeel@ that they are safe in the confines of their home. So who wants to break into my computer? How about Little Johnny? Your teenage daughter's boyfriend?

AIntruders may not care about your identity. Often they want to gain control of your computer so they can use it to launch attacks on other computer systems. Having control of your computer gives them the ability to hide their true location as they launch attacks, often against high-profile computer systems such as government or financial systems. Even if you have a computer connected to the internet only to play the latest games or send email to friends and family, your computer may be a target.@[2]

So, we have determined that there is evil lurking out there somewhere in the digital darkness. But how can this be? You turn off your computer every night when you=re done surfing. You have Aparental locks@ on your current favorite version of a certain web browser. Shouldn't that be enough? The truth of the matter is no computer is really safe, but if you are aware of the vulnerabilities you can reduce the risk of intrusion.

---

[2]Home Network Security, CERT Coordination Center, http://www.cert.org/tech_tips/home_network.html, Section 1c

Performing a risk analysis

Many people believe that computer hackers live someplace else and that this sort of crime happens in 007 movies. This is simply not the case. The more computers that are out there, the bigger chance there is that one of them is in the hands of a criminal.

AUnfortunately, intruders are always discovering new vulnerabilities (informally called holes) to exploit computer software. The complexity of software makes it increasingly difficult to thoroughly test the security of computer systems.@[3]

While it is true that not being on the internet does not necessarily fully protect you from data integrity chaos, it is also true that being on the internet greatly increase your chance of being a digital victim. While technology has brought us high speed CPU=s and great new operating systems, it has brought us exciting new features for home and small business use. The down side is that this brave new world has also invited a host of risks and vulnerabilities. Now that we have identified the reality of potential risk, let=s pursue the concept of implementing a home/small-business security plan. Let=s keep in mind cost and effectiveness; after all- let=s not let the bad guy win. We will address the issue with a three-pronged defense mechanism: A firewall to protect us from external intrusion via the Internet, Viral Software to protect us from malicious code and a backup strategy to fall back on if all else fails.

1. PERSONAL FIREWALLS

Can I protect my home/small business PC in this hostile environment?

The answer is yes, to a certain extent. We have already taken the first step to a more secure personal computer by acknowledging that there is a risk and that there are credible reasons to address the home computer security issue.

One of the most dominant players in the whole big picture is the Awww@. The World Wide Web dot com has become as common as the 1-800 numbers. Instant access to business and it=s resource grew by leaps and bounds. But those web-servers are giant boxes in the basement of some 65-story building in downtown Chicago, right? Wrong. Web-serving host software is now commonly found on everyday PC=s right off the shelf: ADude, you=re getting a security hole!@ To make matters worse, some of these machines may even come with the web software pre-configured as active. Every time you fire up your PC, the whole world may be looking at you, and your entire file system!

Personal web sites have become extremely common. Many people choose to set them up

[3]Home Network Security, CERT Coordination Center, http://www.cert.org/tech_tips/home_network.html, Section 1d

intentionally not knowing the full ramifications of the security issues that come with it. What they also don=t realize is that many of these systems come with a personal firewall to compensate for the security holes that the personal website has created.

This is especially important to the small-business or home entrepreneur:

AThe moment you install a Web server at your site, you have opened a window into your local network that the entire Internet can peer through. Most visitors are content to window shop, but a few will try to peek at things you don=t intend for public consumption. Others, not content with looking without touching, will attempt to force the window open and crawl in. The results can range from the merely embarrassing, for instance the discovery one morning that your site=s home page has been replaced by an obscene parody, to the damaging, for example the theft of your entire database of customer information@[4]

So what do we do to protect ourselves from this seemingly unprotectable resource? As previously mentioned, the firewall is the answer. Large corporations and entities for years have used the concept of monitoring website hits and utilizing hard firewalls to allow access and deny access. New technology has provided the same in the image of the original firewall.

