

Full-Disclosure: RE: [Full-Disclosure] Re: January 15 is Personal Firewall Day, help the cause

RE: [Full-Disclosure] Re: January 15 is Personal Firewall Day, help the cause

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2004-01/0606.html>

From: Wes Noonan (mailinglists_at_wjnconsulting.com)

Date: 01/16/04

To: <tobias@weisserth.de>, <full-disclosure@lists.netsys.com>

Date: Fri, 16 Jan 2004 14:44:07 -0600

> *Am Fre, den 16.01.2004 schrieb Wes Noonan um 18:32:*
> > *Did you really just propose that a viable solution is to remove network*
> > *access?*
>
> *For some systems: plain and simple yes. If the supplier of a software*
> *fails to deliver it in a "secure by default" state and even cuts the*
> *supply of patches (Windows NT4/95/98) these systems should go offline*
> *immediately. There is no compromise.*

In a world that only security mattered, maybe. In the real world however there is always compromise. Too many folks in the computer security business seem to over look this point, or confuse compromise with concession. They hear compromise and think concession, which isn't the same.

> *This "Personal Firewall Day", aimed at the end consumer, may actually*
> *plant the idea in people's head that their unpatched and non-supported*
> *Windows 98 might be safe for the future as soon as they install a*
> *personal firewall. Well, this is just plain BS.*

I haven't seen anyone saying that personal firewalls are the end solution. As Ron (and others) pointed out and to paraphrase that bastion of good security Shrek, security is like onions, there are lots of layers. Personal firewalls are just another component in addition to those other layers, and personal firewalls do mitigate potential exploits that haven't been patched. In fact, that last point is a major reason for running any firewall.

> *This is how people with exactly those "popular" systems perceive the*
> *message that they should switch to a more _secure_ system.*

Yes, because in many cases the message is not what the user is wanting from their software. Don't blame the users in that case; blame the people who continue to fail to grasp the needs of the users. Users don't want to switch to an operating system that is less functional (by perception or by fact) solely for security. As you said, security is a trade off.

RE: [Full-Disclosure] Re: January 15 is Personal Firewall Day, help the cause

Full-Disclosure: RE: [Full-Disclosure] Re: January 15 is Personal Firewall Day, help the cause

- > *This is not the same. Novell has been a propriety system and Windows NT*
- > *has been a propriety system. They both suffered from the closed*
- > *development and security assessment process. This is how Linux and other*
- > *open OS differ.*

Perhaps the biggest disservice being done to security and to Linux in general is the mistaken belief that somehow being an open development system insulates the product from the same kinds of mistakes that happens to every other piece of software out there. Take DNS for example. How many exploits exist and continue to be discovered for it? Belief that merely by being open source there is some kind of protection from exploits is a myth. Sure, you might find more bugs before you hit the street, but it is hardly a panacea.

- > *Linux isn't safer than Windows because it is less popular. It is safer*
- > *because it doesn't have all doors open by default and vendors can define*
- > *the level of security they want for their distribution.*

Actually, these two points go hand in hand. Linux can afford to restrict or not open doors because it doesn't have the broad customer bases that Windows does that have to be catered to. Does this mean that Microsoft doesn't need to do anything? No, of course not, but it merely illustrates the difficulty. If Linux had to cater to the same needs it would, and frankly it is, find that it isn't always a simple undertaking.

- > *Linux is far from being perfect. Being near perfect I'd raise my vote*
- > *for OpenBSD yet something even slips past them. But MS Windows is just*
- > *the plain opposite of OpenBSD yet Microsoft has the potential to do*
- > *better!*

I agree that Microsoft has the potential to do better. Again though, near perfect is in the eye of the beholder. If OpenBSD was so perfect, it would be more than just a specialized OS, but it isn't. Again, we come back to the security compromise bit. Being totally secure, but non-functional in the user's eyes is not perfection.

- > *The sin is that Microsoft's solution to this problem isn't closing*
- > *unnecessary services BY DEFAULT but promoting additional third party*
- > *software to put in between Windows and the Internet which the end user*
- > *has to pay, deploy and operate. This is pathetic.*

Again, you fail to grasp the difficulties in maintaining a broad customer base. MS RPC isn't unnecessary in many, many cases. You want proof? Go block port 135 on all of your internal network routers and let me know the result. Furthermore, just because someone is promoting a 3rd party solution is hardly pathetic. If you don't want to pay for something you can always turn the services off or implement the port filtering/firewalling functions that have existed in every NT flavor since NT 4.0, and maybe even 3.51 though I am too lazy to verify that one.

