# CDM, Cloud, Zero Trust at the Forefront of Federal Cybersecurity

Leads from innovators and fast followers discuss implementing cutting-edge technologies and practices.

James Mersol

Fri, 07/19/2019 - 13:26


DHS CISO Paul Beckman, SBA CISO Beau Houser, USPTO CIO Jamie Holcombe and moderator James Mersol. Photo Credit: Geoff Livingston

As threats to our nation's networks, data and other critical components evolve, so too have the tools and methods to protect them. Agencies are implementing the continuous diagnostics and monitoring (CDM) mandate from the Cybersecurity and Infrastructure Security Agency (CISA) as well as employing cloud services and the Zero Trust framework to balance user access with network integrity. Department of Homeland Security CISO Paul Beckman, U.S. Patent and Trademark Office CIO Jamie Holcombe and Small Business Administration CISO Beau Houser spoke on CDM, cloud security and Zero Trust at the State of Cyber CXO Tech Forum July 18.

All three panelists said that SBA has been an innovator in linking cloud services and CDM for cybersecurity.

"The perspective from the cloud simplified a lot of [our cybersecurity] challenges," said Houser. "We made the conscious decision to make cloud the central part of our cybersecurity. I'm ingesting over 400 gigabytes of data per day from other cloud services, from on-prem into the cloud … and that allows me to centralize the visibility using big data concepts."

Houser introduced other cloud services from his provider, including endpoint security, to ensure data integrity and network security.

"All that IT management that we struggle with – I don't have to deal with it because my cloud services provider is providing these services, I'm consuming those services, and I can focus on cybersecurity rather than the caring and feeding of all of that infrastructure from a traditional standpoint," he said.

"One of the things that SBA showed us about CDM is that it's not about the tools," said Beckman. "It's about the data. It's about the capabilities. CDM was always supposed to be a capability gap-filler."

DHS initially focused on the tools, Beckman added, once his office shifted to thinking about the data sets they needed to gain visibility of the DHS network.

"It became extremely easy" to design the architecture, he said. DHS and SBA partnered on a pilot program to aggregate those data sources using big data tools.

Holcombe described USPTO as a “fast follower” with regard to CDM and cloud security. “We’re going to move to cloud, but we’re going to do it very thoughtfully,” he said. Enabling teleworking at the agency is especially important, Holcombe added, as 88% of the agency’s employees do so, making USPTO the agency with the highest percentage of teleworking employees.

“We send [our patent and trademark examiners] a SOHO router and a laptop that’s configured, and we only trust those items in our network. We control everything,” he said.

Currently, that architecture is “old and stable”, but as USPTO moves to a hybrid, multi-cloud architecture, he looks forward to introducing new tools, such as AI-enabled patent databases and fraud detection, which will further strengthen the security of the nation’s intellectual property data.

Houser added that for both his teleworkers and those in SBA’s office of disaster assistance, which works with FEMA with on-site disaster relief for small businesses, he wants to use the Zero Trust model to go beyond the traditional VPN-enabled access model.

“We want folks to get internet access however they can get it,” he said. “We’re going to build the software onto the system so that the VPN aspect is invisible to the user.” Instead, users will get access to different levels of SBA’s systems based whether their device or network is trusted.

Beckman highlighted that the foundation needed for Zero Trust architecture is not anything new.

“It’s not a solution that you can just go out and buy,” he said. “These are technologies you already have. These are basic network security principles that have been around for a very long time.”

Best practices like mutual authentication, segmentation and compartmentalization are key to implementing zero trust, and it’s a matter of applying those principles to an identity-based, least-access model, he said.

Holcombe said we must balance security concerns between internal USPTO networks and public information about intellectual property.

“We really have to figure out the public versus private trust issues,” he said. “It’s pretty easy on the private issues … it’s the public side that I’m concerned about. Making sure that everyone has good access, and the performance is very important at that point as well. You can’t disregard the fact that everyone wants that data.” His office is introducing emerging technologies like AI and a blockchain register to monitor access and dissemination.

These security controls protect against the full range of threats, the panelists explained, from advanced persistent threats like Chinese intelligence to malicious or merely accidental insider threats.

“First thing – know your network, understand what’s on your network,” Beckman said. “You cannot protect what you are not aware of … second, patching. You cannot exploit a vulnerability that does not exist.” He recommended that agencies invest in protection before they allocate resources towards detection, and that they should think of security as a multi-stage process.

“You do defense-in-depth until the money runs out,” Houser agreed. “You combine that with a threat-based approach. At SBA, we operate like a bank … so our threat model is similar to the financial sector threat model.” His office employs analysts to track threats to the financial sector, including the common methods those adversaries use to infiltrate financial systems.

Holcombe underscored that CDM not only alerts agencies to threats so that they can defend themselves, but also reports the incident and calls for assistance.

“I need the intelligence community to know what my attacks are,” he said. “We rely on them to ensure that we won’t get attacked again."

View printer friendly version
CXO Tech Forum State Cyber 2019
cybersecurity
cloud
Standard