ATypes of firewalls allow the user to define access policies for inbound connections to the computers they are protecting. Many also provide the ability to control what services the protected computers are able to access on the internet. Most firewalls intended for home use come with pre-configured security policies from which the user chooses, and some allow the user to customize these policies for their specific needs.@[5]

The key here is that one must be fully aware of one=s own computer system and the capability it offers. If you don=t utilize your personal webserver, remove it! This is the best prevention of all. If you are utilizing it, configure your personal firewall to provide a measure of security.
The beauty of this approach is that it fits well into our home security paradigm of low/no cost. In this instance, knowledge is the resource. While it is true that off the shelf system development moves so fast that it is hard to keep up with the technological advances of new operating systems, it is also true that not knowing the capabilities and security holes that new capabilities may bring may be digitally fatal. A small investment can be made and piece of mind gained by taking the half-hour to go through the new operating system online tutorial rather than plugging in the machine and jumping right onto the on ramp of the internet superhighway.

---

[4]The World Wide Web Security FAQ, Section 3,Q1, http://www.w3.org/Security/Faq/www_security_faq.html

[5]Home Network Security, CERT Coordination Center, http://www.cert.org/tech_tips/home_network.html, Section III

AChances are, your Windows XP computer is connected to the Internet, and you have probably wondered how safe your computer and your personal information are ... Windows XP includes an Internet Connection firewall that you can turn on to protect your computer from malicious Internauts.@[6]
There are a few options as far as obtaining a personal firewall. One can purchase off the shelf software/freeware to address a specific need. However, one of the best features of Microsoft's latest attempt at an operating system is ICF. Internet Connection Firewall is a personal firewall system that serves as a defense mechanism between the internet and computer. When properly configures, ICF monitors and restricts all data information that flows to and from your local system.

ICF monitors communication activity that it comes in contact with. It then checks where the activity originates and where its intended destination is. ICF creates a table of all internet activity that the ICF-resident computer initiated there by creating a table of allowed traffic. Incoming traffic that is not a part of this table is considered "unsolicited" and not allowed to reach the ICF-resident computer.

The first thing you should do is enable this feature. As mentioned before, new systems do not always come configured with security in mind. They usually come set up to get the anxious user online as soon as possible. You can enable this feature by entering the "Control Panel" and then choosing "Network and Internet Connections". At this point, choose "Network Connections". A "Local Area Connection" icon should appear; select it and you will be able to view your status. Now, choose the pull down tab labeled "Properties" and then "Advanced"; at this point you can activate ICF by placing a check in the box "Protect my computer and Network by limiting or preventing access to this computer from the internet." Upon doing so, the "Settings" box should illuminate. You are now able to configure ICF to meet your specific needs.

At this point, you should be familiar with the services your machine provides. The most common services are FTP, TELNET, mail service and HTTP (www). To find this information if you are not familiar with it, go back to the "Local Area Connection" properties and click on the "General" tab. It will display types of services that may require protection. If you are using this machine for a FTP server, web server mail server or you allow remote access either through TELNET or Remote Desktop, then you should definitely add protection. Upon selecting the "Settings" tab, a list of possible services will appear. Choose the applicable services which require protection. Once this is accomplished, a pop up screen will appear asking you to enter name or IP address information. Do this for all the services that need protection.

The next thing you should do is enable logging. This allows the user to create a record of security activity which can be utilized to verify suspected hacks. You can configure the log to record

---

[6]The Complete Reference: Windows XP, Levine/Young, Network and Internet Security, pg. 802

successful connections and/or dropped packets. This will be helpful in identifying possible security breaches. The log will be very helpful as it identifies source of denied packets, date and time of occurrence and type of protocol.

To enable this feature, select the "Security Logging" tab. You will be asked to select "Options", file location for your log and the maximum size. Selecting successful connections will allow you to review good hits on your website or file service. This can be useful if you need to track this. The downside is you may create a rather large log file and too large of a logfile can be as dangerous as a hack itself! Allowing this file grow to a size as large as your hard drive will bring the system to its knees. Be sure to select a file size that is congruent to your security needs. Also, limiting your file size will stop "Denial of Service" attacks by disallowing an infinite amount of "hits" to your system. Lastly, select the filename; this will be useful when it comes time to review it. To accomplish this task, select the "Browse" tab and a list of files will appear. Double-click on your log file and the data will be displayed.

The last step in the process is to configure ICMP properties and how the firewall reacts to different instances. ICMP is Internet Control Message Protocol; it is a part of the IP standard that allows hosts and routers to relay the status of communications including errors, control and status information. An example of this would be when you send a "ping" to a host on the internet
and the host is "unreachable"; you will get a message back indicating this. Choosing these parameters will allow you to modify how the firewall reacts to ICMP datagrams. For example, if you have "Allowing Incoming echo requests" disabled, the machine will not respond to "ping" requests. This can be a good thing, or it cab be a bad thing. A hacker can launch a "denial of service" attack by utilizing ICMP, by leaving these parameters inactive you are less vulnerable to such attempts. On the other hand, the "ping" utility can be used for more peaceful uses such as checking network connectivity.

