

Re: thanks and Happy New Year

Source:

<http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.general/2005-01/1023.html>

From: JW (*JustPostYourReply_at_ToThisNewsgroup.pls*)

Date: 01/01/05

Date: Sat, 01 Jan 2005 14:49:14 GMT

yes, another excellent posting, Leythos.
very insightful and rich with experience.

again, i really appreciate the detail of your response, and the patience and respect you always show people like me, who are less knowledgeable and less experienced.

now, i am going to take a nap before spending all day watching football.
Have a Happy New Year. we probably will talk here again some day.

Jonathan

"Leythos" <void@nowhere.lan> wrote in message
news:MPG.1c4079884af2643d989dc2@news-server.columbus.rr.com...
In article <RGxBd.1203335\$Gx4.409540@bgtnc04-
news.ops.worldnet.att.net>, JustPostYourReply@ToThisNewsgroup.pls
says...

> *can it happen ? not only can, but has happened, still happens, and will*
> *continue to for 2 reasons. first because there are ways to introduce*
> *Trojans and worms, that bypass the anti-virus protection.*

The same is true for ones that shut down the firewall applications.

> *second, some*
> *infections have been known to outsmart anti-virus protection, and either*
> *shut them down, replace their components, or use vulnerabilities to take*
> *control of the operating system. (this is included for the benefit of*
> *other*
> *readers, since you know this already.)*

The same happens to the firewall software, it's really anything running
on a PC has the ability to stop any protective service on a system – for
the benefit of those that don't already know this.

> *AV protection is only as good as the sleep-deprived programmer hired to*
> *write it.*

I agree, and I've stated that the definitions are "reactionary" and delayed. There are AV programs that have the ability to detect and isolate viruses that have no current definitions – they do this based on virus like signatures.

> *of course, the same can be said about a software firewall, and*
> *many have a history of problems (Norton's firewall, for example). that's*
> *why i firmly believe hardware and software firewalls are both essential*
> *elements of a Multi-layered protection plan. both have strengths -- some*

We agree, a firewall appliance and a personal firewall are necessary for a complete security solution, combined with quality antivirus software.

> *different, some in common. for example, the home user who takes his*
> *laptop*
> *to the airport no longer has his home router to protect him, and, without*
> *a*
> *software firewall, would be at the mercy of whatever cheap router the*
> *coffee*
> *shop decided to use.*

Ah, this is one after my own heart. I travel to clients across the country and take my laptop with me everywhere. I run Tiny personal firewall, an older version, on my laptop and use when I leave the security of my home or office. I even run it inside the clients offices, and have found more than one rogue system because of it. But, again, we're back to people understanding how to use personal firewall solutions – how many people can determine that it's permitted to allow a DNS query when at the airport WAP vs a probe from another WAP users system? How many people can get their firewall working when they check into the hotel without permitting the entire net block? Many personal firewalls automatically trust your subnet – meaning that if your home network was a 192.168.0.0/24 it would trust all 253 nodes, and if you connected at the hotel to a 10.0.0.0/24 it would trust all those nodes too. Many of the professional versions don't do this, but many of the free versions do.

When it comes to laptops I have a small 1 port NAT device I take with me on trips, I use it when I have a cabled connection to a network. When I'm at the airport I use Tiny and know what to allow.

If I had to make a suggestion to a user, a home user, a non-technical type, it would be to get the router first – this would permit them to get on-line, updated, downloaded, etc... before their machine has a chance to become compromised. Second would be to make sure that they have a quality antivirus solution (not a virus/firewall suite) and that it's fully updated. Third would be to install a personal firewall application, but, depending on the user, I might not even suggest it.

My mother in law is a good example of a non-technical user: She bought a new Dell computer while I was on a trip, called me and asked me what to

do, and I said "Leave it in the box till I get home to secure it and install a router". When I got home she was complaining about how slow the computer was and all sorts of pop-ups were taking over her machine. Her oldest son (almost 40) had helped her install it (He's a MAC person) and connected the Windows XP system directly to the Road Runner Cable connection. I was away for about a week, and in that time she had been compromised by more than 400 spyware tools, tool-bar helpers, dialers, and many viruses. In addition she was running as Administrator, had not updated the AV software and had not done any MS Updates.

The simple solution was as follows: Disconnect computer from net, delete partitions, create TWO partitions (OS/Data), install XP, disable file/printer sharing, install NAT DEVICE, connect to internet through NAT device, get OS updates, setup AutoUpdate for 3AM every day to install updates, install AV, get av updates, install MS Office, get Office Updates, install personal applications, install FireFox, install Thunderbird, setup User Account, password both Administrator and User accounts. Set IE for High-Security Mode for all user account and Administrator Account. When she uses the computer she uses the User Account, and does not use IE except for banking sites or POGO (game site). She uses Thunderbird for email. In the almost 1 year that she's been running like this she has not had a single case of spyware or any viruses. The only time she runs as admin is for QuickBooks, it won't run as a user level account.

I was over at her house for Christmas and did a check on her system, not one problem item was uncovered, and the router logs looked clean.

Based on the above configuration I don't think that a personal firewall in place of the router would have protected her system as well, and I don't think that a personal firewall in addition to the router would have protected her any better. Don't get me wrong, a personal firewall solution in the hands of a knowledgeable user is a great tool, but in the hands of the ignorant it's just a threat to them.

For those still on dial-up, there are a few NAT phone dialer devices on the market, but most home users are not willing to pay for one. In their cases a personal firewall application is absolutely necessary, but so is learning how to use it and to understand the threats.

--
--

spamfree999@rrochio.com
(Remove 999 to reply to me)