Zero-trust networks to build on EIS

By Mark Rockwell
Apr 17, 2019

https://fcw.com/articles/2019/04/17/zero-trust-rockwell.aspx

The General Services Administration's 15-year, $50 billion next-generation telecommunications contract will be key for agencies implementing emerging secure network architectures that literally "trust no one," according to a new white paper.

With its cadre of software-defined network (SDN) services and other advanced networking capabilities, the GSA's Enterprise Infrastructure Services contract "is one of the core components of any zero-trust network," Department of Education Chief Information Security Officer Steven Hernandez said at an April 17 ACT-IAC telecommunications and cybersecurity community of interest meeting.

Last May, the Federal CIO Council's Services, Strategy, and Infrastructure Committee asked ACT-IAC to examine the technical maturity, availability and uses of zero-trust networks (ZTN) for federal agencies. The white paper discussed at the meeting is the product of that request.

ZTN is a network architecture that 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. The architecture is drawing interest among federal agencies, where it can not only provide better security, but also more data on user behavior to network operators.

The white paper, set for release on April 18, reports that commercial ZTN solutions are currently available, but warns there isn't a single holistic ZTN solution available from a single vendor.

"Everyone is slapping 'zero trust' on products," said Darren Death, vice president for information security and CISO at ASRC Federal, who presented the conclusions of the ACT-IAC paper at the meeting. That doesn't mean those products can't be used, he said, but it does mean a complete ZTN solution can't simply be bought. Agencies must remember that acquiring a comprehensive solution now requires integrating multiple vendors' products and services, he said. They should approach ZTN technology and techniques the way they first did cloud technology several years ago, knowing it will evolve and shift in the coming years.

Other challenges to ZTN, according to Hernandez, include the federal government's increased emphasis on shared services. Since ZTN 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.

EIS, Hernandez said, will allow SDN capabilities that can limit access to data that not all users on the network should be able to see. SDN and other services available under EIS must be considered by agencies trying to move toward ZTN architecture, he said. EIS has a number of ways to get at future ZTN architecture, "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.