Network Security is Dead...It's All About the Host.

rationalsecurity.typepad.com/blog/2007/05/nextgen_tcpip_s.html

No, not entirely as it's really about the data, but I had an epiphany last week.

I didn't get any on me, but I was really excited about the -- brace yourself -- future of security in a meeting I had with Microsoft. It reaffirmed my belief that while some low-hanging security fruit will be picked off by the network, the majority of the security value won't be delivered by it.

I didn't think I'd recognize just how much of it -- in such a short time -- will ultimately make its way back into the host (OS,) and perhaps you didn't either.

We started with centralized host-based computing, moved to client-server. We've had Web1.0, are in the beginnings of WebX.0 and I ultimately believe that we're headed back to a centralized host-based paradigm now that the network transport is fast, reliable and cheap.

That means that a bunch of the stuff we use today to secure the "network" will gravitate back towards the host. I've used Scott McNealy's mantra as he intended it to in order to provide some color to conversations before, but I'm going to butcher it here.

While I agree that in abstract the "Network is the Computer," in order to secure it, you're going to have to treat the "network" like an OS...hard to do. That's why I think more and more security will make its way back to the actual "computer" instead.

So much of the strategy linked to large security vendors sees an increase in footprint back on the host. It's showing back up there today in the guise of AV, HIPS, configuration management, NAC and Extrusion Prevention, but it's going to play a much, much loftier role as time goes on as the level of interaction and interoperability must increase. Rather than put 10+ agents on a box, imagine if that stuff was already built in?

Heresy, I suppose.

I wager that the "you can't trust the endpoint" and "all security will make its way into the switch" crowds will start yapping on this point, but before that happens, let me explain...

The Microsoft Factor

I was fortunate enough to sit down with some of the key players in Microsoft's security team last week and engage in a lively bit of banter regarding some both practical and esoteric elements of where security has been, is now and will be in the near future.

On the tail of Mr. Chambers' Interop keynote, the discussion was all abuzz regarding collaboration and WebX.0 and the wonders that will come of the technology levers in the near future as well as the, ahem, security challenges that this new world order will bring. I'll cover that little gem in another blog entry.

Some of us wanted to curl up into a fetal position. Others saw a chance to correct material defects in the way in which the intersection of networking and security has been approached. I think the combination of the two is natural

and healthy and ultimately quite predictable in these conversations.

I did a bit of both, honestly.

As you can guess, given who I was talking to, much of what was discussed found its way back to a host-centric view of security with a heavy anchoring in the continued evolution of producing more secure operating systems, more secure code, more secure protocols and strong authentication paired with encryption.

I expected to roll my eyes a lot and figured that our conversation would gravitate towards UAC and that a bulk-helping of vapor functionality would be dispensed with the normal disclaimers urging "...when it's available one day" as a helping would be ladled generously into the dog-food bowls the Microsofties were eating from.

I am really glad I was wrong, and it just goes to show you that it's important to consider a balanced scorecard in all this; listen with two holes, talk with one...preferably the correct one ;)

I may be shot for saying this in the court of popular opinion, but I think Microsoft is really doing a fantastic job in their renewed efforts toward improving security. It's not perfect, but the security industry is such a fickle and bipolar mistress -- if you're not 100% you're a zero.

After spending all this time urging people that the future of security will not be delivered in the network proper, I have not focused enough attention on the advancements that are indeed creeping their way into the OS's toward a more secure future as this inertia orthogonally reinforces my point.

Yes, I work for a company that provides network-centric security offerings. Does this contradict the statement I just made? I don't think so, and neither did the folks from Microsoft. There will always be a need to consolidate certain security functionality that does not fit within the context of the host -- at least within an acceptable timeframe as the nature of security continues to evolve. Read on.

The network will become transparent. Why?

In this brave new world, mutually-authenticated and encrypted network communications won't be visible to the majority of the plumbing that's transporting it, so short of the specific shunts to the residual overlay solutions that will still be present to the network in forms of controls that will not make their way to the host, the network isn't going to add much security value at all.

The Jericho Effect

What I found interesting is that I've enjoyed similar discussions with the distinguished fellows of the Jericho Forum wherein after we've debated the merits of WHAT you might call it, the notion of HOW "deperimeterization," "reperimeterization," (or my favorite) "radical externalization," weighs heavily on the evolution of security as we know it.

I have to admit that I've been a bit harsh on the Jericho boys before, but Paul Simmonds and I (or at least I did) came to the realization that my allergic reaction wasn't to the concepts at hand, but rather the abrasive marketing of the message. Live and learn.

Both sets of conversations basically see the pendulum effect of security in action in this oversimplification of what Jericho posits is the future of security and what Microsoft can deliver -- today:

> *Take a host with a secured OS, connect it into any network using whatever means you find appropriate, without regard for having to think about whether you're on the "inside" or "outside." Communicate securely, access and exchange data in policy-defined "zones of trust" using open,*

> *secure, authenticated and encrypted protocols.*

If you're interested in the non-butchered more specific elements of the Jericho Forum's "10 Commandments," see here.

What I wasn't expecting in marrying these two classes of conversation is that this future of security is much closer and notably much more possible than I readily expected...with a Microsoft OS, no less. In fact, I got a demonstration of it. It may seem like no big deal to some of you, but the underlying architectural enhancements to Microsoft's Vista and Longhorn OS's are a fantastic improvement on what we have had to put up thus far.

One of the Microsoft guys fired up his laptop with a standard-issue off-the-shelf edition of Vista, authenticated with his smartcard, transparently attached to the hotel's open wireless network and then took me on a tour of some non-privileged internal Microsoft network resources.

Then he showed me some of the ad-hoc collaborative "People Near Me" peer2peer tools built into Vista -- same sorts of functionality...transparent, collaborative and apparently quite secure (gasp!) all at the same time.

It was all mutually authenticated and encrypted and done so transparently to him.

He didn't "do" anything; no VPN clients, no split-brain tunneling, no additional Active-X agents, no SSL or IPSec shims...it's the integrated functionality provided by both IPv6 and IPSec in the NextGen IP stack present in Vista.

And in his words "it just works." Yes it does.

He basically established connectivity and his machine reached out to an reachable read-only DC (after auth. and with encryption) which allowed him to transparently resolve "internal" vs. "external" resources. Yes, the requirements of today expect that the OS must still evolve to prevent exploit of the OS, but this too shall become better over time.

No, it obviously doesn't address what happens if you're using a Mac or Linux, but the pressure will be on to provide the same sort of transparent, collaborative and secure functionality across those OS's, too.

Allow me my generalizations -- I know that security isn't fixed and that we still have problems, but think of this as a half-glass full, willya!?

One of the other benefits I got form this conversation is the reminder that as Vista and Longhorn default to IPv6 natively (they can do both v4&v6 dynamically,) as enterprises upgrade, the network hardware and software (and hence the existing security architecture) must also be able to support IPv6 natively. It's not just the government pushing v6, large enterprises are now standardizing on it, too.

Here are some excellent links describing the Nextgen IP stack in Vista, the native support for IPSec (goodbye VPN market,) and IPv6 support.

Funny how people keep talking about Google being a threat to Microsoft. I think that the network giants like Cisco might have their hands full with Microsoft...look at how each of them are maneuvering.