Global Information Assurance Certification Paper

Securing The Desktop

By Al Pelzer
January 4, 2004
GSEC Practical Assignment- Version 1.4b, Option 1

Abstract

Keeping the desktop safe and secure in a corporate environment is an endless task. The people who bring in the business and make the money must be able to utilize the information and remain productive. This means the IT Professional needs to keep the vital information flowing over the network to the people who make the decisions and keep the business running. The hackers are the people who want to interrupt the process for one reason or another and will go after the vulnerabilities that are available to them. If the opportunity to hack into a system presents itself, they will take it. These people know that there are a lot of unprotected systems out there and are just waiting to find and exploit them. Attackers go after known vulnerabilities in the hardware, software and the people using them. There are 7 areas that need to be addressed to keep the corporate desktop up and running and as productive as possible. The seven areas I will be reporting on are file sharing programs, patch management, popup stoppers, spy-ware, antivirus software, firewalls, and the most overlooked area, training.

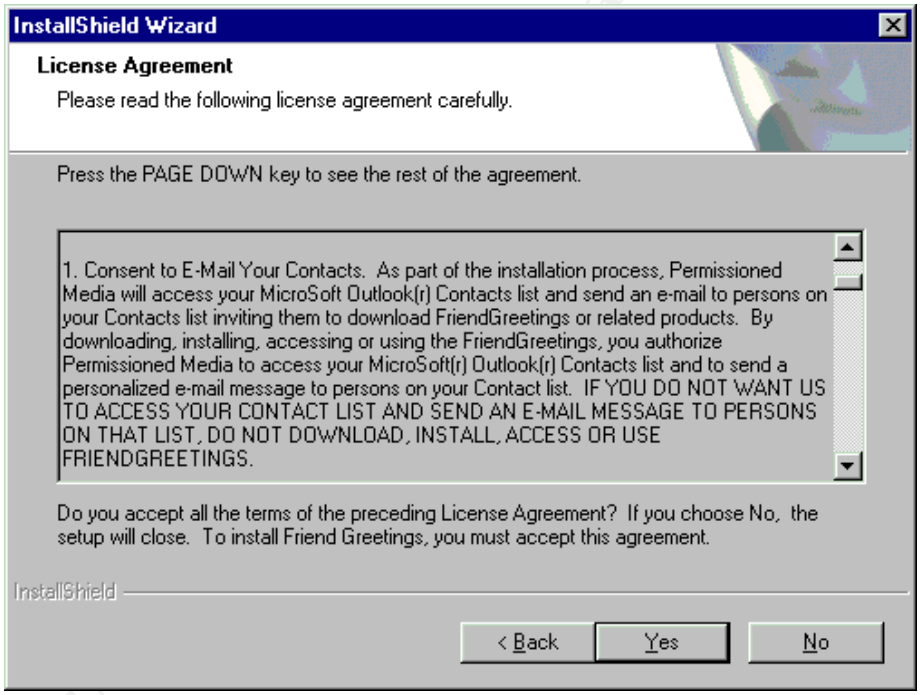
File Sharing Programs

Aimster, eDonkey 2000, Gnutella, Gnucleus, Grokster, KazaA, Limewire, and Morpheus you have probably heard of at least one of these PTP (Peer to Peer) file sharing programs. In fact you probably have one of them installed on your pc right now. Most of the previously mentioned file sharing applications run in the background and will start automatically without any user intervention or permission. Take a look in your system tray or check your running processes you may be very surprised. They have the capability of sharing a folder on your pc making your machine a file server for anyone on the same file-sharing network. Many free file sharing applications come bundled with “adware” or “spyware”, which may be automatically installed on your system along with the file sharing application. Your machine is acting like two servers every time you are online. One is providing the shared files for the community and one is reporting your surfing habits to the various tracking/marketing companies. This will not only slow your machine down but may also affect your network performance as well. These PTP file sharing programs will open up a hole in your network through the corporate firewall, and may be the hole in the armor the hacker has been looking for that will allow him to get inside your network. The majority of the PTP file sharing programs may install some kind of Adware or Spyware when you install the free version of the program. Most of the PTP file sharing networks provide a free version of their software, and as you know, there is nothing free in life. The

so-called “free” install comes bundled with Adware that may be used by marketing companies to track your Internet habits. This may be noted in the End User License Agreement (EULA), but I have yet to meet any person who has actually read the entire agreement.

