

Re: Security discussion regarding hubs, firewalls, anti-virus and Vista Security

Source:

<http://www.derkeiler.com/Newsgroups/microsoft.public.windows.vista.security/2008-08/msg00347.html>

- *From:* Kayman <kaymanDeleteThis@xxxxxxxxxxxxxx>
 - *Date:* Thu, 21 Aug 2008 06:13:48 +0700
-

On Wed, 20 Aug 2008 12:38:57 -0700 (PDT), eganders wrote:

Security discussion

These are a very basic set of questions. Possibly there is an article on the web that someone can point me to that fully addresses each of these:

What security protection should I expect from:

a wireless hub/router

a software firewall

a software anti-virus, anti-trojan program

the security built into Vista

The reason I ask this is that I have a Linksys wireless hub with a WEP code activated and I also had Zonealarm with Windows XP. I had my files shared. I thought that the wireless hub should provide hardware based security from anyone being able to "look" at my files and anything behind the hub. I found that Zonealarm was giving me a lot of warnings of malware and other outside people finding me and trying to access my computer and that Zonealarm was stopping this. I don't understand the Linksys hub's capabilities well enough to not ask "why was the hub not keeping these outside intruders out?".

I now have Vista and the security it provides is suffocating. I have a hard time accessing my own files on other computers on my network and you need an ADVANCED IT degree to work around it. I would think that you could provide a secure "knock'em dead" firewall with a Linksys hub that would allow you to be "naked" behind the firewall so you did not have to deal with security at all once you were safe behind the Linksys firewall. I think this shows why I need to learn all I can so I don't leave my UAC off (which it is right now). I

Re: Security discussion regarding hubs, firewalls, anti-virus and Vista Security

want security, but I want to run my business also.

Security is a process not a product.
(Bruce Schneier)

For Vista the most dependable defenses are:

1. Do not work in elevated level; Day-to-day work should be performed while the User Account Control (UAC) is enabled.
2. Familiarize yourself with "Services Hardening in Windows Vista".
3. Don't expose services to public networks.
4. Keep your operating (OS) system (and all software on it) updated/patched.
5. Reconsider the usage of IE.
- 5a. Secure (Harden) Internet Explorer.
6. Review your installed 3rd party software applications/utilities; Remove clutter, *including* 3rd party software personal firewall application (PFW) – the one which claims: "It can stop/control malicious outbound traffic".
7. Activate the build-in firewall and tack together its advanced configuration settings.
- 7a. If on high-speed internet connection use a router as well.
For the average homeuser it is suggested blocking both TCP and UDP ports 135 ~ 139 and 445 on the router and implement countermeasures against DNSChanger. (Is the Firmware of your router up-to-date?).
And (just in case) Wired Equivalent Privacy (WEP) has been superseded by Wi-Fi Protected Access (WPA).
8. Routinely practice Safe-Hex.

Also ensure you do:

- a. Regularly back-up data/files.
- b. Familiarize yourself with crash recovery tools and with re-installing your operating system (OS).
- c. Utilize a real-time anti-virus application and vital system monitoring utilities/applications.
- d. Keep abreast of the latest developments.

And finally:

Most computer magazines and/or (computer) specialized websites are *biased* i.e. heavily weighted towards the (advertisement) dollar almighty!

Therefore:

- a. Be cautious selecting software applications touted in publications relying on advertisement revenue.
- b. Do take their *test-results* of various software with a *considerable* amount of salt!
- c. Which also applies to their *investigative* in-depth test reports related to any software applications.
- d. Investigate claims made by software manufacturer *prior* downloading their software; Subscribing to noncommercial-type publications, specialized newsgroups and/or fora (to some extent) are a great way to find out the 'nitty-gritties' and to consider various options.

Re: Security discussion regarding hubs, firewalls, anti-virus and Vista Security

The least preferred defenses are:

Myriads of popular anti-whatever applications and staying ignorant.

.