Global Information Assurance Certification Paper

The Key to Internet Security Is Education

GIAC Security Essentials Certification (GSEC)
By Cindy James

Abstract

As Computer Security Specialists we are challenged to create a secure computer environment. This can be achieved by educating people of all backgrounds on computer security. In order to accomplish this task we will have to change the current opinions on computer security. We have to re-educate IT Professionals and then pass that knowledge on to the world of computer users.

A basic knowledge of computer security should be a required for all employees and college students. The curriculum requirements should include a review of the basic computer components and their interaction, together with a simple explanation of networking. The class should also cover the different types of computer attacks, and how to prevent them, and conclude with a guide of generally accepted computer etiquette.

The Perception

A basic change in how computer security is perceived in this country is necessary. There are warnings and alerts given everyday, but until people understand what they mean and how they can affect them and their computers these warnings will continue to fall on deaf ears.

I like many others was raised to look for the good in people and to overlook what minor infractions that they may commit. Computer Security requires us to look at life the other way around. We need to think in terms of worst-case scenarios concerning these issues without alienating the world in other matters. The first step is to overcome the social engineering in which we were raised to succeed in computer security.

Many people equate Computer Security with protecting our children on the Internet. Although this is a part of it, it is a very small portion. In the past few years several good sites have appeared to help parents and teachers of young children (see Appendix I). However we are ignoring a large portion of this country's population. It has become very apparent that a majority of adults have no conception of how a computer works, much less how to protect their computer systems from attacks.

How to make a Change

We need to find a way to educate all of our IT staff and users on safe computer practices: lessons they can use at work, school and home. Every student who graduates from our colleges is required to take classes in English, math and other basic courses. We need to incorporate into the curriculum a requirement a

section on Computer Security so students can learn good personal practices that they can carry forward into their new jobs and homes.

Currently in many states there are requirements in place for students who graduate from colleges and universities to have a basic knowledge in computer applications such as spreadsheets, databases and communication applications. In some states the requirements for computer competencies may include use of the World Wide Web and E-mail, but they seldom incorporate anything on basic skills of safe computing.[1]

Our government has admitted that there is a problem with computer security through the Homeland Security Agency.[2] They have set up a special fund called the Federal Cyber Service a Scholarship for Service or SFS.[3] This fund is designed to create computer security specialists for the government (Note: they must serve a 2-year term to pay back the scholarship). The downfall is that this scholarship is only available through 4-year colleges and universities.

Many businesses and schools have computer policies and guidelines that fall just a little short of covering who is responsible for computer security. All businesses should be encouraged to create clear, precise policies, to be presented to all employees and easily available anytime a question arises. These policies need to cover several topics, including what is acceptable use and what is not, password guidelines, and incident handling.

Many companies have required quarterly meetings or annual refresher classes to cover topics such as safety; drug and alcohol abuse, and discrimination of any kind is not tolerated. Why not also include a course on computer security?

What to Teach

A lecture on computer security, which of every employee, teacher or student should be required to be taken along with his or her computer applications competency. There are several different topics that should be covered.

- The basic components of a computer system and how they work together.
- Network fundamentals and how computers communicate with each other whether it is on a small network or on the Internet (the largest network in the world).
    - Wiring
    - Devices
    - Designs
    - Addressing

[1] "50 State's Certification Requirements." William E. Stilwell. February 11, 2003. 2-20-2003. <http://www.uky.edu/Education/TEP/usacert.html>

[2] "Using 21st Century Technology to Defend the Homeland." 2001-01-20. 12-11-2002. <http://www.whitehouse.gov/homeland/text/21st-technology.html>

[3] "Federal Cyber Service: Scholarship for Service (SFS)." 12-11-2002. <http://www.ehr.nsf.gov/due/programs/sfs/>

- Essential computer security principles
    - Viruses and Antivirus programs
    - Type of Attacks
    - Firewalls – both applications and physical
    - Intruders Detection Software (IDS)
    - Passwords
- Computer Etiquette

Computer Basics

Any lecture on computer security has to start at the beginning; people need to know how the different components work with each other to understand how someone might gain access to their computer. There is no need to go into great details, as you are not creating new programmers. The knowledge of how data is processed and stored along with how computers communicate will set the stage for security.

Networking fundamentals include not just physical components, but logical principles. Individuals should have knowledge of the purpose of the major components from the NIC (Network Interface Card) to the router. Once they have an idea of the components they can learn how they work together and how they communicate to each other. A discussion on the three-way handshake should include an explanation on Syn and Syn-Ack so a Syn Flood attack can be understood. Knowing how machines are supposed to work will empower them to protect the machines.

