

## RE: [fw-wiz] Vulnerability Response

**Source:** <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2004-05/0226.html>

---

**From:** Marcus J. Ranum (*mjr\_at\_ranum.com*)

**Date:** 05/27/04

To: "Ben Nagy" <ben@iagu.net>, <firewall-wizards@honor.icsalabs.com>

Date: Thu, 27 May 2004 13:40:23 -0400

Ben Nagy wrote:

>> *The big problem with host based anything is that the*

>> *management effort scales with the number of hosts.*

>

>*Not linearly, though.*

It scales non-linearly if the problem area is well-defined.

When you go above a simple problem (a/v is a "simple" problem – I'll get to that) then it starts to fall over pretty quickly.

Consider A/V as a case study. The problem is easy because there's no need to make a site-specific policy or enforce it.

The problem's black and white:

- Either A/V is installed on a machine or it isn't

- Either the signatures are up to date or they aren't

There's no case where a user is going to need to be able to run Netsky.V3 on his desktop, or whatever. So administration scales because there's no real complexity.

Now – if you're gonna make a firewall policy for 10,000 desktops and 2,000 servers, that's another story! User bob is gonna want access to file sharing, Fred needs to reach the mainframe, etc, etc.

You wind up adopting one of 2 approaches:

- Use the policy that's most convenient to build (e.g.: permissive)

- Use a policy based on minimizing access (e.g.: secure)

The former is relatively easy but worthless. The latter is extremely hard because it's a Layer 8 problem, but it's extremely valuable.

>*I am convinced that it can be done – AV vendors*

>*already do it, MS is shipping more and more default security plus they even*

>*have a (very very basic) host-based firewall which will be enabled by*

>*default – I don't hear users screaming that XP is "less compatible" than*

>*Win95.*

Wrong!

## Firewall-Wizards: RE: [fw-wiz] Vulnerability Response

MS is shipping more and more default security EXCEPT WHERE IT IS INCONVENIENT. There's a host-based firewall that nobody uses and nobody uses at an enterprise level. There's file sharing that everyone enables with no authentication, etc, etc. It doesn't matter if you have desktops that ship with potentially useful tools if they only remain at the potential stage. Therein lies the rub.

When someone talks about doing mitigation at the host level, it needs to be pervasive to succeed. It needs to have centralized policies to succeed. It needs to enhance administrators' ability to see and enforce trust boundaries to succeed. There are technologies out there that are aimed at doing this, and they work well. Sygate, for example, is probably the best-thought-out enterprise firewall concept/system. But I won't get enthused about host-side mitigation until I see more than 1% of companies using something like that.

*> Managability of host-based agents is basically a solved problem –  
>let's move on.*

Manageability of host-based agents for trivial problems is a solved problem. Management of host-based agents for complex administrative configurations is a HARD problem – not because the software is hard to build but because of the Layer 8 issues.

*>One of my fundamental premises – no company will get secure without  
>corporate will to do so.*

Absolutely! You are 100% correct.

*>To me, change control is an \_enemy\_ when talking about rank and file  
>machines, not a friend. If you start with secure boxes, strip down the  
>services and then monitor the critical applications for problems then change  
>control rocks.*

That *\*is\** change control.

*> If you start with a million desktop PCs, build a standard  
>image based on what works for all the corporate apps and then run change  
>control then you end up with a million insecure PCs that nobody has the  
>authority to fix with any kind of agility.*

That's not change control; "that's centralized management using a stupid configuration." :)

*>Old school networks had less entry points.*

Coincidentally, they were more secure. :)

Firewall-Wizards: RE: [fw-wiz] Vulnerability Response

- > *My only real point is that true*
- > *chokepoint networks are (sadly) a dying breed. I have no doubt that you are*
- > *amused by the trend for firewalls to return to application intelligence like*
- > *it's a new thing, but not even the mjr perfectly secure firewall will work*
- > *if the traffic can get to the hosts another way.*

It's not installed correctly if you don't cut ALL the wires!!!! :)

mjr.

---

firewall-wizards mailing list  
firewall-wizards@honor.icsalabs.com  
<http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>