

Re: How safe am I really?

Source: <http://www.derkeiler.com/Newsgroups/alt.computer.security/2003-08/0069.html>

From: Joseph V. Morris (jvmorris_at_erols.com)

Date: 08/02/03

Date: Sat, 2 Aug 2003 14:20:39 -0400

Craig,

Inline, below . . .

"Craig Millar" <craig00042@netscape.net> wrote in message
news:1059698583.29628@ananke.eclipse.net.uk...
> *Opinions please. My computer runs WinXP and I have Norton Internet
Security*
> *2003. I feel that I am reasonably security conscious – always have the*
> *latest patches etc. .*

If you are running NIS 2003, do you have Security Level set to HIGH and Reporting Level set to MINIMAL? Have you disabled "Automatic Firewall Rule Creation" (wherever that is actually located in NIS 2003)? Have you ENABLED Auto-Protect in NAV (a component of NIS 2003)? Does the NAV console indicate that e-mail scanning is ENABLED? Do you regularly run Norton's LiveUpdate and install the updates?

I rather suspect that what's making you feel insecure is the Alert Tracker (the little half-globe, probably sitting somewhere on the right side of your display). If so, just "Hide Alert Tracker". The firewall still FUNCTIONS in precisely the same way; you just won't get alarmed by all those (largely unnecessary) pop-out warnings (notifications) when you receive an unsolicited inbound communication.

ALL of the associated events will still be present in the event logs, should you be inquisitive about them. Some will show in the Firewall Event log; some others may only appear in the Security Alerts log.. I believe there's also (in 2003) an Intrusion Alert log.

> *I do get regular alerts from NIS, warning me of a*
> *detected intrusion, which concerns me – for each detected intrusion, what*
is
> *the likelihood of someone slightly more competent getting through.*

If NIS 2003 notes it, absolutely none. What you (may) have to worry about are the things that NIS/NAV doesn't detect. What are these?

alt.computer.security: Re: How safe am I really?

Intrusion Detection — While NIS 2003 has a greatly enhanced Intrusion Detection capability (based on the Raptor engine that Symantec acquired), it's still not quite as advanced as what you could find in a dedicated IDS system. BlackICE, for example (which can be used safely in conjunction with NIS) examines incoming packets for approximately ten times as many potentially dangerous unsolicited inbound signature packets as does NIS.

Anti-virus/Anti-Trojan — While NIS 2003 (specifically the NAV 2003 component) does, in fact, check for something in excess of 400 Trojans (unfortunately, only the more common ones), a dedicated, memory-resident, anti-Trojan utility (also regularly updated) will notice the presence of approximately ten times as many Trojans. And, by the same token, 90% of these are rarely found 'in the wild'. Furthermore, NIS 2003 provides only rudimentary protection against spyware (see Ad-Aware or something similar) or key-loggers (see SpyCop or something similar).

What you PERMIT — This can be something as simple as your web browser or something as esoteric as running a web server.

In the first instance, when you PERMIT your web browser to have Internet access, the firewall effectively allows it to download anything that you request from a website. The firewall isn't going to protect you from such exploits and vulnerabilities. You MUST apply all security updates that are available for your browser and then ensure that you've tightened up its security settings as appropriate.

In the second instance, the situation is even worse: If you are running ANY sort of web server exposed to the Internet (and PERMITTED by the firewall) to receive unsolicited inbound communications, it is ESSENTIAL that you keep such servers updated (especially security updates) and then tighten the up the server/service to the maximum extent permissible with your needs. Now, if you ARE running any servers, having a dedicated IDS system (like BlackICE or something similar) is crucial in minimizing (but not eliminating) your vulnerability to exploitation.

Third instance, a lot of people don't realize that IM, Chat, and P2P programs (like KaZaA) are effectively Internet servers, unless properly configured (and also blocked explicitly by the firewall, as a second line of defense).

I presume, furthermore, that you're bright enough not to randomly open unsolicited e-mail or NNTP attachments and that you stay away from obvious blackhat, warez, and porn sites when using your web browser. (These kinds of known websites and these unexpected e-mail attachments are probably the most popular means of 'gifting' you with something you most assuredly don't want.)

I also assume that you are taking advantage of the Win XP/NIS 2003 capability to synchronize User accounts between both the software firewall and Win XP — and furthermore that you don't allow anyone ELSE to log on to your machine using YOUR account (especially if you tend to run using a Win

Re: How safe am I really?

alt.computer.security: Re: How safe am I really?

XP Admin account when on the Internet). Use a strong password for your own account; force other users to use a more restricted account (non-Admin capabilities).

See the recent thread at DSLR Security Forum on this subject for more information:

<http://www.dslreports.com/forum/remark.7550549~root=security.1~mode=flat> .

The whole thread is worth your time, but I was (as you might have guessed) thinking primarily of my own response there.

> *I get at least 10 alerts a day – should I be worried?*

TEN??!! That's it? (Hell, I've got a very security-aware ISP and I'd be HAPPY if I only saw ten of these alerts per day!)

> *NIS itself tells me not to take*

> *any action as it is monitoring the situation and it would obviously be*

> *pointless attempting to report each intrusion.*

Well, it's not really 'pointless'. Indeed, Symantec now provides its own reporting service (Deepsight Analyzer), and then there's www.dshield.org and www.mynetwatchman.com .

> *Is there anything further*

> *that I can do (apart from moving to *nix) to protect myself?*

Going to *nix is not necessarily going to do anything more for you. Indeed, given the fact that you even ask this question, it's likely that you could easily find yourself even more exposed. The only advantage in going to *NIX is that there are fewer viruses, Trojans, and worms out there -- but, if you can't cope with NIS on Windows, I rather doubt that you could set up the requisite protection on *NIX.

More to the point, you subsequently mentioned in this thread that you are running a wireless LAN. I suggest that you work your way through the references at DSLR Security Forum on this topic, which you can find at <http://www.dslreports.com/forum/remark.7562017~root=security.1~mode=flat> . Indeed, this may be your biggest security issue.

--

Regards,

Joseph V. Morris

jvmorris@erols.com

Re: How safe am I really?