The internet has allowed people to learn faster, explore and become more creative. The internet has also allowed hackers to get creative as well. People want to get their information for free and are willing to skip the EULA when installing free software from the web. This opens up a whole new way of distributing malware to the unprotected public using the internet.

I had a case at work where people were installing a greeting card program that would allow them to view e-cards sent from their friends. I found out that this program’s EULA stated that by clicking on “yes”, that you would allow the program to access your contacts list and send an e-mail to the contacts in your address book, as seen below. [1]



This is just one example of what is actually in some EULAs, so be aware when you fast click your way around. Try the “look twice, click once method”; it may take a moment longer but could end up saving you hours trying to uninstall these programs and all the registry entries that the add/remove programs applet will not remove. Explain this to your trainers and your end-users, and maybe they will prevent these programs from spreading.

[1] W32.friendgreet.worm

Napster really started the file swapping revolution, and it gave hackers a great idea. People are willing to download something after only verifying the name alone. This means that they can hide malicious software in normal files and people will voluntarily download it to their machines. What can be better than this; all they need to do is place some type of a remote access program on the unsuspecting user's machine and we now have a new file sharing network. I am seeing more and more trojan horse programs that allow a remote user access to your machine without your knowledge. They can then store files on your pc and tell all of their friends where the files are located to start swapping them from all the unsuspecting, unprotected machines. Not only is this affecting the performance of your machine, but think about what this could do to your corporate network if this was happening to a large percentage of your desktops.

A client contacted me recently and explained that their laptop had been operating very slowly lately. I took the machine to my desk and began exploring. I checked the basics: virus definition, patch level, and file sharing programs. The definitions were not up to date, the patches were not up to date, and there were two file sharing programs on the machine. In five minutes I found that four of the most important areas were not secure: antivirus, patches, file-sharing, and training. The machine was more than a month behind with the virus definitions as well as the patch levels. There were two very popular file sharing programs installed. Both were starting up automatically, and sharing out two directories on the local drive. This could have been completely avoided if the user would have followed our policy of antivirus, patch management, and file-sharing programs. This person needed to be trained once again to follow our policies regarding these areas.

Patch Management

One of the biggest problems we have in IT is keeping up with the many patches that Microsoft publishes to close holes they have left open. On a small network you could just use sneaker net and update and test each machine individually. In a larger environment, that is just not an efficient way to distribute the updates. We all thought that being behind with the patches wasn't a big deal as long as the antivirus software was updated. Thanks to the Blaster virus we found out that wasn't the case.

We needed a way to push out the updates to our desktops without sacrificing the time and productivity of our users. You can use automatic updates if you want to automatically break the integration of the many different applications that you have wrapped into your organization's standard build. You and your team spent months working out the bugs that occurred during integration of the applications used in creating your standard desktop. Now you are going to take everyone out of the productivity game by pushing out Microsoft's update that will plug up a hole in the OS, while seamlessly breaking the integration of your standard core applications.

I may be a bit precautious about pushing out updates, but that is because I am on the team that creates the build, as well as a member of the team who pushes out the updates. I know both sides of this fence, and from experience I know that you can get away with many untested updates, but the one that gets away from you will be your biggest headache. We recently pushed out a "Critical Update" that changed the Userenv.dll for security purposes. We very quickly found out that it also prevented the users from receiving or updating their roaming profiles. The phone in the customer support center will ring off the hook and the next thing you know you will be answering to the CIO about why you pushed an untested patch to all the servers and all the desktops, bringing his network to a screeching halt. So err on the side of caution and test the update before you push the update.

Let us not forget the Standard Desktop Build that needs to be updated with all the latest patches, hot-fixes, and service packs. This is an ongoing task that needs to be done on a regular basis. You don't want non-secure desktops in your production environment, so make sure your team is consistent with checking patches and updating the Standard Build. We have worked long and hard to standardize the desktop environment. You should make sure that all machines that are being deployed have the latest fully patched version.

