Global Information Assurance Certification Paper

HOW TO PROTECT YOUR NETWORK'S HOME BROADBAND USERS – AND YOURSELF

David A. Florea
SANS Security Essentials Practical
v. 1.4, Option 1

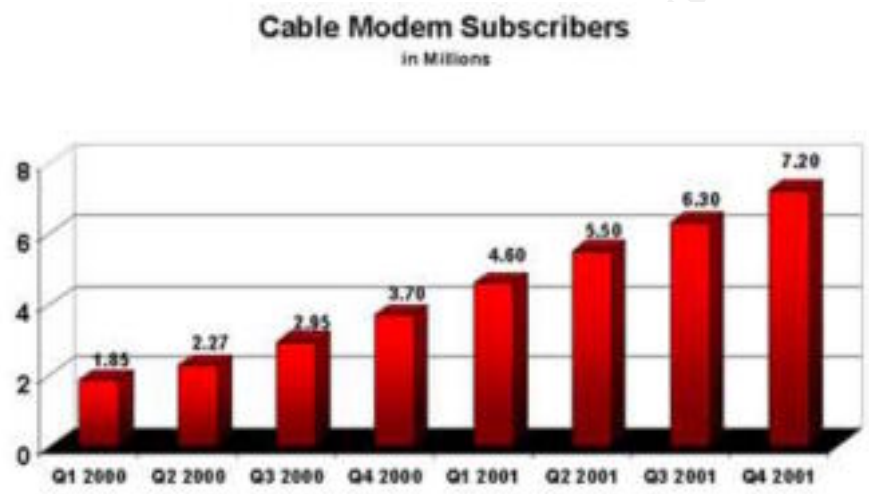
ABSTRACT:

While many of our organizational networks may be closely attended and reasonably secure, if your network allows home users to connect to the inside of your LAN at all, you as a network administrator must also be concerned whether their systems are also secure. This paper is focused on the best advice to give your broadband-enabled home users to ensure their own security, thereby increasing LAN security. I suggest to network admins that as a policy they create a document giving their home users the best advice they can around computing security; have the user acknowledge that they have read and understand it; and only then consider granting remote access privileges to the corporate network.

I'll also be giving some specific recommendations as to software and hardware in this paper, but those recommendations may be outdated in a matter of months. The more important message is that if we help our users to be secure in their home computing, we help ourselves as well.

As system administrators of one kind or another, we toil daily to keep our systems safe. We read the latest security bulletins; we patch our systems, buy the latest firewall technology, run intrusion detection applications, and lust after the latest and greatest bio-authentication systems. We agree all those things are important, and we further believe we have just about all we can do to keep our systems current and safe. And we're almost right.

One of the most fertile hunting grounds for hackers, crackers, and black hats in general is the current explosion of DSL and cable modem users. This requires us to do one more thing, that being to look at the state of our home users' security. Just as an example, look at the growth rate of only cable modem subscribers, as of the end of 2001:



(Courtesy, National Cable & Telecommunications Assoc., http://www.ncta.com/broadband/broadband.cfm?broadID=4)

DSL subscribers are growing even faster, that number growing almost 20% just in the first quarter of 2002[1]; and of course now satellite broadband is increasingly available.

We all know why the home broadband users are easy pickings for the bad guys: Always-on connections; the lack of security features in software defaults; the tremendous speed available to a hacker if he can command the user's machine; and more importantly, the inexperience of most home users.

This paper is dedicated to the potential weak link that often exists in our corporate security chain, the safety and integrity of our users at home. Those administrators who have no home users who access the organizational network are fortunate. Though whether we do or not, most of us are called upon by our

organization's employees to tell them how to fix a virus, how to keep the bad guys from reading their personal documents, and simply in general how to compute safely.

But worse possibilities exist for us as network administrators: This scenario is from one set up by Illena Armstrong in an editor's comment from SC Magazine, October 2000:

> *What about your network user Joe? Not only is he sitting at home with a very fast and easy-sign-on DSL connection thinking all this silly chatter about viruses is a bunch of bunk, he's also signing on to the corporate network from his humble abode. An enthusiast of online shopping, Joe bids for and wins those Red Sox tickets, sends in his check and never sees the tickets. What then? Maybe he files a complaint with eBay, or maybe he thinks, 'Ah, nothing will ever happen, I lost my cash but it's just a lesson learned.' Meanwhile, hackers somewhere not only have Joe's private details, they're knocking around in his always-on system right now, maybe even pinging his corporation's network for security holes.*

So, is it really none of our concern whether our employees practice 'safe computing' at home? I propose that we will get a reasonable return on our effort if we are in fact concerned, and make a good effort to get those employees up to speed on the bare foundation of computer security; for if those home users make mistakes, many of them will come to roost in our own networks.

