

Firewall-Wizards: Re: [fw-wiz] Ok, so now we have a firewall, we're safe, right?

Re: [fw-wiz] Ok, so now we have a firewall, we're safe, right?

Source: <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2005-05/0146.html>

From: Chris Blask (chris_at_blask.org)

Date: 05/30/05

To: "Paul D. Robertson" <paul@compuwar.net>, firewall-wizards@honor.icsalabs.com

Date: Mon, 30 May 2005 13:17:20 -0400

Hello, critters!

At 12:18 PM 5/30/2005, Paul D. Robertson wrote:

.d.

*>If ever there were a wakeup call for people to start analyzing their
>firewall logs, this is it– nobody at any of the companies involved figured
>this out due to firewall logs, an author figured it out because their
>unpublished book was leaking.*

My last gig obviously has me biased (Protego – no current relationship so no axe to grind), but it seems to me that unless you can consume and process logs from fws (at the very absolute minimum) you are doomed to walking around with a fire extinguisher for a living.

o Authenticate and repudiate and investigate and remediate until you're blue in the face, but an inability to see the patterns evolving on the network makes it all a matter of treading water (which beats drowning, but it gets old quick).

o If – on the other hand – you *can* see the patterns on the network, then what specific things you choose to do about it become obvious, you can target the work that you do to improve your posture, and you can have a high level of confidence that you will know whether it worked or not.

Find some solution that can consume all the logs from all your network devices (fw, id/ps, routers/switches/vpn, servers, desktop management...) and show you maps of your network and what is/has happened, and how those data points relate to each other. I've seen 600,000,000 events/day come into a box doing such things at a live site, so you just are not going to do it with an Erector Set, and even trying to put the fire extinguisher back in your hand.

You want to get into the role of watching the known behavior of your network and using your human intelligence to tune that behavior to fit the needs of the people who pay for it's upkeep. You want to get out of the

Re: [fw-wiz] Ok, so now we have a firewall, we're safe, right?

Firewall-Wizards: Re: [fw-wiz] Ok, so now we have a firewall, we're safe, right?

role of spending all your time figuring out how to fix the broken window someone ran a cable out of.

Cisco now has a set of boxes that do that stuff off the shelf, other vendors are sure to do the same. One way or another, you should all be able to get out of the well and see the world around you at some point in the next little while, and I'm interested in seeing how that changes the battlescape... :-)

.d.

*> Seems to also intimate the Trojan being injected via autorun CDs. Anyone
> require users to provide copies of CDs received in the mail to their
> security department for later evidence gathering?*

>

*> AV isn't going to be effective against most custom Trojan Horses. We're
> going to see more of this in the future- "Hey, I'm a Volvo dealer- I don't
> have anything important on-line" or "We're a hardware store, we couldn't
> possibly be a target!" Guess what? It doesn't take much to get those
> cross-hairs pointed at you, no matter what line of business you're in.*

Which is exactly why it's time to crawl out of the well and take the higher perspective. It is good to try to control the human aspect and the endpoint they interact with, but there may always be code floating around and users doing silly things. The fact that we again create the necessary capability in time to do so is yet another example of why the Good Guys can always win the Battle [but there will still be fatalities, so be smart and don't be one!], and why I remain such a persistent optimist... ;-)

Today, imho, the best improvement in posture to be gained by a given amount of resource is to get yourself a perspective on what your network is doing.

-woof!

-chris

Chris Blask
chris@blask.org
<http://blaskworks.blogspot.com>

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

Re: [fw-wiz] Ok, so now we have a firewall, we're safe, right?