Craig Fosnock
E-mail: cfosnock@earthlink.net

Defense in Depth: The need to implement it at Home

Introduction:

Most home users make the mistake of thinking that they do not need to be concerned with computer security in their home. They're rational, is that there is nothing of importance on their computer, so who would want to take the time to "hack" or obtain unlawful access to it? The problem with this kind of thinking is that often the "hacker" (person who obtains unlawful access) has no interest in the personal data on your computer. Instead, they are after the computer itself. Once they have accessed your computer they can use it to launch attacks against other computers. Hackers have also been known for to take over home systems to use them to send spam. Just in case you have been living off the planet or in a cave, spam is defined as unsolicited e-mail, often of a commercial nature, sent indiscriminately to multiple mailing lists, individuals, or newsgroups; junk e-mail (1). Because the level of spam in recent times has reached unprecedented proportions, new legislation has been passed to punish spammers (those who send spam E-mails). This when a hacker compromises your system and uses it to do illegal acts, such as spamming anyone tracing the attack or spam E-mail will believe it came from you, not them. The attacker gets to remain anonymous, and you will get the blame, and possibly the legal fees.

Why Defense in Depth:

Most home users associate defense in-depth with large networks and the question needs to be asked why should they be concerned with it? In a nutshell all home users should be concerned with this because more homes are subscribing to broadband Internet service, and these new broadband services have a large amount of bandwidth dedicated to them. This bandwidth makes your system very valuable, and hackers are now constantly on the prowl for vulnerable computers in this arena. To elaborate the standard office normally has a T-1 line, which operates at 1.544 megabits per second (Mbps) a large office may use a T-3 line, which operates at 45 Mbps. Although not, guaranteed like the above services a single DSL or cable modem line can operate up to 1.544 Mbps. Just one compromised system will have enough bandwidth sufficient for spamming or to cause a Denial of Service (DoS) attack on a T-1 line, and when you add a few more “zombie” machines to the mix you can easily cause a Distributed Denial of Service (DDoS) attack even against even a T-3 line.

What makes the home market even more vulnerable, and is a greater cause for concern is that these types of services just like a corporate network can be connected to the Internet constantly. This includes digital subscriber lines (DSL). Although you may think that DSL is safer than a cable modem because you have to dial into the Internet, and it’s not part of a dedicate network. The truth is that by design both DSL and cable provide an always-on connection. This the “law of averages" goes into effect because a hacker has a virtually unlimited amount of time to work on breaking into a relatively insecure system, and “No matter how good any single network security application is, there is someone out there smarter than the people who designed it with more time on his hands than scruples who will eventually get past it. It is for this reason that common security practice suggests multiple lines of defense, or defense in depth" (2).

How a typical hack works:

The most dramatic way of getting access to a system is to exploit weaknesses in applications or in the underlying operating system. Although this can easily be done in the home environment because most people do not patch their systems, hackers in general will attempt to gain access by using the most direct means available. They will try to entice or trick unsuspecting users into opening E-mail attachments, which contain a Trojan virus. A Trojan horse is defined as a malicious, security-breaking program that is disguised as something benign (3). In other words the potential hacker tricks you into becoming an active participant in the hacking process by having you open an attachment that contains a backdoor. Hackers can then use the Trojan horse to plant or activate programs on your computer; they can even leave additional backdoors that allow them to get back into your computer if the original Trojan is discovered. I'm not sure if anyone remembers the famous "backdoor" from the movie Wargames, in that movie the programmer put in a backdoor to bypass any additional security that the DoD (Department of Defense) had added to his program. Matthew Broderick discovered this backdoor and used it to play "Global Thermonuclear War." In real life a backdoor or Trojan can be used in much the same way, once established it can be used to bypass all security applications or procedures that are in place or put in afterwards.

