NETWORKWORLD

This story appeared on Network World at
http:// www.networkworld.com/columnists/2008/050208-jericho-forum.html

On death and de-perimeterization

The Jericho Forum Outlook By Price Oden and Dan Hitchcock , Network World , 05/02/2008

In this month's opinion piece, Microsoft sounds off in this humorous piece written by Microsoft principal IT security architects PriceOden and Dan Hitchcock.

Click to see: PriceOden

Click to see: Dan Hitchcock

"The King Is Dead!"

OK. I admit. I didn't want to believe it when Elvis died. I didn't reach closure holding a vigil candle outside the gates of Graceland with other shocked fans. In time, however, I came to accept the wretched truth. To this day I still sing along to his albums and recall his movies, but I no longer need convincing that Elvis has left this earthly building.

It is with similar reluctance that I have come to accept the demise of the perimeter. It was the king of security controls for decades. Ah, how I depended on it. I knew every ACL like I knew every line of "Are you lonesome tonight?" But similarly I grieved the loss and moved on. I'm now emotionally and intellectually free to look for new music and newsecurity controls.

How about you? Do articles claiming the perimeter is still hard at work give you the same false hope as an Elvis sighting? Have you come to acceptance, or are you still in denial? Perhaps you're somewhere in between - maybe angry, hoping to bargain your way out, or just depressed? Swiss-born psychiatrist ElisabethKübler-Ross, author of "On Death and Dying," analyzed the "Five Stages of Grief", which provides us a mechanism to gauge where we are in the grieving process. Where do you fall?

Denial

The first, and natural, reaction to the statement that the traditional perimeter is gone, is to insist tha it isn't. Confronting the fact that the lens through which we've been viewing the world is no longer accurate is intensely painful, and our species has done well, in large part, by doing clever things to avoid pain. It is much easier (though utterly futile) to blame the world for the inaccuracy of our lens. Denial is easily diagnosed - does the subject utter one or more of the following?

"The perimeter isn't gone - see, it's right here!" (points to Visio diagram, firewall in a server rack).

"People who say the perimeter is disappearing just don't know how to set it up properly. My perimeter is much better than theirs."

"This talk of a disappearing edge is just anti-firewall propaganda…"

Or, the most common and dangerous of all – denial of being in denial:

"Yes, I get it. I know all about this disappearing perimeter, and I've already taken care of it by putting the stuff I really care about behind these fancy new firewalls."

Anger

If you find yourself sputtering mad about the failure of the perimeter, you are to be congratulated for having moved past denial. You may even feel like lashing out at any of a number of "perpetrators" of this dissolution, asking:

"Why are my users sending our data all over the place? I block the port, and they find another. I kill their Internet access, and they burn CDs. I pull out their CD drive, and they use USB fobs. I take away their computer, and they switch to their own laptop or mobile device, or just pick up the phone."

"Why didn't my security vendors warn me about this? I was paying them to make sure I was secure, and run the tightest perimeter possible, yet all my customer data keeps showing up outside my company!"

"How dare you, insolent *Network World* article author, tell me that I'm in denial! I've been in this industry for 30 years, and I'mCXO of Acme Corp! If there's a problem, I'll tell you about it!"

Bargaining

After sufficient venting, the negotiations begin. The trouble is that this is like cave-people negotiating the beginning of the next Ice Age, in that the results of the negotiation have no bearing on the eventual outcome. This is the stage where we say, "Well, I guess maybe information does want to be free, but I bet the perimeter can still do the job if we just make a few tweaks here and there."

Here are a few common bargaining tactics employed in the face of the disappearing perimeter:

"The old perimeter doesn't work, but how about a bunch of smaller perimeters around my

servers? Surely those will work - we'll call it 'network segmentation' (or sub-zoning, or zones, or micro-segmentation, or islands)."

"I guess it's time to double-down and shore up that perimeter. Let's get serious about 'Defense In Depth'."

"Well, everybody has this problem, and it's too hard to solve. We'll stick to business as usual, and document this as a tough problem that we just can't afford to tackle right now, given all the money and effort we're expending on our current set of security tactics."

Depression

This stage features a wide-angle shot of a guy in slacks in a nearly-empty data center, slumped in the corner, with his head between his knees. He is bereft of hope; he mutters, "The perimeter is gone, and there's nothing I can do about it. All my company's data is going to the highest bidder."

Because folks in the IT industry are paid to solve problems, you likely won't find many people in this stage darkening the halls of your organization. Those who remain on the job, do so because they progress quickly to acceptance. Read on ...

Acceptance

"... I got my mind right." - Paul Newman, "Cool Hand Luke"

In this final stage, we emerge weary and battle-worn from the prior stages, but with our mind finally freed to rationally confront the new reality of a world without traditional perimeters, and to begin to seek solutions. This investigation, when undertaken of our own free will, leads to powerful new concepts . We understand that our fundamental goal has not changed -- we were never really trying to protect our territory (our network), but rather, its inhabitants (the data itself). Our firewalls are not fundamentally flawed, but we accept that our mandate is to provide more granular and portable protection for the assets that actually matter to the businesses we support. The e-mail, the spreadsheet, the dynamic HTML, the ad-hoc query result -- these are the bearers of our intellectual property, trade secrets and regulated data, to which protections are most appropriately applied. We look with gratitude upon the technologies that have served us well in past, and resolve to create, invest in, and ultimately rely upon solutions that will hold fast in a world of dissolved perimeters and ubiquitous inter-connectivity. We understand, deeply and fully, that the data is the asset.

When considering the dissolution of the perimeter, we seem to be primarily trapped as an industry in denial, with a smaller contingent in the bargaining phase, whether we admit it or not. Practically nobody has reached acceptance. This collective refusal to acknowledge the loss of the perimeter undermines the focus we need to build new controls to deal with increasing demands for data security. We cannot accomplish the evolution of security controls, which is critical to ensuring the safety of our digital assets today and in future, until we fully come to grips with the death of the perimeter. Even as we come to acceptance, we will likely find it necessary to negotiate with those still in denial -- far from the "bargaining" that chains us to the past, this will represent an enlightened, practical push to optimize the present, and an opportunity to help others through the grieving process that we have undergone.

The viewing has been protracted, and the corpse is festering. Are we ready, finally, to lay the

perimeter to rest?

The Jericho Forum is an organization dedicated to encouraging broad innovation in e-commerce security. It coined the word "de-perimeterization" to describe the process of reducing or even eliminating the traditional role of the perimeter firewall to assist e-commerce collaboration without sacrificing security. The Jericho Forum, primarily an end-user organization with some vendor membership, also coined the word "re-perimeterization," which stresses pushing security controls closer to critical data.

The complete collection of monthly Jericho Forum Outlook columns can be found on the Network World site.

All contents copyright 1995-2008 Network World, Inc. http://www.networkworld.com