The ZTA Education Challenge

Zero Trust is really kind of the nuts and bolts needed to move out of the old way of doing business into a new way that helps keep us secure in the future.

Charlie Armstrong
CIO (retired)
Customs and Border Protection (CBP)
Department of Homeland Security (DHS)

With the implementation of a Zero Trust Architecture (ZTA), organizations are moving away from a site-based perimeter security approach, moving towards a software defined perimeter approach. This is key because – especially with Covid – you have a workforce working from home or working from anywhere so you absolutely need to extend security far beyond what we used to call the perimeter.

Everybody is migrating to cloud services – not just a service but multiple services. Agencies are hooking up to a variety of different Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS) capabilities, so Zero Trust is really kind of the nuts and bolts needed to move out of the old way of doing business into a new way that helps keep us secure in the future.

Further, because it's more policy-based, it requires a lot more upfront thought not just from the security types, but from the leadership as to what the policies should be and who has access to what. This is more than just getting into the system itself, but what access, what data, what devices is approved for that user.

This will help make security more ubiquitous in the future, so if a bad guy gets in, at least the agency can limit what intruders get access. This is opposed to "I'm in and now I get to go everywhere across the network, both horizontally and vertically". Also ZTA helps contain internal threats; that can be someone who wants to do something bad or someone who accidentally does something that disrupts, not meaning to. ZTA will help us to get to a very different state of trust.

Lifestyle Changes

We are always changing what we do and how we do it; that requires us to think before we make changes as to what does the security need to look like around us. That's something we haven't done in the past.

For me, the challenge for the CISO community is educating people across agencies and across user communities as to what does ZTA mean to them. That is both in terms of how they may need to operate differently or think about things. They need to make sure they are moving forward in lock-step with the security policies and administrative needs in their agency. That way there won't be surprises that either slow down the mission from getting new things done

ZTA is more policy-based and requires a lot more upfront thought not just from the security types, but from leadership as well. This is more than just getting into the system itself, but what access, what data, what devices is approved for that user.

versus losing or compromising security in order to get there.

The education challenge has always been there, but even more so in this Zero Trust environment.

That's because there is no clean slate. There are no agencies being stood up from scratch. So if you look across the federal, state and local landscape, you already have a lot of existing infrastructure and systems that are out there. And everybody has the goal of migrating to the cloud, using more SaaS offerings, maybe owning and operating less equipment and relying more on commercially available services.

The issue is how do you make all that fit together and make it so you can plug and play and move faster. This sets up a framework to move quicker, but move more methodically in terms of thinking about those things that impact access and who should get to do what.

ZTA should also cause leadership to examine who gets exemptions. For years, we have allowed executives and people with special privileges to do things that they didn't need to do or shouldn't be doing inside the network.

This causes problems because the adversaries get access because someone left a door open or because someone doesn't want to use multi-factor authentication or doesn't want to follow the policies in place for everybody else.

As a result, leadership will be more conscious because there will be more accountability and it will be their necks are on the line if this stuff doesn't work. ■

About The Author

During his career at DHS, **Mr. Armstrong** functional responsibilities included software development, infrastructure services and support, tactical communications, the laboratory system and research and development functions, and IT modernization initiatives supporting CBP's core business processes.

He also served as DHS Deputy CIO where he was a champion of the Department's IT initiatives for improving the agency's secure information sharing capabilities through the consolidation of infrastructure and strengthened security. Mr. Armstrong has over 30 years of leadership and technology experience in the operations and management of IT.