AI, Zero Trust Could Be Key to Securing Federal Telework

For many agencies, extended telework policies may require reevaluation of cyber risk posture.

Kate Macri
Thu, 08/06/2020 - 14:47

Federal agencies say teleworking is here to stay, and they’re adjusting their cybersecurity strategies accordingly.

For many federal agencies, teleworking presents a unique cybersecurity challenge: suddenly thousands of employees are using home Wi-Fi networks and personal devices to work, and sometimes view classified information, potentially opening up their department’s network up to cyber criminals and nation-state actors.
Zero trust architecture and constant monitoring of all network nodes are important, but a mindset shift is key, said senior officials from NIST, the Air Force and the Department of State at a FedInsider webinar last week.

Frank Konieczny, chief technology officer for the Air Force, said the service was not prepared for mass telework at the beginning of the coronavirus pandemic, but prioritizing security issues while shifting to remote work ensured it didn’t encounter any major cybersecurity hiccups.

“The first thing we did was ask, ‘how are we going to maintain security, and how many VPNs do we have to establish?’” Konieczny said at the webinar. “The second piece was how can we give security to everybody out there, and how do I communicate with people who do not have a government laptop?"

As a result, the Defense Department set up a Microsoft Teams site that allowed everyone to connect with each other at a lower security level, he added.

Pete Gouldmann from the Enterprise Risk Office at the Department of State said another key issue was educating employees on cybersecurity best practices while teleworking and implementing a zero trust policy for all connected devices.

“I think we need to all accept the fact that a defense model is not going to be enough all on its own, it limits your reach for your ability to work,” he said. “One of the things I would suggest is a very strong focus on data and identity management."

Gouldmann detailed the practice where personnel were cleared for software and services with an all-or-nothing approach is now gone.

"Nowadays we're able to do business with people with a different level of trust. I would encourage the audience to look at a multi-assurance model to reach people wherever they are and based on who they are, where they are, and what they have access to," he said.

Jeff Greene, director for the National Cybersecurity Center of Excellence at NIST, said even a simple phone call while working from home should be thought of as a “data transfer” requiring zero trust authentication.
“You may need to apply more security to have that kind of chat when you're not within the confines of a secure government building,” he said. “Stopping and thinking and getting people to build that pause in is going to be hard. There is a mindset shift when you can't just walk down the hall and talk with someone.”

Knoieczny said telework is “here to stay” for many Air Force employees, which is why the branch is doing a zero trust demo to enhance its cybersecurity posture.

“We realized people were sitting at home on their own devices and they wanted to get into a high-level-five email that they could not get into,” he said. “We're looking at that risk posture [and] maybe [employing] a graduated risk profile where I may need more authentication information before I go forward. Authentication could be biometric .... I think we're always evolving to looking at risk, and the resiliency of the mission is what we want to maintain."

During a second FedInsider webinar about AI powering zero trust, Education Department CISO Steven Hernandez said the agency has been using AI for intrusion detection and network security.

"Really where we want to be with AI is headed toward this idea of zero trust," he said. "We're building out that architecture."

Hernandez said he hopes AI could help sift data to predict cyber threats before they happen and help the Education Department make more accurate, thorough decisions about how to handle cyber threats and take action more effectively.

"No human in our organization could possibly get their arms around the volume of data we have and make sense of it in real time so we can take action," he said. "In our [cyber] strategy, AI is one of the core components of our defenses."
Standard