FIFTH DOMAIN
CYBER

When zero trust in government is a good thing

Jessie Bur,
May 9, 2019

https://www.fifthdomain.com/civilian/2019/05/09/when-zero-trust-in-government-is-a-good-thing/

What might be considered paranoia in real life has become the standard that many government officials are looking to achieve in protecting their data and networks from cybersecurity incidents.

According to both industry and government experts that spoke at an April 8 ACT-IAC event, applying a "zero trust" model to agency cybersecurity could provide an ideal route to protecting sensitive government data, while checking the boxes on many government security requirements.

Zero trust is not a product, said Sean Frazier, advisory chief information security officer for federal at Duo Security. Rather, zero trust is a mindset where no user is automatically deemed trustworthy, and every system must verify the user before granting access.

"It's a direct conversation between a user and an application on a device," said Frazier.

Effectively, a zero trust framework ensures that every system verifies the identity of the user and their authority to access various types of information before granting access to its data or operations. And just because one system granted a person access, doesn't mean that the user suddenly has the ability to see everything on the network.

But according to Lisa Lorenzin, that doesn't mean that systems should feel more closed off than they were before zero trust was implemented.

"'Zero trust' is a misnomer. You start off by not implicitly trusting anyone, but that's not our goal. Our goal is to figure out who we can trust, how we know we can trust them and what we trust them to do or to access," said Lorenzin.

“For me, zero trust is a way to ensure that the end user can get to whatever they need with as little friction as possible, and everything else is window dressing. We need to take cybersecurity from the group that says ‘no’ to the group that says ‘yes,’ and I think zero trust is how we do that.”

Despite the fact that zero trust is a mature and tested cybersecurity model, according to Lorenzin, it may take the federal government some time before that model can be widespread, no matter how well it works.

Steven Hernandez, director for information assurance services and CISO for the Department of Education, said that federal agencies can’t be like private sector companies such as Google, which revamped its entire architecture to adhere to a zero trust model.

“Don’t expect all agencies to put out one requirement that’s going to say, ‘yeah, I want zero trust.’ It’s going to look different, it’s going to feel different, but it’s all going to have some kind of intersection with zero trust,” said Hernandez.

Limited budgets, deeply entrenched legacy IT systems and inadequate IT workforces can all hold back a wholesale transition into zero trust-based cybersecurity.

Meanwhile, agencies should look into ways that they can map their “crown jewels” up to a zero trust framework, according to Hernandez, and work on getting the rest of their data into a zero trust model in the future.

“Zero trust implementations will need to be very scalable,” said Jeffrey Flick, acting director of the Enterprise Network Program Office at the National Oceanic and Atmospheric Administration.

According to Hernandez, the side benefits of zero trust can also be used to sell the concept to agency leadership.

“Zero trust can drive a lot of the existing compliance programs we already have, if we do it right,” he said, adding that the model can allow agencies to maintain that compliance while expanding the devices or locations where users can access agency systems.

“That’s how we’re going to sell zero trust if we’re going to be successful. We’re going to show that, instead of government-furnished equipment with five-factor authentication for getting through, adding tons of latency, we’re going to say ‘any device, anywhere, with very simple authentication to get into that data.’”