Laying the groundwork for zero-trust networks

BY MARK ROCKWELL
APR 18, 2019

https://gcn.com/articles/2019/04/18/zero-trust-networks.aspx

With mobile and cloud technologies expanding and complicating today's networks, securing the perimeter is no longer a viable option. Many agencies are investigating zero-trust solutions to address expanding threats.

ZT network architecture steps beyond traditional cybersecurity technologies because it assumes intruders are already on the network. Rather than relying on perimeter security to keep threats out, the platform requires network users be constantly authenticated, which can block bad actors already inside networks from moving laterally. Besides providing better security, the solution also gives network operators offers more data on user behavior.

In May 2018, the Federal CIO Council's Services, Strategy, and Infrastructure Committee asked ACT-IAC to examine the technical maturity, availability and uses of ZT networks for federal agencies. The organization's white paper, which was released April 18, discusses the suitability of ZT networks in government and the challenges implementing ZT solutions would present for agencies.

ACT-IAC reported that commercial ZT solutions are currently available, but it warned there isn't a single holistic ZT solution available from a single vendor, so agencies would have to integrate products and services from multiple vendors.

"Everyone is slapping 'zero trust' on products," said Darren Death, vice president for information security and CISO at ASRC Federal. Agencies should approach ZT technology and techniques the way they first did cloud technology several years ago, knowing it will evolve and shift in the coming years, he said at an April 17 ACT-IAC meeting where the white paper was first presented.

Other challenges to ZT, according to Department of Education Chief Information Security Officer Steven Hernandez, include the federal government's increased emphasis on shared services. Since ZT relies on collecting and analyzing enormous amounts of network user data to establish behaviors, shared services providers are challenged in understanding the intricacies of other agencies' customer data.

A bright spot may be the General Services Administration's 15-year, $50 billion next-generation telecommunications contract. As agencies modernize their networks and move to the governmentwide Enterprise Infrastructure Services contract for telecommunications and network infrastructure, they can include ZT components as part of their transition.

With its cadre of software-defined networking services and other advanced capabilities, EIS "is one of the core components of any zero-trust network," Hernandez said, and must be considered by agencies trying to move toward ZT architecture, he said. EIS has a number of ways to get at future ZT architecture, he added, "but it's about how to ask for the right thing from EIS."

The white paper's release comes as GSA has granted the first authorities to operate under EIS and the first "working" contract for services has been awarded.

This article was first posted to FCW, a sibling site to GCN.