COVID-19 Accelerating Federal Cybersecurity Development at USDA, VA

The demands of a remote workforce have put renewed emphasis on instating zero trust and secure cloud access.

Adam Patterson
Thu, 07/16/2020 - 14:27

The transition to a remote workforce has put abrupt and unforeseen demands on federal IT systems, particularly around secure connectivity and use of potentially sensitive information. This has left a strong impetus for government tech executives to instate cybersecurity measures commensurate with the demands of dispersed access.
One of the preliminary steps involved determining exactly what capacities federal employees would need to work remotely, and noting the new IT demands and potential security vulnerabilities this produced.

“One of the first things we all did was make sure we had the capacity in our network and VPN access,” said Venice Goodwine, CISO at the U.S. Department of Agriculture, speaking at the Splunk Cloud Virtual Summit this week.

This led to widespread discussions about how to best understand and conceptualize the broader security space, particularly since the majority of federal employees no longer work within the secure confines of on-site facilities.

“What I thought of as a CISO is that the data is my new perimeter, no longer am I concerned just with those inside the walls of USDA, but what happens with the data that’s being accessed at home by the over 100,000 employees from the Department of Agriculture. How do I address that?” Goodwine said.

Much of the ongoing cybersecurity development across the federal government has rested on understanding that while the essential data security protocols remain unchanged, the technical circumstances have shifted rather drastically. This includes a newfound focus on relying upon the diligence of individual users who may be accessed information remotely.

“From a cybersecurity perspective our mission remains the same — to protect our data and prevent and respond to potential events. It’s just the environment that has changed,” said Paul Cunningham, CISO at the Department of Veterans Affairs. “We rely heavily on users at a scale we haven’t before.”

This has also included a particular vigilance around the evolving threat environment, particularly the novel ways in which malicious actors might use uncertainty around the COVID-19 pandemic to increase the efficacy of phishing attacks.
“We need to be aware of our adversaries as well. They’re going to respond to the environment, and they’re going to change their approaches. For instance we’ve seen phishing, where adversaries still see phishing as a very keen method because it works. They’ve just used what’s in the newspaper — predominantly COVID-19 — as bait. So implementing anti-phishing tools has helped out immensely,” Cunningham said.

Despite the shift to remote access and development of technical capacities to better accommodate a remote workforce, federal CISOs recognize that human security and training remain essential components of rigorous cybersecurity.

“We’ve still got to work on that human element. We’ve got a new environment and new tools, but people who weren’t predominantly used to teleworking are now remoting in — have they been trained, and do they have the good habits to keep our information secure?” Cunningham said.

As a result, federal agencies are moving quickly toward embracing zero trust as a fundamental cybersecurity precaution. This is a development that federal cybersecurity experts appear to realize should have been a greater priority before COVID-19 and are shifting resources toward more comprehensively implementing this across their agencies.

“We were already on a path to start our zero trust journey, and really [COVID-19] just catapulted that. We had a strong ICANN program, we made an investment in understanding what was on our network ... I think I should have accelerated that earlier,” Goodwine said.

As an addendum to this, federal CISOs also seem attentive to the importance of sharing cybersecurity best practices and methodologies across agencies with an eye toward cross-governmental collaboration to more comprehensively bolster federal cybersecurity as a whole.

“There was a national level [cybersecurity] exercise from 2017 when I was at the Department of Energy that talked about pandemics and the lessons learned, and it contained incredible insights. And it went right over our heads," Cunningham said. "We didn’t even fully understand what we wrote at the time, but now we really feel it and have embraced the learnings."
This move toward a consilience of cybersecurity practice has been understood as an important foundation of the simultaneous cloud modernization initiatives ongoing across the federal government, especially considering the increasingly data-intensive work handled by major federal agencies.

“We know that 10 years from now that the technology is going to be way different from how it is today. And it will rely heavily on cloud due to greater capabilities and access reliability. However, we’ll still have cybersecurity elements baked in. So the sooner we can get together organizations and partnerships to expedite [cybersecurity readiness], the better,” Cunningham said.