When talking about basic computer communications you must include a section on Network addressing and the different types of addresses. The Machine name, the Domain name, the Media Access Control (MAC) address and the Internet Protocol (IP) address and their differences should all be discussed. When teaching non-IT users we need to be cautious not to overwhelm them in this area. The average user really doesn't need to know how IP addresses are derived. Simply understanding that every machine on a network, the Internet or the World Wide Web has an address would be a good start.

Viruses

Essential computer security principles should involve (but not be limited to) information on Viruses. This section should cover the different types of viruses, how they work and how they propagate from computer to computer. Most importantly users need to know how to decrease their chances of getting a virus. And, finally what to do if a virus finds its way into their system.

People need to recognize that viruses come in different forms and affect different operating systems in a different manner. There needs to be an understanding that Trojan Horses, Worms and Viruses have different meanings and behaviors.

A computer virus is an executable code that produces a corrupting influence. "Some computer viruses are malicious, erasing files or locking up systems; others merely present a problem solely through the act of infecting other code. In either case, though, computer virus infections should not go untreated."[4]

- A Virus is a program that can reproduce itself by attaching to other programs. This would include Boot Sector Viruses, File Viruses and Macro Viruses.
    - A "Boot Sector Virus" can hide on a hard drive or floppy disk in either the program code that loads the OS or in the Master Boot Record.
    - A "File Virus" hides in an executable (.exe or .com) or within a document that contains a macro.
    - A "Macro" can be automatically executed when the document is loaded or by making a particularly keystroke. (Note: not all Macros are viruses, by definition: A macro is a series of Word commands and instructions that you group together as a single command to accomplish a task automatically. Instead of manually performing a series of time-consuming, repetitive actions in Word, you can create and run a single macro — in effect, a custom command — that accomplishes the task for you.)[5]
- A "Trojan Horse" on the other hand comes disguised as something other than what it truly is. It may appear as a game, screen saver or hidden inside another file. Trojan Horses usually have file extensions such as "exe," "vbs," "com," "bat," "pif," or "scr." Their goal is much more serious than a worm, such as collecting users' accounts and passwords or some more famous full Trojans like Back Orifice and Sub Seven that can take total control of a system.
- A "Worm" is just a self-replicating virus. They can be easily passed on in networks and across the Internet.

No discussion on viruses would be complete without talking about the blended threats and hoaxes. We need to make it clear that we are now seeing more viruses that are a combination or blended viruses. People also need to understand that viruses can be written to behave differently on different operating systems. The Nimda[6] virus from the fall of 2001 is a great example of this. This worm could be received in an email or by visiting a compromised Web server on the Internet. Nimda also created network shares on infected machines allowing access to the system. Although Macintosh machines could not be infected they could pass it on. Removal of this worm was possible, but the instructions varied based on the operating system.

---

[4] Theall, George A.. "Computer Virus Information." 12-27-2002. <http://open.jeffersonhospital.org/tju/dis/virus/>.
[5] Microsoft Office Word 2000 help definition
[6] Chien, Eric. "Symantec Security Response - W32.Nimda.A@mm." 9-18-2001. 12-28-2002. <http://securityresponse.symantec.com/avcenter/venc/data/pf/w32.nimda.a@mm.html>.

For many years people have been told not to open Email from people they don't know, but that is no longer sufficient advice. Some worms have recently replicated themselves by sending themselves to a number of addresses listed in the address book. Users need to be cautious of everything even if they know the person the file came from. In the past few years it has been a common practice to have hidden file extensions, or to use "time saving" features to preview or automatically open files. Users need to be careful on websites that they visit and running any commands or programs from people that they may not really know (a common trick in chat rooms).

Intrusion

Also in this area should be a discussion of Hackers or Black Hats and how they may try to gain control of computer systems: whether it is by creating a virus to infect a computer, hacking into the system to gain information or inserting files onto computer systems. Knowing that all systems look like a potential host to hackers is not enough; people need to know why such proper vigilance must be kept.

Some of the reasons hackers may want to control systems they don't own may include the thrill of gaining control of someone else's system. For others, it may be the "bragging" rights of what they have done. Still others are looking for information that they can then exploit (such as stealing customers or credit information). Finally, there are hackers who are out for the oldest reason of all, revenge. These threats can be both internal and external.