The bottom line is you must decide how much protection you actually need and from what. You must be sure about which services need protection and if you even need particular services activated. If you don't need to have a service, say like TELNET, active then you should remove it from your list of active services!

So, you're one of these renegade LINUX users and WINDOWS XP means nothing to you? You still have alternatives that can provide you with a measure of ICF-like security.

TCP Wrappers is a freeware program written to protect internet services much like ICF. One of the main differences is that it is a multi-platform as far as UNIX is concern. It will support HP-UX, SUN Solaris and the ever popular, ever growing LINUX platform. While TCP Wrappers is not actually a "personal firewall" it functions much the same way; it queries incoming users of localhost FTP, TELNET, RLOGIN, FINGER and other tcp/ip services and checks to see if they are authorized users.

"The package provides tiny daemon wrapper programs that can be installed without any changes to existing software or to existing configuration files. The wrappers report the name of the client

host and of the requested service; the wrappers do not exchange information with the client or server application, and impose no overhead on the actual conversation between the client and server application."[7]

That's the upside: a relatively simple architecture that protects your services from misuse. The downside is that the configuration is not nearly as user friendly as the Windows XP ICF. You must have a certain amount of system administrator savvy to install this. In addition, the host table is not automatically updated like ICF; you must manually initiate and update the tables to allow or disallow users or subnets.

You must also manually replace the service executable with the "wrappers" and then manually configure your /etc/inetd.conf. The "tcp" wrapper is loaded into the /etc directory and every time an outside source attempts to use a service on your system it is queried by the "tcp" wrapper. If the source is not correlated with the "hosts.allow" file, access is rejected. In addition, if it matched with an IP or hostname identified in the "hosts.disallow" file, access is rejected. TCP Wrappers does generate a logfile, but the overall capability and performance is not anything close to ICF. The upside is that it is "freeware" and it does offer some measure of service protection.

2. ANTI-VIRUS DETECTION

So we've installed a firewall and we're done, right? Wrong. There are a couple of other high profile issues that must be covered as well. Besides, I need a few more pages to satisfy the requirements for this course. So what else is out there? We have addressed the www issue with the firewall, how else are you vulnerable?

Probably the most prolific security medium weapon known to even the novice hacker has to be e-mail. E-mail is everywhere. At home, work, at the airport, on pagers- everywhere. It has become as common a mode of communication as the telephone. But what can be done with e-mail that makes it such a threat and how can I protect myself.

It=s not so much that e-mail is the problem, but what can come with it. Much in the way a bomb can come in a letter or package.

AOne of the less appealing aspects of the Internet has been security and the potential for becoming the victim of a virus: a program that reproduces by infecting- or copying itself into other files or computers. Some viruses and worms are just annoying, but others are destructive, deleting or altering files or clogging up e-mail systems...@[8]

To address this issue we must purchase and install anti-viral software and effectively maintain

7 ftp://ftp.porcupine.org/pub/security/tcp_wrappers_7.6.BLURB

[8]The Complete Reference: Windows XP, Levine/Young, Network and Internet Security, pg. 802

and tune it in order that it remains useful. Anti-viral software can be configured to detect, remove, monitor and insure that a local or remote file system is free from infection. While this concept is not 100% guaranteed, it is very effective in detecting downloaded viruses before they attach themselves to your home or small-business machine.

This software must also be Amaintained@, that is, it will require updates from time to time to keep up with the new viral threats that are continually developed by the bad guys. Some of your more well known anti-viral software companies offer free updates, trial software and auto-update options to allow your system to virtually run automatically.

An excellent example of this product is McAfee VirusScan offered by Network Associates. This software is readily available online and can be downloaded to your machine, configured and running in a short period of time.

"McAfee.com provides online personal computer management products and services for consumers. Through its website, www.McAfee.com, the Company allows consumers to secure, repair, update and upgrade their PC's."[9]

By activating the "ActiveShield", the program will actively search for virus signatures in existing files, new files, e-mail attachments and peripheral device inputs. When a file is found to be infected, the software will clean and/or delete the file, notify the users or halt computer operations depending on the user settings.

