How DHS is Securing Data in the Telework Era

Zero trust is more than verifying users, it's also verifying infrastructure.

Kate Macri
Mon, 08/31/2020 - 14:22

Securing data in a remote environment means constantly verifying and re-verifying users, and distrusting all connections on a network until they're verified.

Conditional access is a key tenet of zero trust, which the Department of Homeland Security is actively working toward across its components.

Along the zero trust model, the agency has been on working to establish a more "human-centric" cybersecurity policy, which is especially important during the current telework era.
“We got through the first sprint around conditional access,” said DHS Executive Director of IT operations Luis Coronado said at a FedInsider webinar last week. “[What] we thought was normal behavior before, but now it may be abnormal [in a remote environment]. It may not be tied to the user, but now it may be tied to something else. We're looking at that from the cloud secure gateway perspective and TIC 3.0. How are we going to go through and access these cloud services without going through the physical infrastructure?”

When moving to a cloud or remote environment, there is no physical infrastructure that outlines boundaries. As such, government agencies should think about their cybersecurity not as a "castle moat" with a perimeter.

“The dissolving of the [physical] perimeter has rapidly changed the way cybersecurity personnel need to work and protect their infrastructure,” said Eric Texler, vice president of global governments and critical infrastructure at Forcepoint. “You still need boundary firewalls — no one is going to argue that doesn't make sense. But what happens when a larger number of your transactions never cross the physical boundary of your data center?”

That's where conditional access and zero trust come in. Coronado said access to data might be granted to an employee depending on what attributes they possess — like security clearance or job duties. Depending on an employee’s credentials, they may gain partial access to certain data, full access or no access at all.

“If I'm coming in from somewhere where I don't have those attributes, maybe it doesn't block me 100%, but maybe gives me less access to that data,” Coronado said. “To get to a full maturity where you can get your data accessed based on specific attributes you're presenting from an authentication and authorization perspective, now we're moving from zero trust and getting more granular on the access of the different levels of the data itself. We're not there yet, but I think that's the full maturity.”

Continuous scanning and real-time visibility go hand in hand with conditional access and zero trust, he added.
“The [DHS] components have identified toolsets to allow them the capability to continuously scan the actual containers as part of the continuous diagnostic pipeline,” he said. “As you're deploying them out, they're conducting this scanning. If you're using the full extent of the cloud, you're using scanning the same way — that addresses the infrastructure-as-a-service perspective.”

Because more and more government employees aren't working in a traditional office environment anymore, Texler advised government agencies to think about their data networks and users as a series of constantly shifting risk equations.

“Understanding what they're doing and what they're doing it with, the value of the data ... I think that's the future,” he said. “You can't manage the threats anymore; you lose more and more money. We'll talk about zero trust and inspecting behaviors and automation, those are the concepts of the future that will better protect us.

View printer friendly version
Department of Homeland Security
Zero Trust
Federal Cybersecurity
Standard