- > > *This security through obscurity mantra is laughable.*
- >

RE: [Full-Disclosure] Re: January 15 is Personal Firewall Day, help the cause

Full-Disclosure: RE: [Full-Disclosure] Re: January 15 is Personal Firewall Day, help the cause

> *Changing topics... not so fast! What happened to the old one ;-*)

Actually, I see them both as the same. The constant pushing of the false belief that by merely changing the operating system to something other than Microsoft (obscurity) instantly buys you protection (security) is security through obscurity by every sense of the phrase. "Choose something that most people aren't running and you won't be affected by the same things that most people are". The problem is that more threats will continue to be released, and as more folks move to the platform of choice, the threats will follow.

> *Linux is following (or should be) a strict open source philosophy. How is that to be "security by obscurity"?*

I explained it above. In this case it's the concept of "by running something few people do, you aren't as susceptible to threats". That only works as long as the choice you made remains obscure. As more people move, more threats will occur. This is true in all market segments. Hell, look at firewalls. First people stopped using Check Point because it was constantly being attacked. Then they stopped using PIX because it started constantly being attacked. Who is the golden boy of the week now? SonicWALL? Netscreen? No matter what choice you make, there will always be threats.

> > *The top dogs always get the most exploits.*

>

> *No. The most lousy systems get the most exploits. Face it.*

>

> *Take the market for webservers.*

>

> *Apache virtually owns the market with more than 60%. How come that Microsoft IIS gets the most exploits? When I look into my Snort logs I don't get any Code Reds from Apache installations trying to sneak into my net. Funny, isn't it? Why isn't there a Code Red with the level of spreading for Apache as there is for IIS yet Apache is deployed on more than 60% of webservers?*

Because they are Microsoft. No one distinguishes one Microsoft brand from the other, that's why. This all in addition to the well known fact that Microsoft shipped web services on virtually every system before Windows 2000 on by default, something which isn't counted in your 60% market share number.

Besides, Apache has had more than its share of bugs which further illustrates my point – you are not going to protect yourself by simply running something different. Sure, you may lessen the quantity or types of threats, but there will always be new ones waiting for you regardless of vendor.

> > *Accept the reality. When everyone*

> > *else starts using Firebird, Thunderbird or whatever other obscure program*

> > *you want to mention as your own personal bestest solution, then it will*

RE: [Full-Disclosure] Re: January 15 is Personal Firewall Day, help the cause

Full-Disclosure: RE: [Full-Disclosure] Re: January 15 is Personal Firewall Day, help the cause

- > get
- > > *hacked and exploited beyond belief. History proves this.*
- >
- > *In fact, "history" or better reality has proven you wrong. Or is the*
- > *Apache case just an exception?! I don't think so. It only differs from*
- > *the Linux-Windows comparison as Apache _already has_ an advantage in*
- > *market share.*

Actually, history hasn't as I explained above. This all in addition to the fact that Apache (or should we call it a patchy) has had more than it's share of exploits.

- > *Why is delivering a system with all doors shut an unrealistic*
- > *expectation? Why is delivering Windows XP Home with a closed RPC port an*
- > *unrealistic expectation?*

Why? Because it is already delivered. Besides, when you have many of the same people bitching and moaning about how Microsoft is dropping support for antiquated products and trying to move people to more secure operating systems at the same time that they bemoan why security is an unrealistic expectation, it kind of sends a mixed message. Which one do you want?

- > > *And people wonder why users don't understand, but certainly fear, a good*
- > > *chunk of computer security...*
- >
- > *Because they are told they have bought a secure operating system and*
- > *some time later they are told to buy a virus scanner, a personal*
- > *firewall, keep track of updating the OS, the virus scanner, the personal*
- > *firewall, ...*

They were never told that. They were told that it is more secure, and it is. As for patches and updates, this is true for every product. Finally, as for the need to buy third party applications, I would be willing to bet that you are one of the folks who would complain that if Microsoft started offering everything they were being an anti-competitive monopoly...

- > > *Wes Noonan*
- > > *mailinglists@wjnconsulting.com*
- > > *<http://www.wjnconsulting.com>*
- >
- > *Now, of course this is from someone who is listing Microsoft operating*
- > *systems and applications in second place for vendors...*
- >

Indeed, if the best that you can offer is a critique that I know Microsoft operating systems, I'd say you have run out of valid points to make.

All this typing and the bottom line remains the same.

If you think that by merely switching products (pick the scenario, it isn't just operating systems) that you are somehow protecting yourself, you are

RE: [Full-Disclosure] Re: January 15 is Personal Firewall Day, help the cause

Full-Disclosure: RE: [Full-Disclosure] Re: January 15 is Personal Firewall Day, help the cause foolishly naïve. There is far more to it than that.

Full-Disclosure – We believe in it.

Charter: <http://lists.netsys.com/full-disclosure-charter.html>