

## Re: Is complete home security possible?

**Source:** <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2005-02/0255.html>

---

**From:** Leythos (*void\_at\_nowhere.lan*)

**Date:** 02/06/05

Date: Sun, 06 Feb 2005 13:29:23 GMT

On Sat, 05 Feb 2005 23:17:26 -0800, Charles Newman wrote:

>  
> "Leythos" <void@nowhere.lan> wrote in message  
> news:pan.2005.02.05.20.50.41.170111@nowhere.lan...  
>  
>  
>> 3) Block outbound ports 135,136,137,138,139,445,1433,1434 (these are  
>  
> 1433 and 1434 should also be blocked to prevent Kazaa from being  
> used on your network. Kazaa uses port 80, and ports 1000-5300

1433 and 1434 are the ports for MS SQL, the SQL Slammer worm that about shut-down the internet.

>> destination port blocks, not local port blocks).  
>>  
>> 4) Install a quality antivirus program - one that gets frequent updates  
>> and ranks in the top 3 by most corporate users.  
>  
> The thing is that the major antivirus makers want you to pay a  
> subscription fee now. Avast is free for home use, and no subscription  
> fee, and it will scan everything on your PC that goes in or out of your  
> network.

There are those that say you get what you pay for, when it comes to a mission critical system I never run the "Free" versions of AV software on them. Corporate versions of AV software don't always have a subscription base, they update for years without renewal.

>> 5) Setup Windows Updates to install at 3AM every day.  
>  
> The best way is to have it search for and download updates  
> every time the machine is booted.

Nope, I have not rebooted my XP machine in almost a month, 3AM every day is the proper method (or 2AM or any other time as long as you check once a day).

comp.security.firewalls: Re: Is complete home security possible?

- >> 6) *Download and install FireFox and ThunderBird – free browser and email clients.*
- >
- > *If you want to use Usenet, you will need Outlook Express installed.*

Sorry, wrong, Outlook Express is the WORST Usenet reader available to ANYONE. ThunderBird does Usenet as does about 30 other Windows Usenet readers. I would NEVER use OE for Usenet (or email either).

- >
- >> 9) *Create a "User" type account and use it instead of an "Administrator" level account – only use Administrator to install software or to run programs that won't run as User – do not play with email/web when as Administrator.*
- >
- > *If you are a gamer, some computer games will only run in administrator mode. Flight Simulator does this I know. If I log in under anything other than an administrator level account, I will an error message on FS98, FS2002, and FS2004, saying that I need to be an administrator to use the program, and I have heard of a lot of other games having this problem.*

Then you still need to ONLY run as administrator to do the tasks that require administrator access – if playing your game, don't browse the web, don't get email, don't do anything buy play the game, then switch back to a User account when done. Trust me, even if you don't like it, this one thing will prevent a LOT of issues.

- >> 10) *Monitor the in/outbound logs from your NAT router – this will tell you what's going on with the public network connection. If you get a linksys router you can download WallWatcher for free and it's very clear as to what's happening with your Internet connection.*
- >>
- >> 11) *If you're machine is compromised, get a router with NAT, get behind it, and then wipe/reinstall your system – while you're get people telling you that you don't have to go to that extreme, do you know of any way YOU can be sure that you have a clean machine? I've never signed a document saying a compromised system was clean unless I wipe/reinstall it, and I won't either.*
- >
- > *No argument there. I have a clean disk image made from Norton Ghost, and I regularly ghost my machines once a month. You should regulrly ghost your machines once a month.*

I've used Ghost since it was owned by BinaryResearch (5.0) and I would never ghost once a month – there are to many updates and patches and security issues to deal with to do it monthly, and on a properly configured system once a year is too much (unless it's a heavy development system).

comp.security.firewalls: Re: Is complete home security possible?

- > *In another newsgroup, one guy called my crazy for regularly ghosting*
- > *my machines to get rid of any malware, but it is the only way to be sure*
- > *nothing bad is lurking inside your machine. Where I went to college, they*

If you don't do any serious work with your computer then re-imaging it would not really be an issue, but you're failing to address the real issue – security. Re-Imaging is not addressing the issue of security. If you were to take the amount of time you invest into imaging, updates, patches, reinstalling apps, you could easily protect the machine from malware and not have to waste so much time.

- > *had a program they ran daily before closing the labs for the night*
- > *which restored the machines to a specific configuration and got rid of*
- > *any software that any students may have installed during the day, as*
- > *well as any viruses and the like that may have come in.*

Completely different scenario – we always reimage training center machines before each class – it only takes about 15 minutes and ensures that the student has a clean and working machine. This is not the same as you, being the only user, re-imaging your machine because you've not taken the time to learn about securing it.

I have been using computers since 76, never had a virus on any of my computers or computers that we manage for clients – and re-imaging had nothing to do with it. Take some time to learn about Security.

--  
spam999free@rrohio.com  
remove 999 in order to email me