CISA Cybersecurity Program Head Outlines Capabilities and Priorities

Advances in cloud computing and mobile data require a new approach to protecting federal networks.

James Mersol

Thu, 03/28/2019 - 09:45

LeoWolfert/iStock

Continuously evolving threats, as well as new technologies and capabilities like cloud-based information systems and mobile computing have spurred the Cybersecurity and Infrastructure Security Agency in the Department of Homeland Security to rethink its approach to continuous diagnostics and mitigation (CDM).

Planning to protect government data, especially high-value assets, requires working on multiple aspects of CDM at once rather than focusing on one part at a time.

“We started out with the idea that this was going to be a phased approach,” said Kevin Cox, the CDM program manager at CISA, at the 2019 RSA Federal Summit in Washington, D.C. Tuesday. “What we found is that the threat is constantly evolving, the technology is constantly evolving, and so we’re really dealing with capabilities and working to make sure that agencies have all the capabilities that they need in order to protect their data, protect their environments and ensure that their missions are secure.”

Despite the shift from phases to capabilities, Cox said the four main components of CDM have not changed: asset management, identity and access management, network security management, and data management. These components will be visible to each agency through a dashboard that tracks the data and alerts agencies’ individual CDM program managers if the diagnostic tools detect an intrusion or other suspicious activity.

The agency-level dashboard is a level below where Cox envisions federal CDM architecture will go in the next couple of years. CISA is planning a “federal dashboard” to greater integrate CDM. This dashboard is still in conceptual stages, and Cox anticipates DHS will issue the contract to build it in May.

For now, Cox is focused on ensuring that the diagnostic tools and sensors are integrated into agencies’ systems so that data is standardized, searchable and understandable. “There is a vast amount of value in the data that’s feeding up from these sensors,” Cox said. “It’s not just security value. It’s operational value. It’s awareness value. We really want to expand what the agencies will be able to do there.”

Cox recognized additional technological changes for which CISA must plan. “You get out into the internet,” Cox said, “and then you have different infrastructure platforms, software-as-a-service environments, your remote users, your peer-to-peer connections in different agencies, as well as your mobile environment.”

As agencies move away from the old model of networks and data located on and only accessible from the premises (referred to as “on-prem”), all of the above represent changes in the way CISA has to think about data security and CDM.

One of the biggest changes is the transition of federal data to the cloud. The National Cybersecurity Protection System, also known as EINSTEIN, provides capabilities for intrusion detection, tracking, analysis and protection on current federal networks. As government agencies transition their data to more efficient and cost-effective cloud-based systems, CISA will need to update EINSTEIN or create a version of it designed to work in the cloud, recognizing that the architecture is fundamentally different from an on-prem network. CISA is partnering with cloud service providers now so that CDM tools are more integrated and effective throughout the process.

“We’re essentially baking in security from the start rather than having to nail it on later,” Cox said.

Mobile data represents another challenge for CDM. “Most agencies have mobile device management systems in place” to track user logins and manage their mobile assets, according to Cox. However, as CISA looks to protect mobile data, it will look to private sector partners to develop and implement mobile threat detection systems that report that data to the agency dashboard.

With data technologies evolving so rapidly, CISA cannot issue a plan that will take years to implement if it does not allow for adjustments that recognize shifts in technology. In the short term, it will use CDM Dynamic and Evolving Federal Enterprise Network Defense (DEFEND) task orders to bring in new services through the acquisition process as needed. There are currently five CDM DEFEND task orders in place, each with a six-year term.

“Because of the length of time, we weren’t looking to define all of our requirements up front,” Cox said. “We needed a mechanism to stay flexible and to be able to bring in new technologies to address new requirements, and the way we do that is with our request for service process.”

CISA has partnered with the General Services Administration Federal Systems Integration and Management Center to keep ahead of any emerging technologies and issue a request for service when the DEFEND task order calls for it. The first requests have focused on data protection and high-value assets.

“We’ve been working with the agencies to understand the systems, understand the data and look at the right solution to protect that data,” Cox said. “In some cases, that’s additional encryption; in other cases, it’s data loss prevention. There’s going to be some HVA environments where data or information rights management makes sense [or] re-architecture makes sense. But we have started on the first of these efforts to really lay the groundwork.”

View printer friendly version
Federal Cybersecurity
Department of Homeland Security
cloud computing
Standard