The Trojan Horse:

Just like the Greeks in the Iliad, the current batch of virus writers are quite devious. They can cause a virus to "spoof" or disguise the sending E-mail address so that it looks like it is coming from someone other than the computer that infected it. The most likely source it will "spoof" will be from someone you know and trust, and it will use wording that will intrigue you into opening the attached file which among other things may contain a Trojan. Two of the most infamous viruses using this technique are the "Love letter" and the "Anna Kournikova" viruses. This form of compromising a system is called "social engineering." Social engineering is defined as "attacking or penetrating a system by tricking or subverting operators or users, rather than by means of a technical attack. More generally, the use of fraud, spoofing, or other social or psychological measures to get legitimate users to break security policy "(4). Once you open the attachment and activate the code, the virus\Trojan will open a port, and either report back to the hacker or the hacker will scan across the Internet for this open port. Once the compromised system is found, the hacker will then connect on the above-mentioned open port. At this point he now "owns" the computer in question.

How Defense in depth protects against hacking:

In this article we will learn how to protect against hackers, and their associated malicious code using "defense in depth." Defense in depth is the proposition that multiple layers of security are better than a single protection mechanism. The layers may be technological, procedural, or policy (5). A hacker may develop a knack for breaking through certain types of security software, effectively rendering that type of defense useless, these hackers will eventually get past a single defense such as a personal firewall and compromise the computer. I’m sure everyone has heard all about the E-mail virus floating around the Internet with names like the infamous Beagle virus, which currently has more than 26 variations, for the purpose of this document we will use the threat of being compromised by a E-mail virus containing a Trojan horse to demonstrate how defense in depth mitigates if not out right stops this threat

Layer One:

In a business setting the first layer of defense is writing proper policy and procedures. Although for home users there are no formal policies in place, and there are no means to enforce even if there were, that is unless you want to count taking away your children’s allowance. You can still keep yourself informed and inform family members not to do harmful things. Some of the harmful things you can avoid are, not activating file and print sharing, downloading files from suspicions sites, using peer-to-peer networks such as Napster, and of course not opening E-mails from unknown people. Unfortunately as you know the E-mail with the virus containing the Trojan could be coming from someone you know and trust, so you will need to inform your family to read each message carefully before opening any attached files. They must look for bad grammar as viruses and worms writers are known to use poor grammar. Another thing to consider is whether the person in question would really have sent the E-mail or forwarded the attachment. If in doubt, contact that person in question to confirm they truly sent it

Layer Two:

To see the next layer of defense lets assume that your 6-year-old wanted to see “Big Bird” and opened the attachment. Now we can see the layer of protection that every computer cannot afford to be without, and that is anti-virus software, with updated pattern (database) files. The last part of the sentence “with updated pattern files” is important because a lot of home users do not bother to periodically update their pattern files, and an anti-virus program without updated pattern files is only marginally better than not having anti-virus at all. A pattern file is a small database that contains all the known virus strings, this if you forget to update it will not recognize any of the latest virus threats. Anyway Because you know this and constantly update your pattern files, once your six-year-old clicked on the attachment your anti-virus software would immediately give you a popup screen warning you of the infected file. It then should do one of three things:

1. Clean the file so it is not infected
2. Move the file to a safe location like a quarantine folder,
3. Delete it

Most anti-virus software will attempt to do all three in the order above, this if the virus cannot be cleaned, it will attempt to move it, if it cannot move it, the file will be deleted from the system. Because of the hazards posed by viruses there is no reason why you should not have some sort of anti-virus software on your system. You can even get free anti-virus software; to elaborate AVG Anti-Virus is available free-of-charge to home users for the life of the product. This product comes with rapid virus database (pattern files) updates, which are also available for the lifetime of the product. This is a decent product, and as long as you update the pattern file it will be an effective second line of defense for your system.

Layer Three:

Well for the sake of argument you did not know about AVG Anti-Virus, and your 30-day evaluation of the anti-virus that came with your computer ran out last year, or for the sake of argument lets say that you have followed all the rules but that this is a new Trojan and it is not detectable because no pattern file exists to detect it. This is where defense in depth really helps because you have installed a personal firewall. Firewalls are designed to restrict access based on various rules. A firewall can be hardware or software-based. Most hardware-based firewalls are stand-alone devices used to protect networks, while most software firewalls are designed just to protect the device that is running on. In the home environment most of the firewalls used are software based and called personal firewalls. These firewalls can be obtained for free from numerous vendors, with ZoneAlarm apparently the favorite. Although the free ones will have certain features turned off, it is still highly recommended that you obtain, and use a firewall product. For those of you unfamiliar with personal firewalls the firewall would protect you in two ways. The first one would be to issue a warning usually in the form of a popup that a program is attempting to access the Internet. This should be a clear warning sign especially if you do not even know the name of the program or have not attempted to run it. The second way it will help defend you is by blocking the hackers who maybe attempting to communicate with your system, this would include a hacker attempting to talk or scan for systems infected with a particular Trojan.