There are five security areas that home users need our advice on, listed more or less in the order of importance:

ANTIVIRUS Software. System administrators know how silly it is to connect a computer in any manner to the internet without running a current antivirus application. Home users may not.

FIREWALLS and Intrusion Detection. Personal firewalls are very important, and especially for your broadband users. The good ones even handle many of the concerns around intrusion detection. Best of all, several of these can be had for free!

WIRELESS Networking. Wireless connections have exploded, as 802.11b devices give way to .11a, .11g, and other wireless protocols. The problem is, many wireless devices come natively with almost zero security features enabled.

ANTI-SPYWARE Applications. Privacy being a growing concern, I've chosen to tell my home users how to protect themselves against the increasingly obnoxious spyware bugs that attempt to log their internet

browsing. The better applications will also detect many Trojan applications.

Miscellaneous Advice. Disable file and printer sharing, but don't stop there: Encourage your users to be paranoid.

Antivirus – the most important thing

While network administrators know how basic and critical antivirus applications are, those who monitor their log files also know how terribly many machines out there have no such protection, or whose virus definitions haven't been updated anytime in the past year – often not updated since the personal computer was purchased.

Antivirus products are concern number one for all users, whether on broadband or dial-up services. But should you recommend a specific antivirus product to your users? My recommendation is to not concern yourself with the specific product as much as why and how to use it, and how to keep it updated. That being said, there are some current products that I recommend to my users without hesitation:

Norton (http://www.symantec.com/product/index_homecomp.html) has one of the best antivirus products today. PC Magazine noted, "*Of all the utilities we tell you about in this issue, antivirus software is the most important. And Norton AntiVirus remains the best choice***.**" (June 11, 2002). Their Live Update application makes it easy to keep current on virus definitions. Even better, Norton Internet Security 2002 (NIS) includes most of the tools suggested in this paper – antivirus, firewall, privacy protection, and (in the Professional Suite) intrusion detection.

Trend Antivirus from TrendMicro, thought not usually preinstalled on OEM machines, gets rated very highly in tech user groups. Their PC-cillin 2002 product also includes a personal firewall. http://www.trendmicro.com/pc-cillin/products/.

Panda Antivirus Titanium from Panda Software is another antivirus product (http://www.pandasoftware.com/titanium/discover_titanium/key_features.asp), which has received awards and favorable comments in the industry.

Often, your users will want to use whatever antivirus service came with their computer. So long as they have a current edition of their product and can figure out how to update the virus definitions, I recommend you let them use it. It's much more important that they use a product, than which product it may be.

For reasons we'll mention later, their AV product really should come with a plug-in that interfaces directly with their e-mail client.

Strongly encourage your home users to either schedule their virus definition updates to run automatically, if the product supports it, or set themselves a reminder to do so at least on a weekly basis. If their updates are more than a couple of weeks old, they will be in great danger of getting hit when the next "new and improved" virus hits.

Firewalls and Intrusion Detection – the only way to go for broadband

As noted above, the explosion of broadband availability has brought new, fertile ground to the 'black hats.' Even if an attacker can't find any worthwhile information on a users' PC, he may not care – his main motive may be to take control of that machine to be used along with hundreds of others in distributed attacks against other networks. (For an interesting account of a real-life distributed attack by "bots," see http://grc.com/dos/drdos.htm).

Tell your users they can count on it – if they're not using a firewall with their broadband connection, it's wide open and folks have – not 'may,' but have – in fact already been snooping around in there. Most estimates of how long an unprotected machine can be on the net before being compromised are under 24 hours.

There's some good news here, though; some very effective firewalls your Windows users can actually put up are free for home use. Three of the free firewalls I recommend without hesitation to my users are:

Tiny Firewall (http://www.tinysoftware.com/home/tiny2?s=8698768489789720373A4&pg=solo_download) Version 2 is free. They also have a paid-for version with perhaps a better interface, but the free version seems to work just fine.

Zone Alarm (http://www.zonealarm.com/store/content/home.jsp) They have a paid-for version as well which has some increased functionality around prevention of spyware, and cookie control.

Outpost by (http://www.agnitum.com/products/outpost/).

The main paid-for product I recommend to my users is **Norton's Internet Security 2002** (NIS, noted above under antivirus products), which also includes a firewall. The firewall component also has received high marks.[2]

All of these products require some setup work when they are first used, in order to 'guide' them to what one's computing habits are and what activities are normally safe. But that effort is well worthwhile, for if and when they do get an alert of an incoming connection, it is more likely to be a legitimate intrusion. A "reasonably" intelligent home user can do most of the configuration work required.