There are many products out there that will allow you to scan your network and look for vulnerabilities. Some of the most popular products are MBSA, Nmap, GFI LANguard, 5MegaPing, Nessus, Retina, Saint 5, and Security Analyzer 5.0. I have listed these programs strictly for information purposes only. I have not used them all but would like to say one thing that holds true to all of these products. If you are not relentlessly consistent in using these products to make adjustments to your network you are wasting your time and money. These products are only as good as the person or persons that are administering them. You need to be able to devote time to become proficient with them as well as the time that is needed to fix the issues that they uncover. We utilize ZENworks in our environment to push patches and updates, as well as applications. You need to know the product used in your environment so you will know what you can and can't do with it.

The biggest buzzword in the security arena is "Zero-Day" attacks.[2] These are attacks that occur when there are no fixes available for the vulnerability that has been exploited. This is a major problem that needs to be addressed going forward because even if all the areas in this paper have been secured, a network can be compromised. It is going to be interesting to see what will happen and what will be developed in the future to help with "Zero-Day" attacks.

Popup Stoppers

[2] Vijayan, Jaikumar, p.1.

All of us know and hate the advertisements that continuously clutter our browser window while surfing the Internet. These have been named popups because of the nature in which they are displayed in your browser window on top of whatever it is you are reading at the time. These have been labeled a nuisance and a big cause of productivity loss. We have implemented another program that will stop popup advertisements from doing their job. Sometimes you need to see these popup ads, and that can be configured from within the many programs that are out on the market today.

Our users asked us to find something to stop the annoying popup advertisements that plagued them every time they browsed the internet for information. We searched the web and found the best fit for our environment was Popup Stopper Professional. This quickly became a standard program in our build and most people love it. A few want it removed or disabled, but that is how it is with any new application that is introduced into the environment. It does make it easier to work, and you just need to press the Ctrl key if you want to view a popup that has been blocked. After all, some of the websites I review on a daily basis have pop-ups that I need to read.

You may be thinking as you read this that this is not a program that is helping to secure the desktop. My feeling is that anything that interferes with the availability of information is a security violation. If someone is doing research on the web and can't get the job done because of annoying popup advertisements, then that is when you need to deploy an application that will stop the popups from occurring. Just like antivirus software, there is a large amount of vendors making popup stopping software. A few of the products that I have looked into are Popup Stopper, Popup Killer, Popup Cop, and Popup Smasher. They all stop the advertisements and will allow your users to see the popup ads if they wish. It all depends on what you are looking for as far as the functionality and the ease with which you can manage the various settings. Most even have options to exclude certain websites from the blocking list that can be edited for your convenience.

Spy-Ware

According to Steve Gibson-Gibson Research Corporation, "Spyware is any software which employs a user's internet connection in the background without their knowledge or explicit permission."[3]

Spyware by definition is any software technology that can gather information about a user and his or her surfing habits and send this information to a third party that can be used for any purpose, good or bad, without the knowledge of the user. If you were to agree with Gibson's definition then programs that are installed **with** the user's knowledge and/or permission are not considered spyware, if the user fully understands what data is being collected and with

[3] Gibson, Steve

whom it is being shared. Whether it is spyware by definition or not, the problem with this type of programming is that it can have a direct effect on our users, as well as an effect on the call volume of your customer support desk. When spyware is installed on a desktop accidentally or intentionally, it can cause performance issues as well as reliability issues. It seems that every other website, or free downloaded software installs some sort of spyware in order to keep the website and software free to the Internet public. The companies that create this software always say that they don't send any personal information to the marketing companies. How are we supposed to know this? Maybe the program grabs your credit card number in a text file and emails it to the programmer. Nobody knows the impact these programs have on our lives. What I do know is that I have completely re-imaged many of my client's computers because of spyware that may have been the direct or indirect cause of instability.

Antivirus

Antivirus software is the "never use your pc without it" software, that may keep your machine free of all discovered malicious software also known as malware. According to the Symantec website, there has been 65,000 + reported versions of malicious code.[4] Remember, this is reported versions; don't forget about all the code that is still out there that has not been reported! I think this number is just a sign of what will be created in the future. The internet has become a necessity to all of us in either work or play and there are many talented people that want to exploit all of its vulnerabilities for fun and profit.

Antivirus has lulled our technology-based society into a sense of false confidence. Antivirus software is only as good as its last update and for a lot of people that is not very often. Thank the technology gods for automatic definition updates! Even armed with the most current definitions, a machine is still vulnerable to all of the new threats and exploits that are coming out on a daily basis. I monitor the antivirus websites and see many new viruses or variants of old viruses every day.

