

Re: [fw-wiz] Worms, Air Gaps and Responsibility

Source: <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2004-05/0048.html>

From: Devdas Bhagat (devdas_at_dvb.homelinux.org)

Date: 05/05/04

To: firewall-wizards@honor.icsalabs.com

Date: Wed, 5 May 2004 20:29:09 +0530

On 05/05/04 08:24 -0400, Paul D. Robertson wrote:

> *Hospitals, banks, the U.K. Coast Guard... The damage from the latest*
> *Microsoft-based worm isn't as widespread as that from the last one, but*
> *it's pretty darned bad in point cases.*

>

> *Why do people continue to connect critical production networks to*
> *user/administrative networks?*

Lack of clue? Clue has a high cost. Monkeys work for peanuts.

> *Surely networking equipment is cheap enough that a real honest air gap*
> *(not some marketingspeak switch thingie) isn't all that difficult to*
> *deploy?*

How much does it cost? I know a lot of smaller ISPs and organisations here who buy hubs because they are cheaper than switches. You can forget about managable equipment. The cost of insecurity for most of these organisations is low enough that it doesn't matter. The trouble for the rest of us is that they are in large enough numbers that the problem doesn't reduce. Until the rest of us can drive the cost of not implementing security higher than the cost of implementing it, we are going to see these issues repeatedly.

Even those people who have some kind of firewall tend to use it as a glorified NAT device and nothing more. I know of at least one organisation with three firewalls for various purposes where the network crawls due to viral infections, and they don't have the clue needed to setup proper ACLs on their Win2K boxes. The internal IT management is outsourced and that group barely knows how to run setup.exe.

It isn't so much of a technical issue here as a people issue.

Implementing proper security has a cost. Not implementing it does not have an equivalent cost most of the time. Management decides to risk not implementing proper security because the other option is too expensive.

> *Air gaps make great firewalls. They rarely need upgrading, they're*
> *low-power and low-heat, and they're less filling and taste great.*

>

> *Worst-case, a few low-end firewalls to segment the users off from the*

Firewall-Wizards: Re: [fw-wiz] Worms, Air Gaps and Responsibility

> *production stuff should be a no-brainer these days.*

Except that doing that needs people who understand networking. I know I don't know enough a lot of times either, but then I don't purport to be a networking person either.

> *All the money, effort and time people are spending on IDS, IPS, and all
> the other buzzword-compliant devices, and yet we still don't have good
> solid separation and segmentation in places where, one would expect that
> the responsibility for running a critical network would require some level
> of protection to be displayed.*

Its not the buzzword compliant devices that matter. What matters is that the marketing department is able to say "We have a firewall and IDS and IPS and \$buzzword_du_jour, so you can trust us".

Its the administrators of the system who make or break the whole system and often they are overworked and not allocated enough resources.

<rant>

How often have admins had to deal with "The idea is good, but too expensive" comments from management about even basic security stuff?

How many administrators can choose to have their users not use Outlook/Outlook Express/IE in their organisations? (I'm not product bashing, just giving the most common examples. As far as I can see, those three products are still the most common attack vectors for a desktop.)

</rant>

Perhaps the corporate environment really needs thinner clients than we have today. A stripped down desktop would be really nice to have around where not everything needs to run as root/administrator, and users can't install their own binaries and run rampant all over the system.

Devdas Bhagat

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