

Re: Newbie security question

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2003-09/2495.html>

From: Torti Schlumpf (tortischlumpf_at_arcor.de)

Date: 09/29/03

Date: Mon, 29 Sep 2003 22:08:59 +0200

Lynn Malmberg wrote:

> *Computer 1 Windows 98SE – my computer...home finances, e-mail*

Consider installing Kaspersky instead of Norton on this computer. Do **neither** use Internet Explorer for browsing **nor** Outlook Express for mailing, cause both are **basically insecure**. Use e.g. Firebird / Opera (browsing) and Thunderbird / Pegasus (mailing) instead; read mails just in plain text.

Keep in mind you have to care about that **no** malware will be installed on your computer. That's the main point.

If there's a malware installed on your computer, it can disable, tunnel or sidestep a personal firewall without any problem. An anti virus program can be disabled too, if it doesn't detect the malware before it's active.

And you mustn't trust in your av programm – especially not in norton – that it would detect the malware (early enough). Keep in mind that **unknown** malware normally won't be detected.

Conclusions:

- 1.) Don't trust just in your av prgram.
- 2.) Don't use usecure applications like IE and OE.
- 3.) Don't open executalbe files which you get via internet, (from untrustworthy sources) e.g. via mail. Don't even open them if they seemingly arrive from friends. Also untrustworthy sources: filesharing applications (p2p -> Kazaa, etc.), files received via messenger (AIM, ICQ,...).
- 4.) Read up on new applications before you install them to protect against unwanted spyware, for example.
- 5.) Keep **all** the applications up to date, including your operating system (Windows e.g. at <http://windowsupdate.microsoft.com>).
- 6.) Configure them restrictive (e.g. for messenger: accept files just from users on contact list, for mail: read mails just in plain text), and much more.

comp.security.firewalls: Re: Newbie security question

7.) Configure Windows to show *all* files (system files & hidden files, too) and *all* file name extensions – so you'll be able to discover double file name extensions like filename.jpg.exe. This way

> *Computer 2 Windows ME – teenage daughter...primarily AIM, some word processing for school work*

In addition to what I said above:

– She also should check word files which she gets from friends with Kaspersky before she opens them (locally or here: <http://www.kaspersky.com/remoteviruschk.html>)
– Use .rtf documents instead of .doc to protect against macro viruses.
– Consider using Miranda IM instead of AIM client. Never open executable files arriving on this way.

> *Computer 3 Windows ME – teenage son....primarily AIM*

See everything above.

> *and online games*

Don't use Internet Explorer.

> *Do I need a software firewall or is the Netgear router sufficient?*

Neither you *need* a software firewall nor the route ist sufficient. What you need is a kind of security concept which you can call "firewall". This firewall consists of all the steps mentioned above.

What ever you do: the main ambition must be to avoid a malware infection.

> *Also, my husband is very concerned about the connection being always on and wants the individual computers and/or the modem, powered off when not in use.*

I agree. At least disconnect from internet.

> *The kids want to keep their machines on 24/7 in order to leave their AIM away messages up (sort of like an answering machine). Is that asking for trouble?*

It's not a good idea. As far as I already said: disconnect if there's nobody using the computer!

> *Thanks for any answers you can provide. I'm just trying to keep peace in the family and strike a happy medium between being stupidly naive and being overly paranoid.*

comp.security.firewalls: Re: Newbie security question

Always remember: the best instrument to protect against malware is
knowledge and *learning* – it's better and more effective than any
software!

--

Regards, Torti