The last thing you want to do while protecting the corporate network is to bring down all of your desktops with the implementation of a bad virus definition. I have had to roll back definitions in the past because a certain definition would cause our desktops to function improperly. The definitions need to be pushed out to an assigned test group to make sure they function normally just as they did prior to pushing the new definition. If they function for two days, then you can push the newly tested definition to all of the desktops and servers on the LAN.

So, you see, you can never be completely protected at any time! You will always be vulnerable to the new code, or the variants of the old, until the virus definition writers come up with the next batch of antivirus updates. Do you want to be

[4] Symantec.com

responsible for the aggressive antivirus administrator who blindly allows the network to be updated with the untested virus definitions? I am the antivirus administrator in my office and we are always 1-2 days behind in the definitions because I refuse to cause more damage to my network or my desktops by pushing untested definitions.

There are many companies writing antivirus software for corporations and home users. Some of the more popular are Symantec, McAfee, Trend Micro, Panda, Sophos, and Grisoft. What is the biggest variable that makes one antivirus software better than the other antivirus software? The antivirus administrator, and the update policy that has been implemented. All of the protection in the world will not matter if the antivirus programs don't know what to look for. You must remain relatively aggressive with the updates to keep your end-users safe.

Firewalls

This is the most talked about security device on the network and a completely useless device unless the following five areas have been addressed: file sharing programs, patch management, popup stoppers, spyware, and antivirus software. What good is a firewall when a laptop user takes their machine home for a few weeks, connects to the internet with a cable modem directly connected to their laptop, and downloads songs from a file sharing network? Along with the songs, they now have a few different viruses. These will wreak havoc on your network Monday morning unless you have addressed the issues with all your users and have set up the desktops/laptops with standards that have the preventive measures necessary to keep the malicious programs out of your network.

The Blaster worm jumped into our network with a scenario like the one previously mentioned. A user took a laptop home, connected to the internet without the use of a firewall, and had a vulnerable pc that was not patched. He came into the office and plugged into the lan and his machine started to give out the Blaster worm to all machines in the area. Before we knew it we had a full scale panic and the Firewall admin had blocked the ports in question the previous day. "It's silly to build a 6-foot thick steel door when you live in a wooden house, but there are a lot of organizations out there buying expensive firewalls and neglecting the numerous other back-doors into their network."[5]

Who is watching your network perimeter, and do they know what they are looking for? How often are they examining the logs? Are they only allowing what is needed in and out or are they closing per incident? The corporate firewall, like all of the other network security areas, is only as good as the people working with it to protect your network. They need to know that all the file sharing programs open them up both ways on a given port allowing an attacker a way inside the network through one of the user's machines. If that user is a Power user on your network then the stranger who just took control of their machine is as well. The

[5] Curtin, Ranum, Drakos

next time you have a conversation with your Security administrator ask them if they know which port the most popular PTP file sharing programs use. You will most likely get a blank stare, or they will say that all ports are denied except what is explicitly allowed. Then the next time you go to the end users desk you can completely ignore Kazza and all the music that person has on their machine because there is no way it could be there.

Training

According to Rhonda Tamulonis, President of MBR Consulting, "Investments in firewalls, virus protection software, and power protection devices are important, but potentially wasted unless there is also investment in continuous employee training."[6]

All of the software, testing and new tools will not help you or your network remain safe unless you train the people who will be using your desktops and laptops. These users need to be instructed in methods of safe computing. They need to know what to look for when setting up a safe home network. They need to know what types of software could install various forms of malware. We need our users to be the first line of defense for the security of our networks. Our users need to be a part of the solution to eliminate these threats. We don't want them to be the source of the problem. They will only know this if we explain it to them in a way to bring them in as part of the team. We don't want to alienate them and make them feel that when they call with a possible problem that they will be reprimanded. They should be aware that we are here to help in the event of a security situation, and if they don't know what to do, they should call the Customer Support Center. If a user ignores a potential problem, it could cause the network to be infected with a form of malware, and then that user would be responsible for bringing that inside our environment. The desktop users may not be technical but they do know when their systems are not functioning properly. Listen to your users: they may be the early warning system you need to stop the spread of malware on the network. If you have properly trained the users in your environment you can stop a large percentage of incidents that originate from inside.