For most home users, I don't recommend trying to push them further into Intrusion Detection (ID) than where their 'default' software might take them. To do ID right is simply more than 98% of home users can manage, and will likely result in your answering user's questions like "I'm getting these weird alerts about some Orifice program, should I click OK or cancel?" Indeed, some recent tests indicate that even the high-end enterprise ID applications are far from effective.[3]

Wireless Networking – lousy security, unless…

The use of wireless (WAP – Wireless Application Protocol) devices has exploded, and the security concerns have exploded even faster. As most technical people know, the out-of-the-box security for many wireless devices is almost non-existent. While the industry is trying to change that[4], if your users insist on using WAP at home, and especially if they will be connected to your network while doing so, it is absolutely imperative you help them secure their network.

Most home WAP today is done with the 802.11b protocol, though the newer 802.11a is coming on strong, along with others even more new and improved.[5] Regardless, there are several things that are important you recommend to your user:

1. All wireless access points (known as WLANs) come with a default SSID (Service Set Identifier) – the name of your wireless network. Have your user change it immediately – to an alphanumeric name, and schedule regular changes to the SSID, perhaps every 2 or 3 months (such changes may be impractical in a large network, but should be possible for home users). And if the user's WLAN permits, disable the automatic SSID broadcast feature; there's absolutely no need to advertise the network name.

2. All users of wireless should use WEP (Wired Encryption Privacy), it's a critical tool to ensure your privacy. Various WLANs come with either 40-bit or 128-bit, the latter is highly preferred. Either way, simply enable it, then immediately change the WEP key from its default. If the interface permits, have the WEP keys generated dynamically when a user logs on, so that the encryption key is always a moving target for hackers.

3. If a home user has the expertise and/or you have the time to help, he should set up MAC address-based ACLs (Access Control Lists), to allow only his specific devices to access the network. While MAC addresses can be spoofed, it's difficult – and taking this step creates another substantial lock on the front door.

4. If your users depend on wireless communication, advise them to watch for suspicious vehicles parked near their residence – they may be getting probed by a war-driving attack.[6]

Anti-Spyware – who's watching you?

Did you think that just by recommending to your users that they delete their browser's internet cache occasionally, that their privacy is protected? Afraid not. Spyware today can take the form of cookies[7], actual installed programs, or trackable bugs[8] on downloaded pages.

We know that a great many internet sites use these devices, ostensibly to get feedback on users' browsing and purchasing habits. The problem is, however, that one finds it very difficult to trust the various entities' assertions, which are essentially that they would "never use their power for evil." Accurate or not, but the point is, they *could.* I prefer to at least offer my home users the opportunity to decline to be "tracked" by these rather shadowy entities.

To help safeguard users' privacy I recommend a couple of products. The leader in the field of privacy has been the freeware application AdAware by Lavasoft (http://www.lavasoftusa.com). I have found this product to do an extremely good job of cleaning spyware off my computers.

The second product that I like even more is Pest Patrol (http://pestpatrol.com). Pest Patrol searches for spyware in much the same manner as AdAware, but in addition it does more, by searching for Trojan Horse files that may have found their way to the users' PC – a junior version of an intrusion detection system. Pest Patrol has a free evaluation version, and the full version is not expensive ($40). I run both AdAware and Pest Patrol on my personal machine, and find them to compliment each other very well, each finding a few things the other did not.

Miscellaneous Advice – a sensible paranoia

1. If your home user only has one or two machines, undoubtedly the norm, get them to disable File and Printer sharing, which is enabled by default in most installations.

2. Make sure your user knows how to update their operating system with the latest security patches. For Windows 98-2 users and later, the link is usually available on the start menu; but can always be found at http://windowsupdate.microsoft.com.

3. Talk to them about the concept of strong passwords at home as well as at work. Get them to implement a password-protected screen saver along with a boot (BIOS) password. And yes, as part of physical security, recommend they secure the machine (chain or cable) so that it cannot 'accidentally' walk off.

4. Explain to users what a "social engineering attack" is – that no one from AOL, MSN, your organizational LAN, nor other legitimate network will call them up and ask them for their logon and password information. If anyone ever does, that person is an imposter and should not be given the time of day.

5. This is particularly important, and works in with the immediately previous point – talk to your users long and hard about e-mail security; and e-mail security includes those who use IRC and Instant Messaging. Most viruses and Trojans today enter a system through an e-mail or an IM-type client. These are often the result of social engineering.[9] Another source has estimated that as of today, one in 300 e-mail messages is infected with one of the Klez family of viruses. (Internet Security Newsletter, Vol 7, No. 1, 2nd Quarter 2002)[10]

6. I mentioned earlier that it is important that the user's AV client "plug in" or integrate tightly with the e-mail client; the reason for this being that several recent viruses are able to trick Microsoft Outlook, IE, and Netscape Navigator into opening an attachment as soon as an e-mail was read. Most mainstream AV clients have this plug-in feature. (If your user's application does not, his only alternative is to save each attachment to disk and scan it before opening.)

