Federal officials advised agencies to rethink their cybersecurity strategies in terms of data and disinformation.

Kate Macri  
Fri, 09/04/2020 - 15:17

One of the biggest challenges for cybersecurity professionals in 2020 is information warfare and establishing a baseline of trust at their organizations. Criminals and nation-state actors routinely flood the internet with deepfakes and disinformation for political reasons, but can use those same tactics to undermine a federal agency's IT infrastructure and steal information.
“Everything about a modern IT infrastructure has this premise of trust, and information warfare modifies that underlying level of trust until you don't know what's what anymore,” said Chris Johnson, director of the Cybersecurity Operations Center at the National Geospatial Intelligence Agency. “On the government side, we don't think that much about brand management. It's something our partners in private industry are very concerned about and monitor the internet for very specific attacks against their brand, like social media, deepfake videos. That is an aspect of cybersecurity that a traditional cyber defense analyst isn't going to be very well-versed in and pick up on. It's a new discipline we need to start exploring and training our workforce on.”

Chet Wall, technical director for the 688th Cyberspace Wing of the Air Force, said federal security analysts need to dramatically ramp up their critical thinking skills in order to combat cyberattacks in the disinformation era.

“As an analyst you have to be able to not only identify malicious behavior, but also the intent as well to find out exactly what that individual was going after because you can probably identify their next steps in an attack,” Wall said at the FCW event. “It takes a little bit more awareness and knowledge for an analyst to cooperate across the different types of attacks and types of attackers to find out what the intent was.”

Understanding how attackers use disinformation to undermine a federal agency’s cyber defense also helps security professionals use those same tactics against the attackers.

“How we can maybe misinform our counterintelligence aspects by using data in a warfare capacity as misguiding an adversary's TTPs through deception as well?” Well said. “Information warfare is key in all aspects of this.”

The first step is recognizing that the physical perimeter no longer exists. IT infrastructure largely operates via the cloud, especially in the COVID-19 telework era, so cybersecurity professionals need to stop thinking about cybersecurity first in terms of hardware.

“Data is the new perimeter,” Wall said. “Data plus intent is information. We're more mobile; the perimeter no longer exists.”
Maintaining a zero trust mindset could help federal cybersecurity professionals stay on top of evolving cyber threats, but requires constant vigilance and constant learning. What your IT infrastructure looks like today is not a guarantee for what it will look like tomorrow.

“You rarely know or understand your current state when it comes to your cyber infrastructure,” Wall said. “Knowing where all the vulnerabilities are, where access points may be residing. ‘Know thyself’ is one of the first steps in any warfare aspect. Many times we don't do a good job of knowing that [in a cybersecurity setting]. For zero trust, it's understanding where you were before you understand where we're transitioning to.”

Johnson advised federal security professionals to operate from a point of distrust in order to really do their jobs well and keep their networks secure.

“Zero trust isn't something you can go out and buy, it's an ideology for IT professionals,” Johnson said. “It's a commitment across the enterprise. When you're dealing with very very sensitive systems that are interdependent and running intelligence operations, zero trust could have significant implications and impacts for the mission. ... Trust itself is under attack and has been compromised, and our only way to get ahead of the adversary is to treat everything as untrustworthy.”

Because data is the new perimeter, Johnson also suggested data analysts and security analysts work alongside each other in order to maximize cybersecurity efforts at federal agencies. If a federal agency wants to automate a cybersecurity response, for example, the agency must ensure the data providing the automated response is correct.

“You have to go back to the basics — unpacking your data, understanding your data flow, then building the analytics up to support those,” Johnson said. “It's not just about the security analysts anymore. ... We have data analysts sitting alongside cyber analysts to understand the data and adversarial movement with these data sets, to customize better algorithms and better data science to predict what they're going to do before they do it then put it in place before it becomes a problem."