The scan engine runs constantly, looking for malicious software and can also be run manually of from a command prompt for complete system sweeps. The scan engine works with a ".dat" file which is provided with the download. The dat file contains the latest known virus, worm and Trojan horse signatures. They and are used to compare with your data. If a match is found, the file is flagged and the software takes action. As you can see, it is very important to keep this file up to date. If you don't, you can be attacked by a new virus and your system could be damaged even though you took the time to install such software. McAfee VirusScan can be programmed to automatically download the latest dat files on a regular basis. This can help to keep your system up to date.

In addition to protecting your system, McAfee also provides support in the area of recovery. In the event that malicious code does slip through, instructions are available online to take the necessary steps to clean your hard drive. A logging feature is also available which shows important data, such as when the last time your system was checked, if viruses have been found and what was the course of action. This included dates and times which can be helpful when tracking the source of malicious code.

Specific information on how to download and install VirusScan can be found at http://www.mcafee.com/. The instructions are full featured and offer support for various system

9 http://dir.yahoo.com/Business_and_Economy/Business_to_Business/McAfee_com_Corporation "Web Directory"

platforms such as Windows 95, 98, Me, 2000 and XP. The website also offers a myriad of information regarding viruses, worms, droppers, bombs, Trojans and other forms of malware that users may need to be aware of.

This approach also fits into our paradigm of low-cost implementation for home and small-business use. Anti-viral use for personal and/or small-network use will probably cost less than $250; a small price to pay to avoid major loss of data and/or prolonged denial-of-service situation. Anti-viral software is a necessity now that e-mail, www downloading and just plain old internet connectivity is as common as the TV set in the family living room. There are many different versions and vendors that carry this sort of software at your local office supplier store or your favorite multi-media megastore.

III. SYSTEM BACKUPS

The most often overlooked action that anyone can take is the concept of the system and data backup. From the single-platform microuser to the veteran mainframe megasystem data administrator, many times formal and routine backups often fall to the wayside for other priorities or even forgotten and possibly non-existent!

When all other precautions fail, the up to date backup of your system and your data will provide you with system recovery. A system that has been hacked into and destroyed, or damaged beyond repair because of a virus or worm is still repairable with the help of a viable backup. If backups are old or do not exist, you are in big trouble.

AWhen an incident occurs (and it will occur in nearly every organization), recovery from the incident requires up-to-date backups and proven methods of restoring data. Some organizations make daily backups, but never verify the backups are actually working. Others construct backup policies and procedures, but do not create restoration policies and procedures. Such errors are often discovered after the hacker has entered systems and destroyed or otherwise ruined data.@[10]

The first step is to have a plan. You must determine what kind of medium you wish to use, what will be the mechanism for the backup and what will be the procedure for recovery in the event of catastrophic failure. Many operating systems used by today's home and/or small business owners actually have utility software built in to the system that will facilitate system and/or data backups in a full, partial and/or incremental format. They can also be setup to be done automatically during off-peak, low use hours so as to not interfere with the performance of the system.

ABacking up files is something you should do regularly, so it=s worth taking some extra time to

[10]SANS Institute Resources, The Twenty Most Critical Internet Security Vulnerabilities, Section G3, pg5-6. Http://www.sans.org/top20.htm

create backup up jobs for the files that are most important to you and to schedule them to run daily (or at least weekly).@[11]

Now that you have identified a plan and a process, either through your existing operating system utility of some other third-party software solution, you must now carry the plan out. The plan should be carefully administered and executed, leaving no margin for error. You should maintain a primary, secondary and tertiary backup to prevent latent loss of data; that is when you realize you lost a file- two weeks ago. If you don=t have a few sets of backups staggered out through some time sequence, you may never see that data again! It is also important to test your backups are working and valid from time to time. You should backup and attempt recover of some backup files to be sure that your plan, medium and hardware are all working. This is important because it will verify the full functionality of your plan if and when the need arises to fall back onto your backups. The last issue to consider regarding backups is one of physical security. Now that you have a set of full and /or incremental backups to help you recover from data disaster, you have also unwittingly created another security issue. While the backup set serves as an insurance policy against total data loss, it is also representative of all your data. Anyone who gains physical access to the set can take it and use it. Any confidential information like passwords, account information or important database information can be extracted from the backup set. It is important to properly safeguard the set just like any other valued information. AA second problem involving backups is insufficient physical protection of the backup medium. The backups contain the same sensitive information that is residing on the sever, and should be protected in the same manner@[12]

Take some physical steps to safeguard your backup set. Store them in a locked, secure cabinet. Consider placing them in a safety deposit box with other important valuables. If these are not cost efficient solution, at least but them in a spot not readily available to prying eyes like the top shelf of an obscure closet or the trunk of your car.