7. Be sure your user knows (1) how to ensure their e-mail client has the most recent security patches, and (2) why you DO NOT open any mail attachment unless you know precisely who sent it and why.

8. Encryption: Try to avoid situations where your user has to download work documents to his home machine. If it absolutely has to be done, however, get your home user to set up an encrypted disk using any of several very user-friendly applications. PGP (the free version) is available at http://www.pgpi.org/download/, and I have also used a powerful

encryption program named Steganos Security Suite, at http://www.steganos.com/en/products.htm, and there are others.

9. Finally, and this is a word just to network admins: Carefully consider how you will allow a remote user to connect to your network – a VPN connection may be secure, but that user is also authenticated straight to your network, just as if he were in the building. If his computer ends up compromised in spite of all your good advice, your network is in serious danger of being attacked from within. Examine the IPSEC protocol[11], and give some thought to Terminal Services[12], PCAnywhere[13], or even one of the other remote access tools such as GoToMyPC[14].

Conclusion

All of these things an admin may do to help their floundering home users are merely another part of layered security. Network administrators should all know the mantra about layering; if you have multiple layers and the bad guys keep running into roadblocks, they will likely choose a different target and your network will survive. And as one SANS author, Jim Willert, succinctly observed, "it is more important to have the layers than it is to have the best at each layer."[15]

I've covered what some of the most important things are for your home users to know. I recommend highly that you take what you like from the information in this paper, along with any other items you feel are important in your specific situation, and put it in a memo to your users, and have them sign it.

Only after the user has affirmed they've read and understood what you're trying to say, do I suggest that you give them access to your organizational network. Even then, only do so – if you politically can – when it is absolutely necessary.

It probably is not feasible for you or your staff to inspect your users' home computers to see that they've complied with your security suggestions – but having them acknowledge what the best practices are may at least give them some sense of appreciation for computing security. That, in itself, is a considerable accomplishment.

FURTHER RESEARCH MATERIALS

McClure, Stuart; Scambray, Joel; Kurtz, George. Hacking Exposed, 3rd Ed. New York: McGraw-Hill, 2001

Scambray, Joel and McClure, Stuart. Hacking Windows 2000 Exposed. New York: McGraw-Hill, 2001

Reavis, Jim. "Be Proactive In Your Security." SC Magazine. April 2002 (2002)

"Home Network Security," CERT Coordination Center, December 5, 2001. http://www.cert.org/tech_tips/home_networks.html

[1] "DSL growth continues at full speed," http://www.point-topic.com/cgi-bin/download.asp?file=DSLAnalysis\Q1+02+Growth+figures+5+June+2002.htm
[2] "Scot's Newsletter" at http://www.scotsnewsletter.com/28.htm#review1.
[3] "Crying Wolf: False alarms hide attacks," http://www.nwfusion.com/techinsider/2002/0624security1.html
[4] "Wireless LANS: The 802.1x Revolution," Powerpoint presentation by Dr. Bernard Aboba, seen at Wireless World 2001. http://www.drizzle.com/~aboba/IEEE/BAWUG.ppt
[5] Id.
[6] "Enhance Wireless Network Security and Mobility with Windows XP," http://www.microsoft.com/mspress/it/feature/default.asp
[7] Definition of spyware cookies, http://searchebusiness.techtarget.com/sDefinition/0,,sid19_gci214518,00.html
[8] "Web Bugs – FAQ," http://www.privacyfoundation.org/resources/webbug.asp
[9] "Social Engineering Attacks via IRC and Instant Messaging," http://www.cert.org/incident_notes/IN-2002-03.html
[10] "Opening e-mail attachments in a time of viruses," Internet Security Newsletter, 2d-2002, p. 1. http://www.securecomputing.com/pdf/ISN_Q202lowres.pdf
[11] Jason Halpern, "White Paper: Safe VPN, IPSEC Virtual Private Networks in Depth," Cisco, August 16, 2001. http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safev_wp.htm
[12] "Terminal Services," http://www.microsoft.com/windows2000/technologies/terminal/default.asp
[13] http://www.symantec.com/pcanywhere/Consumer/
[14] http://www.gotomypc.com
[15] Willert, Jim. "Best Computer Security Practices for Home, Home Office, Small Business, and Telecommuters". October 22, 2001. URL: http://rr.sans.org/homeoffice/best_practices.php/

Last Updated: July 21st, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
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 Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 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 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