Layer Four:

Patch management is critical when dealing with defense in depth. Almost as fast as new viruses are discovered, new vulnerabilities are discovered as well. Many times they are in the underlying operating system, but vulnerabilities can also found in applications like your browser, E-mail software and other tools. Left unpatched, these vulnerabilities can be exploited by hackers to obtain access and control of your computer. Even more damaging there are now computer worms that once launched will automatically spread by exploit these vulnerabilities. These worms can infect thousands, if not millions of unpatched systems in a few hours or even a few minutes. Keeping your patches up to date can be difficult, but fortunately most vendors, have automated utilities that check for updates. Other vendors have an E-mail mailing list you can join so they can notify you of any new updates. As a last resort you can just periodically visit any of your vendor's support web site and check for any new patches or updates.

Additional Layers for Advanced Home Users:

For you diehards or computer literate people the following suggestions could also be used for even greater defense in depth. First I would recommend buying a small router designed for cable modem or DSL, even if you do not have multiple computers. This is because these routers also contain a firewall. Although these simple routers tend to restrict or direct traffic based simply on what port it is coming in on, and can easily be fooled, this is a good practice because it extends the outer boundary of protection. A personal firewall running on a PC gives the hacker access right up to your computer before it is stopped, while a DSL\Cable router would stop most traffic before it could touch your system.

The second thing I would recommend is some sort of Intrusion Detection systems or IDS. Although I will not discuss the technical details here there are two types of IDSs. One is host-based, and the other network-based. Although some really advanced users would have a dedicated system to use for this purpose, most home users would simply run a host based IDS, and it would be similar in nature to running a personal firewall. The IDS would add a different layer of protection because “IDS differs from a firewall in that a firewall looks out for intrusions in order to stop them from happening. The firewall limits the access between networks in order to prevent intrusion and does not signal an attack from inside the network. An IDS evaluates a suspected intrusion once it has taken place and signals an alarm”(6). In other words an IDS would notify you when unauthorized access has occurred.

Conclusion:

As a home computer user accessing the Internet, whether through a broadband connection or traditional dial-up, you should do the following things at a minimum to protect your computer:

1. Keep informed and keep your family informed about the latest threats on the Internet. Take extra precautions opening any attachments even if you know and trust the source.

2. Install and maintain anti-virus software. There are plenty of great anti-virus software packages available including those that are available for free. Regardless of what software you use it is important to consistently update the software's pattern files.
3. Install and maintain a Firewall. Once again there are plenty of free firewall packages available.
4. Keep your computer patched against known vulnerabilities, using the vendors' tools and mailing lists to stay current.

If you follow these guidelines, and establish defense in depth you will not only keep out unwanted traffic from all but the cleverest and most dedicated hackers, you will also protect your computer from known Trojans, worms and viruses.

Works Cited

1. URL: Yahoo.com (http://education.yahoo.com/reference/dictionary/entries/08/s0600850.html).

2. URL: Netsecurity.com (http://netsecurity.about.com/cs/generalsecurity/a/aa112103.htm).

3. URL: (http://foldoc.doc.ic.ac.uk/foldoc/foldoc.cgi?Trojan+horse).

4. URL: (http://sun.soci.niu.edu/~rslade/secgloss.htm#social%20engineering).

5. URL: Wikipedia.org (http://en.wikipedia.org/wiki/Defense_in_depth).

6. URL: Wikipedia.org (http://www.webopedia.com/TERM/i/intrusion_detection_system.html).

Michael Whitman, and Herbert Mattord. Principles of Information Security. Boston: Course Technology, 2003.