Global Information Assurance Certification Paper

The Need for Multi-layered Defenses on the Personal PC

Joe Runnebaum
MCSE, MCP+I
November 28, 2000

In today's evolving information age, technical professions spend countless hours and dollars securing enterprise networks only to overlook basic security on personal PC's at home. The corporate security infrastructure often includes firewalls, intrusion detection solutions, vulnerability assessment utilities, and complex security policies enforced with the vigor of mid-evil swordplay. Conversely, most personal use home PC's barely have minimal virus protection let alone security measures to insure information confidentiality, data integrity, and data availability. These are the hallmarks for information security. Keeping data confidential to those who need it. Maintaining data integrity, assuring the data is the same today as it was yesterday. Keeping the data available.

This document outlines various safeguards, when implemented, can provide a level of assurance with regard to your data's confidentiality, integrity, and availability. Implementing a virus-scanning product to detect and safeguard against malicious software is essential in today's environment. As well as the implementation of a personal firewall product for any computer connected to the internet. Assessing your systems security and hardening it to withstand known vulnerability exploits is also key in personal system security. Protecting personal and confidential email through an encryption product is also recommended. Addressing the method of 'physically securing' your information through power on passwords will be discussed. This is not an all-inclusive guide to securing your personal computer against every attack that can be exploited. The purpose of this document is to raise awareness with regard personal information security and suggest common sense practices to increase personal data integrity and confidentiality.

Virus Protection –No Longer an Option, A Requirement

The past two years have seen the very best (or worst) virus activity to date. Initially the Melissa virus ran rampant through corporate email systems bringing many of them to their knees. System administrators scrambled to apply the latest virus signature files to their anti-virus engines. For months virus scanning companies touted there ability to detect and resolve with quickness Melissa and the few dozen variants she spawned. Little over a year later another little virus, 'I Love You', came along, the single most expensive computer virus in history. The need for virus protection is more evident than ever. However, virus protection solutions are often based on virus signatures. Virus signatures are definition files created after a virus is detected and profiled. Which means if a new virus is propagated before the signature is defined and published your anti-virus software will not protect your system against it. This alludes to the importance of updating your anti-virus software regularly. Installing virus protection software is only the first step in protecting yourself against malicious software. Regularly updating your software improves the current revision of the virus definition files that drive the virus protection product.

There are several well known virus protection products on the market today, McAfee VirusScan, Norton AntiVirus, and Dr. Solomon's AntiVirus to name a few. Features to look for in a virus protection product are the ability to constantly scan a system, looking for files containing malicious code, as well as performing a scan on system initialization (boot up). A matter of precaution would also be to scan any file downloaded from the internet or received through email. Be sure to register the product as soon after installation as possible to allow for the updating of virus definition files. Develop the habit of updating your software regularly.

Maintaining a virus scan product on the personal computer can no longer be considered an option it is a necessity. Striving to preserve your data's integrity, confidentiality, and availability are all reasons to implement and keep current a virus protection solution.

Personal firewalls- Keeping the Bad People out

With the advent of cable modems and DSL high-speed connectivity for the home, personal firewalls are becoming a mainstay for PC security. This technology is not limited to 'always on' internet connections, dial up connections to the internet could also benefit for the protection provided by a personal firewall product.

Personal firewalls are mostly software products that run on the host machine (the personal computer) connected to the internet. These products provide a barrier between the internet and anyone connected to it, and your computer. The main function these products supply is preventing an unauthorized individual from accessing your computer using facilities that would normally provide access. Most of the personal firewall products available offer an amount of configuration that is based on your need, or comfort level. The most common 'attack' against any system on the internet is a scan of available services and ports. If an attacker can find any open port or service on your computer with a known vulnerability, he or she can concentrate their efforts to compromise your system. Some well know viruses have been known to open ports on a system to facilitate communication between your computer and the attackers. This would allow the attacker to copy files, execute commands, and even utilize your computer to launch an attack on another system.

There are several personal firewall products available including BlackIce Defender by Network Ice, ZoneAlarm by Zone Labs, McAfee Personal Firewall, and Norton Personal Firewall 2001. The following is not an endorsement or recommendation of any kind, rather an opinion of the author on the product I utilize. The product I have the most experience with is BlackIce Defender by Network Ice. The product offers four different security settings based on the users criteria. BlackIce runs in the background and reports any events that occur. There is also a log file that contains records of any events that are triggered. When an event is triggered the system alerts the user and logs any activity. It also gathers as much information as is available from the attack source. This information includes IP address, DNS information, and attack type whether a scan or attempted exploit of a known vulnerability. As always register the software as early as possible and keep abreast of current updates. Utilizing a personal firewall for your computer that connects to the internet is a vital part of keeping your information confidential and preserving its integrity.

Assessing Your Systems Vulnerabilities

Given that the bad people are going to try to scan your system looking for exploits, we should examine our own system and plug whatever security holes exist. One of the most important aspects of system security is keeping up with current software revisions and patches. All too often people will purchase a computer, install the software that was provided and not give another thought to updating the system. The majority of systems purchased today run Microsoft operating systems. Microsoft has been very proactive in the dissemination of product updates. It is as simple as visiting their website and choosing the updates required for your system.