Each release of an operating systems has become more secure than the previous version. Since no operating system is perfect out of the box, users need to understand the importance of updating their systems with upgrades and patches. The holes in a particular operating system are well known (actually they are published on the Internet) and hackers are known to exploit these weaknesses.

Everyone needs to know that there are several different types of attacks that have diverse results. Although it sounds like a strange new language, people need to know how attacks are executed in order to make proper decisions for their protection.

- Buffer Overload: An attacker overwhelms a computer or device by sending it more information than the program can handle. Once overwhelmed, the machine becomes vulnerable to just about any code or instructions sent to it by an attacker.
- DoS (Denial of Service) attacks: Designed to make a system unavailable to legitimate users.
    - IP Spoof: Uses a fake Internet Protocol (IP) address to bypass security settings, which may bar access from the real address.

    - Ping of Death: The Internet Protocol (IP) defines the maximum size for a ping packet. However, some Ping programs can send packets that are larger than this size that can cause some systems to crash.
    - Syn Flood Attack: An attack where a client opens a connection with a server but does not complete it. If the servers queue fills up with partially open connections, no other genuine clients can connect.
- DDoS (Distributed Denial of Service) attacks: Uses a large number of machines to simultaneously send packets to a victim.
    - Bots or Robots is the term used to refer to the host machines used in this type of attack. Hackers will place a small program on multiple machines in order to launch an attack at the victim, which causes them to have a DoS attack. There have been reports of some of these hackers having hundreds, if not thousands, of bots under their control.

After your staff and users have an awareness of the different types of attacks, instruct them what they can do about them. This will empower them to help in the fight against the Black Hats.

Prevention

One of the most important lessons taught is how important it is to keep protection up to date. New viruses and security holes are released every day only to be exploited on the Internet. Every home user needs to know how to update his/hers operating system and the software applications; in a business environment the IT staff should handle these updates. Much of the recent SQL Slammer virus could have been avoided if users had applied a patch that Microsoft issued more than six months ago.[7]

Explain that there are two types of Firewalls; both can help protect you from invasion, and both of them require management. The decision on which one to get is normally a financial choice.

- Physical firewalls, which are a separate devices that are designed to protect a network of computers.
- Software firewall, which are applications installed on individual server or machines.

Firewalls use a set of "rules" to decide whether or not to allow a series of code to process. By default, they are normally set to deny all traffic from one machine to another, whether within a network or between a machine and the Internet. These "rules" will need tweaking or updating as time passes.

Two other topics that should also be covered are:

[7] VIJAYAN, JAIKUMAR. "Unprepared Firms Slammed - Computerworld." 2-3-03. 2-19-03. <http://www.computerworld.com/securitytopics/security/story/0,10801,78105,00.html?nas=FIN-78105>.

- Intrusion Detection Software (IDS) monitors the host machine on which it is loaded and will provide clues as to any attempted or successful attack. Thus armed with this information, it will enable the restoration of the system as well as an awareness of deficiencies in system's protection that will safe the guard against further, more damaging attacks.
- Passwords – A strong password policy is the good start to Computer Security.

Recently, many computer attacks have preyed upon weak or default passwords. A password should not be left as the default, easy to guess, blank or a simple dictionary term. Having the same password for every system or application will allow an attacker access to multiple systems once they have broken the first one. A strong password will have a combination of alphanumeric, a combination of upper and lower case letters and numbers and symbols. A strong password should have at least 8 characters, but remember that most systems also have a limit (for example: Windows 2000 will not accept more that 14)[8]. Users should avoid the use a single letter or the word "password" Neither one is secure. Passwords should also expire periodically. Passwords should never be written down or left near the computer system for others to witness.

Having a plan for recovery after an attack should be a requirement, but just having a plan is not enough. The plan needs to be put into place, and tested before an attack so adjustments can be made before it is too late. This plan should identify who is responsible for handling an incident and specifically what each person addressing the incident is responsible for handling.

Computer Etiquette

The final section that should be covered is Computer Etiquette. This area should reinforce the computer policies of the school or business and what some people may regard as simple common sense.

- If a user is using a system in a business environment they need to be reminded that it is intended for job related activities, not personal use.
- Everyone should be reminded that they should only use information and resources that they have been authorized for access.
- People should neither read over other people's shoulders nor should they read or browse through others data.
- They need to remember that resources cost money, CPU time, memory, and network bandwidth.
- Remember to log off their workstations when not in use.

This is a good place to talk about copyrights and licenses, explaining that making or having copies of any program (and not paying to HAVE those copies) is illegal.