Conclusion

Confidentiality, Integrity, and Accessibility, also known as the CIA Triad,is the cornerstone of the security industry. Everything I have discussed must address one or more of these three principles. As IT Professionals we need to aggressively address these issues and come up with a security plan that will keep our users and our network up, running, and safe. This stems back to the root of IT Security; that we will be able to access the information when we need it, and where we need it to do our jobs in the best way we can. After all, that is what we are here for. We are the protectors of the information that drives the

[6] Tamulonis, Rhonda

business process. We need to embrace the technology and utilize the tools that are available to protect our networks, systems, and our users from the intruders lurking on the Internet. It is our responsibility as the security professionals to spread the word and teach the people how to utilize the enormous amount of information in a safe way.

Keeping security in mind while asking the questions, "who, what, where, when, why and how?",[7] you can really get a good idea of the issues that are involved when granting access to the information on your network. You as a Security Professional need to ask yourself the following questions when evaluating the security of your network and writing a security policy:

Who needs the information?
What is the information?
Where is the information?
When is the information needed?
Why is the information needed?
How is the information accessed?

It is the responsibility of every IT/Security Professional to educate the people we come in contact with about the many good and bad creations the Internet has given us. We need them to be aware of the tools we have that enable them to browse the Internet safely. The people need to understand that they are directly responsible for their computers and neglecting them could allow an attacker to disrupt millions of people and cause businesses to lose millions in time and revenue. After all, the network I am responsible for is directly connected to your network, and our network- The Internet.

It is the responsibility of every IT Security Professional to keep themselves up to date on all of the latest developments in the technology world. Whether on the good side or the bad side we all need to keep learning and growing to protect against the latest threats. Make sure as part of your daily routine that you browse the latest security websites. I have my favorites and go through them every morning as part of my routine. The only way I will be able to help the people on my network remain safe is to educate myself and keep on top of all the trends.

Benjamin Franklin was quoted as saying, "A little neglect may breed great mischief."[8] The one day that we neglect to do something to secure our networks may be the hackers lucky day. I wrote "Securing the Desktop" because as a new security professional I felt that there was too much emphasis on the outside in approach to securing the network and a lot of the problems actually began inside with the desktops. We need to secure the network from the inside out and only then will we be able to guarantee the Confidentiality, Integrity, and Availability of our systems and the vital information that flows through them.

[7] Tamulonis, Rhonda
[8] Franklin, Benjamin

List of References

"The SANS Top 20 Internet Security Vulnerabilities"
Version 4.0 October 8, 2003
HTTP://WWW.SANS.ORG/TOP20

NIU Customer Support Center. "FILE SHARING PROGRAMS SECRETLY USE YOUR BANDWIDTH" APRIL 2, 2003
HTTP://WWW.ITS.NIU.EDU/ITS/HELPDESK/BANDWIDTH/ALLP2P.SHTML

Symantec Security Response. "W32.FRIENDGREET.WORM" MARCH 17, 2003
http://securityresponse.symantec.com/avcenter/venc/data/friendgreetings.html

Curtin, Ranum, Drakos. " Internet Firewalls." December 1, 2000 Rev.10
http://www.interhack.net/pubs/fwfaq/#SECTION00033000000000000000

Franklin, Benjamin.
http://quotedb.com/quotes/452

Gibson, Steve. Gibson Research Corporation "What is Spyware?"
October 6, 2003
http://grc.com/optout.htm

Schwartz, John. "FILE SHARING OPENS NEW DOOR FOR HACKERS"
DECEMBER 8, 2003
http://www.iht.com/articles/120653.html

Stewart, James Michael. "My Top 10 Tips for Passing the CISSP Exam"
September 25, 2002
http://certcities.com/editorial/tips/story.asp?EditorialsID=21

Tamulonis, Rhonda. MBR Consulting. "Continuous Employee Training"
http://www.iisw.cerias.purdue.edu/business_industry/continuous_employee_training.php

Vijayan,Jaikumar. "USERS WORRY ABOUT "ZERO DAY" ATTACKS, TRY TO SECURE SYSTEMS" COMPUTER WORLD DECEMBER 15, 2003 VOL. 37 NO.50
http://www.computerworld.com/securitytopics/security/story/0,10801,88201,00.html

Last Updated: May 28th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event