Many platforms come equipped with backup software included. Windows95 and beyond comes with a local backup feature which is relatively easy to use. Unfortunately, you must manually kick off some of these backups in order for them to occur! Because of this, it may be beneficial to use one that will automatically backup your system at predetermined times to make the process more efficient.

One such program that can be used in this manner is WindowsNT backup. Because WindowsNT supports “at” commands, which are scheduled actions, one can set up their system to perform automated backups.

---

[11]The Complete Reference: Windows XP, Backing Up Your Files with the Backup Utility, Levine/Young, pg. 215

[12]SANS Institute Resources, The Twenty Most Critical Internet Security Vulnerabilities, Section G3, pg. 6.

"The Windows NT Server 4.0 backup application, NTBACKUP, has two obvious advantages: it's included with Windows NT 4.0 (so it's free), and, as a bundled application, compatibility and reliability problems are less likely to occur. Balanced against these advantages are NTBACKUP's paucity of high-end features and limited options. If your LAN is relatively small, the LAN's architecture is simple, and your backup requirements are modest, NTBACKUP suffices. For single-server environments that use a simple tape-rotation method and have no need to backup workstations from the server, NTBACKUP is more than adequate."[13]

A tape drive is a good choice to go with for backups over other mediums because they are cheap, reusable and reliable. They are easy to change and can be cataloged to provide full, incremental and differential backups as your system requires. Try to find one that uses dat or 8mm tapes as they do not require any sort of preformatting. All you have to do is load the tape and away you go!

The program can be found under "Administration Tools" and is labeled "Backup". Click on "Backup" and you have started the Backup user interface. At this point, the available data on your system shows up under "Drives". Here you can select what you want backed up. When you have completed your selection you choose the "Backup" button and a backup menu appears. Now, you can select features such as tape name, type of backup and logging information. The log data can be very important, especially if you need to restore data at some time.

The "Restore" feature is every bit of important as the "Backup". There would be no purpose in backing up your data if the restore capability was not equal to the task. It is every bit as simple to use as the backup feature. To use it, you bring up the backup application as previously mentioned, only this time you select "Tapes" instead of "Drives". Here you will see a catalog of information that is contained on the tape. Simply select the data or data set you wish to have restored. The application will extract the data selected from the tape to its original location.

As mentioned before, you can use "at" commands on a WindowsNT system to automate your backup tasks. This feature comes with the WindowsNT resource toolkit which, if you don't have, you should get as it is essential if you are administering an NT Server. Click on your Resource Kit icon and find "Scheduler". A window will appear prompting you to choose a computer; pick the one with the tape drive, most likely your server. The, under "Edit", add your command line.
"BACKUP C:\data" and then use the radio buttons to indicate when you want the command to be invoked.

Once again, this concept is one that falls within the framework of being within the means of the small-business owner or even the home microuser. The main resource here will be your time and

---

[13] Using Windows NT Server 4, Special Edition, Roger Jennings, Installing File Backup Systems, pg. 288.

dedicated effort. You may choose to procure a tape drive or some third-party software utility to make the task more manageable, but your outlay here should not be more than $500. Most systems offer some sort of backup capability built into the actual operating system. The key to making this step work is one of practice and not necessarily one of expenditure. If you read this paper and decide that these are all good ideas but you only have time to do one of these in the immediate future, pick this one to be your choice.

Summary

We have now installed/configured a firewall on your system to limit the access to your system of unwanted users. Hopefully, we used the one that came with your operating system. What=s that you say? Your flavor of operating system does not offer such a capability. This is an awareness issue. A good tip here is to involve yourself in a website that offers information about security issues from your perspective.

AThe mission of NIST=s Computer Security Division is to improve information systems security by raising awareness of IT risks, vulnerabilities and protection requirements, particularly for new and emerging technologies.@[14]

This portion of the NIST website offers to user's insight on security issues and concern. Why should you use it? Because you have already have paid for it. It is offered by the federal government and includes important guidelines and information to users both large and small.