[8] "244448 - Password Field Has a 14 Character Length Limitation When You Use Connection Manager." 10-10-2002. 12-20-2002. <http://support.microsoft.com/default.aspx?scid=kb;en-us;244448>.

Unless you are the owner of the computer system you should not download or install any program without permission.

Copyrights for software give credit to the original author or developer. Normally, licenses must be purchased for each machine on which the program is to be used. The exception to this is “freeware” or “shareware”

- Freeware is totally free forever and can be distributed or given to anyone.
- Shareware programs normally ask for a nominal fee or cannot to be used in a business environment. Shareware often asks that the user to register and may stop working after a time period.

Business users need to grasp the idea that any data files they have created do not belong to them but to their employer when developed while on the job. Many companies have their professional staff employees sign a non-disclosure agreement prior to their employment. This should include any electronic data to which they may have access.

Like the marketing ploys of PC manufactures that give demonstration or trial versions of antivirus software with the purchase of a new PC, new PC’s should also come with personal firewall application and Intrusion Detection Software (IDS) automatically installed on them.

More people and businesses are getting on the Internet with a high-speed connection than ever before. This has created a larger population to attack. Although there are a few Internet Service Providers (ISPs) that offer a firewall protection, this is limited and an additional fee is usually required that many choose to live without. We as consumers should be requiring this service. This may be equated with having your Hotmail account scanned for viruses before you ever open it. The largest problem with this is a false sense of security. Email filtering should only be used as another line of protection.

The Black Hats’ manipulation of social engineering is very successful in getting users to open emails, visit websites or open attachments that have embedded surprises. We simply have to look at some of the attacks of the past few years to see how they convey their messages. The old saying about curiosity and the cat comes to mind; people have a hard time ignoring a message from someone that they know that has interesting subject lines like “I Love You” or “Happy Christmas”.

Users need to know that everything they read might not be completely true. They should be cautious of Hoaxes and passing them on in error. A hoax can be just as troublesome as a real virus; the difference is that it relies upon people to pass it on instead of computers passing it on. Hoaxes may ask people to do anything from deleting a file (i.e. jdbgmgr.exe file hoax) or forwarding the email message to a number of their friends and family (i.e. M&M hoax).

Our society demands that we hold people accountable for their actions, but many assume that it applies to everyone but himself or herself. This leaves the question of computer ethics in the hands of the computer users. Leaving the teaching of ethics to college or business may be late considering the case of the 12 year old in Florida who used his teacher's access to switch his grades.[9] The teaching has to begin somewhere.

Conclusion

We can change how people perceive Computer Security by teaching them what it truly means. Every school needs to develop a lecture concerning computer security that every student is required to take it along with his or her computer competency coursework. Schools should also offer a one-day course or section for their staff and teachers. Businesses will also need to make the time to retrain their staff. These classes should include regularly reviewing Information Security Policies and conducting computer security awareness training for all computer users. Once people become aware of how computers work, they will then comprehend the vulnerabilities in their systems. Armed with this knowledge people will put into place safeguards such as Antivirus and Intruder Detention Software. Requiring users to implement safe computer practices at work or school will follow them to home.

The bonus that may result from educating computer users will hopefully be more patience when there is a problem with a computer system. Understanding what the IT workers have to do and what they are going through to keep systems running may take the "bite" out of the calls to technical support desk.

We will create a more secure computer environment, which is what every Computer Security Specialist hopes to achieve.

[9] Shah, Nirvi. "PalmBeachPost.com: Sixth-grader charged in grade switch caper." The Palm Beach Post. 2-19-03. 2-19-03. <http://www.gopbi.com/partners/pbpost/epaper/editions/wednesday/martin_stlucie_e394fc8032005260000b.html>.

Appendix I
Sites for the protection of children on the Internet:

"Stay Safe Online | Home." 12-11-2002. <http://www.staysafeonline.info/index.adp>.

"Consumer Information Security - Federal Trade Commission." 12-7-2002. <http://www.ftc.gov/bcp/conline/edcams/infosecurity/>.

"Teaching the Teachers." Surette, Jo. 12-4-2002. <http://www.electronic-school.com/0398f1.html>.

"CyberCitizen." 12-11-2002. <http://www.cybercitizenship.org/index.html>.

Reference:

"National Infrastructure Protection Center (NIPC) - Home Page" 12-11-2002. <http://www.nipc.gov/>.

"Virginia Community College System Home Page." 12-17-2002. <http://www.vccs.edu/>.

