

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