Kevin Bingham
Zero Trust Technical Lead
Cybersecurity Directorate
National Security Agency (NSA)

At NSA, Helping Customers Get To Zero Trust

The main attribute of a successful Zero Trust program is getting that full buy in from the senior leaders of the organization all the way down to those engineers, the architects, the administrators, the implementers of the capabilities themselves.

Progress: Embracing Paradigm Change

We are trying to continually advance and improve our customer's networks over time. For a decade NSA has had this belief that the "assumed breach model" was really a good one – one that customers needed to take into account. But what we found was that there were a lot of people that just continued to do things the way they had done them in the past. To have the confidence to break away from that legacy mindset of those programs and those activities that you have been doing in the past to do something different and new is hard – even when you accept that an assumed breach model is what you have to go with.

Mr. Bingham comments are from the Federal Executive Forum on Zero Trust Architecture broadcast on Federal News Network.

And two years ago when we started studying how can we get a push for improving the security on the inside of some of our networks, we looked at Zero Trust and thought that it gave a nice disciplined approach to start being able to understand the different pillars of functional capability areas that people needed to start putting attention into. That is what really attracted us to it.

That way we would be able to have a security model encompassing a paradigm change in the way we do things to accept that assumed breach model and actually do some things that are different. We started locking down those privileged accounts and those accesses from the users and the devices to stop the adversary's ability to maneuver through the network. So we are pretty excited it and think that as the adoption of this security model starts to gain momentum and as people start seeing positive results of their work in this space that we'll see not only improvements across the federal and DOD space, but also in the vendor community too to support the needs of their customer base.

Success Improves Using Red Teams For Assessment

My team is externally focused so we're focused on customers. In our effort to learn and help customers get to Zero Trust, we have looked at a number of different examples and we've worked with a number of different partners along the way. As a result, we've seen those efforts that work well and get up to speed quickly and those that don't.

I would say that one of the attributes of a successful Zero Trust program is really getting that full buy in

from the senior leaders of the organization all the way down to those engineers, the architects, the administrators, the implementers of the capabilities themselves. When we see that, things roll pretty quickly. When we don't see that, it's not that the organizations don't come around to recognizing the value of Zero Trust but it slows things down a lot. So that's an attribute of a successful program – making sure you have that full support of the organization and buy in. When you get that it's fantastic.

This is a paradigm change so we need to make sure that people aren't just saying "sure I'm doing some Zero Trust and I know that I got to worry about users and devices and whether or not those devices are able to access resources", but accepting that an adversary is assumed in the network you really need to have Zero Trust there in order to drive change. It's not necessary to be paranoid about protecting those privileged accounts; in truth it's the way we should have been doing things for years and the assumed breach model helps us get there. Understanding that paradigm change drive changes within your network.

This is a paradigm change so we need to make sure that people aren't just saying "sure I'm doing some Zero Trust" and actually take action.

A good mental exercise is to think about the capabilities that you choose. For example, if you're on an open Wi-Fi coffee shop network that you're trying to secure, how would you do that differently? It's not about the technology either, it's about implementation of the capabilities, the implementation of the model itself.

We've seen customers buy new products to drive change and we've seen some military partners do it with very little cost using enterprise software licenses and capabilities successfully. That is fantastic but ultimately the resources need to be both on the people side and the funding side.

Another important factor for success are having the right the methods to do validation right. An example of that could be bringing in a Red Team in so that you have an assessment that has baselined your environment in the past and then be able to measure your effectiveness as you start rolling out Zero Trusts in the future to where you are doing better.

Are you shutting the Red Teams down or are they still able to get around? If they are, then have them help you figure out what changes need to happen in order for you to tighten up that network. We're seeing success out there with a little going a long way; and as people are starting to roll out a properly implemented Zero Trust model, we start seeing success from those Red Team assessments pretty quickly.

Priority: Create Guidance Documents To Move Towards Zero Trust

My team is externally focused on customers. Our customers are critical system owners including national security systems that include DOD customers as well. We've been working with the Defense Systems Information Agency (DISA) and Cybercom over the last year to try to create guidance documents that will help the DOD specifically to understand and move towards Zero Trust;

So DOD released a Zero Trust reference architecture back a few months ago which we're hoping will help people understand within the DOD how to apply Zero Trust principles. Following from that our team is focused on partnerships with DISA to make sure we understand what test beds we need to continue to develop in order to learn, practice, innovate and turn that into future guidance; and then evolve and learn how to do Zero Trust capabilities more efficiently whatever those challenge areas happen to be.

That might be in data tagging, data protection, identity. Those are challenging areas for us already; but for us it's going to be trying to stay connected with our customers in the community and try to produce the guidance that we feel will help them in areas that may need help. ■