After applying the appropriate updates and fixes to your system you may want to test your system and look for any vulnerabilities that can be exploited. There are various websites that offer this as a service. I have difficulty asking anyone to scan my system for any reason. There are commercial products available that can scan across networks and log vulnerabilities and even recommend action to resolve the issue.

Keeping your system up to date with current versions of software and patches for known vulnerabilities

will assist you in keeping your data available when you need it. As well as protecting the integrity of the data as it resides on your system.

Encryption? What is it and why would I do it from home?

Encryption in the process of 'locking' a file or email message with a 'key' that you have provided the recipient to 'unlock' it with. Unfortunately what many people do not realize is that most email traverses the internet in clear text format. Which means that anyone who can capture the information as it travels to its destination can read the content with little effort.

Things as simple as vacation schedules, retirement fund information, and letters of credit are transmitted across the internet with no preventative measures taken to insure confidentiality. A vacation schedule could contain information relating to a house being vacant and open to robbery. Retirement fund information and letters of credit contain personal information including social security numbers, account balances, and even credit limitations. Do you think this information would be valuable to the wrong people?

The most common product available to protect information like this is PGP, Pretty Good Privacy by PGP Security. This is a free download available form http://web.mit.edu/network/pgp.html The product is a basic public/private key pair generator for the exchange of confidential encrypted information with confidence across the internet. A simplified overview of the process is as follows:

Install the software
Reboot the computer
Generate a key pair 1 private to your computer, 1 public to publish to key server
Advise friends and associated to download your key from the key server
Generate an email, encrypt and send
The recipient will decrypt with the public key and be able to read the message

Utilizing an encryption product will promote the confidentiality of the data contained in email you send through the internet.

Physically Securing Your Computer From Unauthorized Access

One often-overlooked area of personal information security is securing your computer in the event of theft or unauthorized access. Unauthorized access could be anyone accessing you computer without your permission or authority. This is not limited to strangers. Perhaps income information, fund information, or asset listings are things you intend to protect from everyone.

This can be accomplished through a number of basic settings on your computer. You can set a power on password in the system BIOS to require a password prior to completing the boot process. This will limit the availability of the information contained on your PC to people who either know the password, or are savvy enough to bypass this security measure. An added measure would be to disable the ability to boot from a floppy disk. This would prevent bypassing file system security if available on your system.

Another security measure that can be enacted is document security. This is the process of assigning a password to a document in order to access the file. This could be used to secure word documents and spreadsheets containing personal and confidential information. Caution should be used in not forgetting the password. While there are options should you forget a document password, these options are time consuming and can cost money.

Protecting your system from unauthorized access through these measures promote both confidentiality and the integrity of the data contained on your system.

Bringing it all together.

Personal computer security is often overlooked. In striving to bring a confident level of personal information assurance a layered approach is required. The approach should contain but is not limited to the following:

Virus protection: Protection from malicious software is paramount in defending the information contained on your personal computer. These solutions need updated on a regular basis to provide accurate and reliable protection.

Personal firewall: Providing a barrier between your computer and the internet is essential in providing a sound security solution for personal use.

Vulnerability Assessment: Examining your system for security exploits and applying fixes, as they are available is necessary in addressing personal computer security.

Encryption Solution: Providing secure confidential communication between yourself and others is essential in data integrity and assurance.

Physical Security: Protecting your system against unauthorized access through passwords and system settings, assists in the overall system security scheme.

While one of these measures will enhance the security of a personal computer system a combination of all will provide the best overall protection for your data. A multi-layered approach is utilized in corporate enterprises to secure data and maintain its integrity. The same standards can be scaled down and applied to personal computer systems as well. Finding what your level of comfort is with regard to data assurance will determine to what extent you implement these solutions. You may find that installing a virus protection package as well as a personal firewall solution provides you the security you require. Still others may not feel comfortable until they have implemented all measures mentioned, and more in some form or fashion. Whichever the case, a layered defense provides the best protection for your data's integrity, confidentiality, and availability.

References:

Grubbs, Linda L. "Safeguard Your System" PC World, May 12, 2000
http://www.pcworld.com/downloads/article.asp?aid=16691

Rigney, Steve "Pro Protection for Novices" PC Magazine, September 21, 2000
http://www.zdnet.com/pcmag/stories/reviews/0,6755,2630889,00.html

Bigelow, Steven J. "Practicing Safe Computing" ComputerUser.com, July 1, 1997
http://www.computeruser.com/magazine/national/1513/cadv1513.html

Bensimon, Michael "Review: Software Firewalls for Personal Protection" 8wire.com November 17, 2000
http://www.8wire.com/headlines/?AID=1384

Brandt, Andrew "For Your Eyes Only" PC World, March 30, 2000
http://www.pcworld.com/hereshow/article.asp?aid=15963&pg=1

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