"Computer/Technology Skills Curriculum - Grade 4 Go." 12-2-2002. <http://www.ncpublicschools.org/curriculum/computer.skills/4.html>.

"Berkeley Lab Computer Protection Program." 12-15-2002. <http://www.lbl.gov/ICSD/Security/>.

Anderson, Jared M. "Day Three: Copyrights and Software Piracy." 11-15-2002. <http://courses.cs.vt.edu/~cs3604/lib/Schools/Anderson/day3.html>.

Brenton, Chris with Cameron Hunt, Active Defense A Comprehensive Guide to Network Security, San Francisco, Sybex, 1999

Skoudis, Ed, Counter Hack, Upper Saddle River, N.J., Prentice Hall, 2002

Last Updated: January 21st, 2019

Upcoming Training

SANS Las Vegas 2019	Las Vegas, NV	Jan 28, 2019 - Feb 02, 2019	Live Event
SANS Security East 2019	New Orleans, LA	Feb 02, 2019 - Feb 09, 2019	Live Event
Security East 2019 - SEC401: Security Essentials Bootcamp Style	New Orleans, LA	Feb 04, 2019 - Feb 09, 2019	vLive
SANS Anaheim 2019	Anaheim, CA	Feb 11, 2019 - Feb 16, 2019	Live Event
SANS Northern VA Spring- Tysons 2019	Tysons, VA	Feb 11, 2019 - Feb 16, 2019	Live Event
SANS New York Metro Winter 2019	Jersey City, NJ	Feb 18, 2019 - Feb 23, 2019	Live Event
SANS Dallas 2019	Dallas, TX	Feb 18, 2019 - Feb 23, 2019	Live Event
SANS Secure Japan 2019	Tokyo, Japan	Feb 18, 2019 - Mar 02, 2019	Live Event
SANS Scottsdale 2019	Scottsdale, AZ	Feb 18, 2019 - Feb 23, 2019	Live Event
SANS Reno Tahoe 2019	Reno, NV	Feb 25, 2019 - Mar 02, 2019	Live Event
Open-Source Intelligence Summit & Training 2019	Alexandria, VA	Feb 25, 2019 - Mar 03, 2019	Live Event
Mentor Session @Work - SEC401	Raleigh, NC	Feb 27, 2019 - Mar 06, 2019	Mentor
SANS Baltimore Spring 2019	Baltimore, MD	Mar 02, 2019 - Mar 09, 2019	Live Event
Baltimore Spring 2019 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Mar 04, 2019 - Mar 09, 2019	vLive
Community SANS Indianapolis SEC401	Indianapolis, IN	Mar 04, 2019 - Mar 09, 2019	Community SANS
SANS Secure India 2019	Bangalore, India	Mar 04, 2019 - Mar 09, 2019	Live Event
SANS Secure Singapore 2019	Singapore, Singapore	Mar 11, 2019 - Mar 23, 2019	Live Event
SANS London March 2019	London, United Kingdom	Mar 11, 2019 - Mar 16, 2019	Live Event
SANS San Francisco Spring 2019	San Francisco, CA	Mar 11, 2019 - Mar 16, 2019	Live Event
SANS St. Louis 2019	St. Louis, MO	Mar 11, 2019 - Mar 16, 2019	Live Event
Mentor Session - SEC401	Fredericksburg, VA	Mar 12, 2019 - May 14, 2019	Mentor
SANS Secure Canberra 2019	Canberra, Australia	Mar 18, 2019 - Mar 23, 2019	Live Event
SANS Norfolk 2019	Norfolk, VA	Mar 18, 2019 - Mar 23, 2019	Live Event
SANS Munich March 2019	Munich, Germany	Mar 18, 2019 - Mar 23, 2019	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201903,	Mar 19, 2019 - Apr 25, 2019	vLive
SANS 2019 - SEC401: Security Essentials Bootcamp Style	Orlando, FL	Apr 01, 2019 - Apr 06, 2019	vLive
SANS 2019	Orlando, FL	Apr 01, 2019 - Apr 08, 2019	Live Event
Community SANS Raleigh SEC401	Raleigh, NC	Apr 01, 2019 - Apr 06, 2019	Community SANS
SANS London April 2019	London, United Kingdom	Apr 08, 2019 - Apr 13, 2019	Live Event
Blue Team Summit & Training 2019	Louisville, KY	Apr 11, 2019 - Apr 18, 2019	Live Event
SANS Riyadh April 2019	Riyadh, Kingdom Of Saudi Arabia	Apr 13, 2019 - Apr 18, 2019	Live Event