In addition to this site and/or sites like these, you should also acquire the resource of the software which you have purchased. Many, if not most, major operating system and application producers also offer websites that provide information regarding security risks and provide software hotfixes and patches to address these issues. When you legally purchase a copy of operating system or application software and you register your purchase properly, you are allowed to download patches and utilize the websites that offer information regarding security risks. Make it as point to use this resource. After all, you have already paid for it!

Addressing your webserver security is of paramount importance. This is where you will attract the most flies. Just the nature of having a site Aout there@ soliciting for hits makes the scenario inherently dangerous from an IT security perspective.

AMaking sure that what you publish on your web site can be relied on is a major and expensive problem. No one wants their customers misled of dismayed because their site has been hacked, defaced or spoofed- even from pages cached on another site@[15]

---

[14]Information Technology Laboratory, Computer Security Division, http://csrc.nist.gov/mission.html , pg. 1

[15]ITsecurity.com, http://www.itsecurity.com/tecsnews/apr2002/apr91.htm

Your personal firewall is your first line of defense against website hackers. Using this resource and configuring it properly will decrease your chances of a web attack and make your other cumulative security actions more effective.

AThe operating system itself is just a small contributor to your Web server=s security posture. If you (or your provider) don=t consider the full environment, then it doesn't=t matter which operating system you use- you can=t reasonably expect to maintain security.@[16]

Yes, your TOTAL security effort is essential. Install and configure your viral software to meet your needs. Be sure to find out what kind of online services they offer and add it to your Afavorites@ on your preferred web browser. Set your scan parameters and be sure to find out how to upgrade your protection files before the next ILOVEYOU virus scare, not after it has been proliferated and 2,000,000,000 users are trying to gain access to the same website and/or 1-800 numbers. This is a proactive approach to the problem rather than a reactive one. Those that find themselves simply reacting to website crashes, virus/worm attacks and data losses usually do so in an unorganized and inefficient manner: Plan for the worst; you won=t be disappointed.

Last but not least is the backup plan. Implement your plan carefully and be sure it works to meet your needs. Keep them safe and orderly so that when you need these to recover your system, and you will need to recover your system, they will be ready and valid.

Using this three step approach is a concept known as Adepth-in-defense@. The multi-tiered approach allows for several lines of defense which work together as a cohesive unit to protect your system. Maintaining then so that they function at their highest capability is your responsibility. It=s kind of like maintaining your checkbook: the more religious you are about keeping it up to date, the less likely you are of having a Amistake@- especially one that could have been avoided by proper security techniques.

These concepts which I have addressed in this paper have been specifically designed for the home user or small business administrator. They are low dollar, big bang concepts as they allow for great effectivety without putting a big hole in your wallet. The vulnerability is there and so is the threat. Answer it with an educated approach revolving around low-cost solutions and security awareness: the data you save could be your own.

[16]WEB TECHNOLOGIES, Jay Heiser, May 1998, pg. 40.

REFERENCES

2. Federal Computer Week, Volume 16, Number 8, March 25, 2002

3. Home Network Security, CERT Coordination Center, http://www.cert.org/tech_tips/home_network.html, Section 1c

4. The World Wide Web Security FAQ, Section 3,Q1, http://www.w3.org/Security/Faq/www_security_faq.html

5. The Complete Reference: Windows XP, Levine/Young, Network and Internet Security

2. TCPWrappers v7.6 BLURB (README), ftp://ftp.porcupine.org/pub/security/tcp_wrappers_7.6.BLURB

2. McAfee VirusScan Online, http://dir.yahoo.com/Business_and_Economy/Business_to_Business/NcAfee_com_Corporation

2. SANS Institute Resources, The Twenty Most Critical Internet Security Vulnerabilities http://www.sans.org/top20.htm

3. Using Windows NT Server 4, Special Edition, Roger Jennings, Installing File Backup Systems.

4. Information Technology Laboratory, Computer Security Division, http://csrc.nist.gov/mission.html

5. IT Security, http://www.itsecurity.com/tecsnews/apr2002/apr91.htm

6. WEB TECHNOLOGIES, Jay Heiser, May 1998, pg. 40.

Last Updated: July 24th, 2017

Upcoming Training

SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor