DISA Leader Calls for Increased Zero Trust in an Era of Cloud

A layered defense approach won’t work anymore — zero trust is necessary as the Defense Department moves to the cloud.

Melissa Harris

Thu, 02/20/2020 - 14:38

Photo Credit: Sonja Filitz/iStock

As the Defense Department continues to move toward cloud capabilities, it also is looking to lean into a zero-trust model of securing those capabilities and cloud environment. Such a model is necessary amid breaches, insider threats and other cybersecurity concerns that department faces daily.

Traditionally, DOD has approached cybersecurity with a layered approach, which Defense Information Systems Agency Cloud Portfolio Chief John Hale called “defense in depth.” After gaining access through the many layers of DOD security — from firewalls at the edge to intrusion detection devices, reporting and aggregation of data — a user gains full access to the network.

Although this “defense in depth” approach was effective in DOD’s internal, closed-network environment, Hale highlighted that this model is problematic in an era of client-serving cloud computing.

“We’re seeing now the problems with the layers model,” Hale said at the FCW Cloud Security Workshop Thursday. “Once you’re inside, you’re inside. And then lateral movement is the big fear that everybody has from a cloud perspective. Once you get past your defense and you’re inside, that lateral movement from one system to the other, elevation of privilege down the chain, is the scary part.”

Hale noted that zero trust is data centric, which he said works well with the nature of cloud infrastructure.

“The data is the cloud is what’s valuable, and access to that data is not guaranteed at any time, so in order to gain access to the data, there’s a myriad of pieces of information that have to come together for you to grant gained access to that material and that data into processing,” Hale said. “That could be anything from who you are, where you are, what kind of device you’re on, what network you’re on. A myriad of factors ultimately drive to an authentication decision, so that you can gain access to that data and utilize it.”

In particular, DOD is looking to use mobile devices to help create an authentication signature. Once DOD personnel and warfighters generate an authentication through their mobile device, Hale said that those individuals will be able to access, process and manage data in the cloud.

“That’s kind of where we see things going, is that integration between the mobile world and the cloud world [in] how the communications are going to happen between that, how zero trust is going to be directly influenced by the end-user device that they’re using to access the capabilities and how they’re able to process that information accordingly,” Hale said.

With this zero-trust approach to cybersecurity, Hale said he hopes to see industry partners help move the department in that direction as well.

“The missions are pushing toward zero-trust model, and we’re really hoping that commercial products catch up and leads up in that way, in that direction,” Hale said. “Zero trust is one of those things where we’re looking at commercial partners to really help us get to that model and to help us across the board to make sure that we can continue to push the cloud capabilities to enable the warfighter to complete their mission.”

View printer friendly version
Zero Trust
cybersecurity
DISA
DOD
cloud
Standard