McAfee

SIGNAL
More than a magazine: We're AFCEA.

https://www.afcea.org/content/closing-all-dod%E2%80%99s-cyber-doors-zero-trust

Securing all of the entryways into U.S. Defense Department networks with zero trust is a multistep process, says Alex Chapin, vice president, McAfee Federal. Credit: mkfilm/Shutterstock

Closing All DOD's Cyber Doors with Zero Trust

February 16, 2021

By Alex Chapin

Fulfilling the zero trust vision is a multistage effort.

Ask someone in federal IT what zero trust means and you're likely to hear that it's about access control: never granting access to any system, app or network without first authenticating the user or device, even if the user is an insider. The term "Never trust; always verify" has become a common way to express the concept of zero trust, and the phrase is first on the list of the Defense Information Systems Agency's (DISA's) explanation. For DISA, "**Never trust; always verify**" is followed by "Always act as if an adversary is already present in the environment," and "Verify explicitly," corresponding to the basic stage of the Department of Defense (DOD) Zero Trust Maturity Model. Similarly, NIST's initial publication on **Zero Trust Architecture** emphasizes access control, calling the goal of zero trust "to prevent unauthorized access to data and services coupled with making the access control enforcement as granular as possible."

The basic stage, access control, is indeed a critical first component of zero trust, and the DOD should be commended for undertaking it aggressively. The zero trust journey does not end there, however, and the recent nation-state attacks on U.S. government infrastructure via Solar Winds provide an even more compelling reason for the department to accelerate its move to the intermediate and advanced levels of zero trust.

The DOD's own Digital Modernization Strategy has made one of its principal objectives to "treat data as a strategic asset," and the department recently published a separate DOD Data Strategy that lists "data governance" as the first step to operationalizing the strategy. The application layer, layer seven, which speaks to app and data-centric security, is at the heart of zero trust.

It might be useful to think of the basic stage of zero trust (identity/access control) as analogous to securing the front door of a house—and maybe even the interior doors that lead from room to room. You want to make sure every entrant is verified and authenticated—even when they want to enter another room from within the home. But the front door is not the only entrance. There are side doors, back doors and basement doors that also need securing. For these doors, the main concern should be data. DOD IT personnel need to make sure they understand activities at all doors through multicloud/multi-app visibility and command and control on any data flowing in and out on the side and back doors. Without these controls, data can leak out, exposing sensitive information. In an actual house, you would never leave these doors and windows unlocked or without additional security such as cameras and alarms.

In a recent interview about COVID-19's effect on security, DISA Director Vice Adm. Nancy Norton, USN, says, "With zero trust, we will affect every arena of our cyber domain, allowing us to shield our data better by closing every compartment in the ship." Very well said, and what's needed to accomplish that is moving beyond access control—or securing only the front door.

Let's take a couple of examples. It's well known that both cloud usage and the threat landscape have skyrocketed during the pandemic. The DOD deployed the Commercial Virtual Remote (CVR) cloud productivity tools to 1.1 million users in just a few months, rapidly expanding their cloud usage in 2020. A recent report found that cloud use from unmanaged devices doubled between January and April, and external attacks on cloud accounts increased 630 percent. Therefore, protecting data by securing more than just the front door is especially important, as so many in the DOD are working from remote environments and accessing data and apps from both multiple cloud and hybrid cloud environments.

Say a service member is working on a personal computing device, not going through the unit's virtual private network, and wants to access an app from the cloud service Microsoft

Teams. While the unit has a secure connection to Teams, the app plug-in is likely hosted by another cloud provider, which might be secure but might not. This cloud-to-cloud connection opens an aperture, a side door, that needs to be locked to prevent sensitive data from being exposed. Access control won't help that situation; that's a role for unified cloud policy data protection.

Let's take a backdoor example that's more technical. Open S3 (Simple Storage Service) data buckets have been responsible for recent data breaches, because when misconfigured, they allow for data leakage. An open data bucket is like a back door that is left unsecured. The S3 bucket can be made public or kept private, and it's not difficult to mistakenly choose one over the other, especially when technicians are overworked and managing multiple buckets across an enterprise. Choosing the wrong option opens this backdoor to the public by accident. Again, access control and identity management do not fix this, but intermediate stage multicloud data protection solutions do.

As the DOD progresses toward the intermediate and advanced stages of the Zero Trust Maturity Model, key capabilities that will ensure their success include complete visibility into multicloud environments, security analytics used to assess user behavior, dynamic policy enforcement for advanced data protection for sanctioned, unsanctioned, and most importantly DOD-coded mission apps, and automated and orchestrated threat detection in hybrid cloud environments.

Fulfilling DOD's objective of a zero trust cybersecurity framework is a multistage journey. After implementing the basic stages with access control, identity management and encrypting the data stream from the endpoint to the cloud, DOD will begin moving towards the intermediate and advanced stages of zero trust. In these stages, data-centric security takes the spotlight. Access control will always be critical, but it is just the first important step of the zero trust journey.

Alex Chapin is a vice president on the ***McAfee*** *federal team.*

Enjoyed this article? **SUBSCRIBE NOW** to keep the content flowing.