'DevOps Is Security': What Federal Agencies Can Do to Boost Cybersecurity

CISA and NSA provide guidance for how federal agencies can address critical vulnerabilities in their networks.

Kate Macri
Thu, 07/09/2020 - 10:39

The Department of Homeland Security wants federal agencies to have constant real-time visibility of all nodes on their networks — whether they be devices, routers or servers — but in order to meet that goal, cybersecurity professionals need to work closely with developers to catch vulnerabilities before they happen.
Constant real-time visibility is even more important during the age of COVID-19 when most federal agencies are working entirely remotely, said Cybersecurity Infrastructure and Security Agency Program Manager for Continuous Diagnostics Mitigation (CDM) Kevin Cox at a Nextgov event this week.

“We're helping agencies answer questions like: what is connected to their network, who has access, what's happening,” he said at the event. “We help them get sensors and scanners out on their network to identify each and every node and get a handle on their access management for all their users and their activity on their network, whether that be on the network or the perimeter, activity out in the cloud or a mobile device.”

CISA’s goal is to make all that data available on agency-specific dashboards for agencies to use and also on one master federal dashboard for federal leaders to use.

“We want agencies to get a better understanding and a real-time understanding of what's happening on their network,” Cox said. “We put it on an agency dashboard where they have object-level and data-level views to see down to a particular endpoint or vulnerability and update that to the federal dashboard so federal leadership has an idea of what the federal landscape looks like, what critical vulnerability [there is] and where it resides across agencies.”

Cox said CISA looks at two metrics with this program: one evaluating how well agencies are gaining real-time visibility and another evaluating how many nodes each agency has.

“We found there were 75 more more assets than were manually reported [across agencies],” Cox said.

Once an agency obtains clear visibility of its network, they can use CISA’s AWARE Algorithm to ramp up their cybersecurity efforts.

“Now that we're starting to operationalize the tools we need to help them better understand the attack surface, we're in the process of rolling out the AWARE Algorithm agency wide,” Cox said. “It's going to help agencies understand where their biggest issues are and fix the worst problems first over time.”
Agencies’ first security priority should be protecting “soft targets” by making the easy fixes and patches before moving on to protecting “hard targets,” even though “hard targets” are more valuable to hackers.

“They're going to go where it's easy to get in and where they need to spend less resources,” Cox said. “We know when a critical vulnerability is hit, our adversaries are aware of them even faster than we are, and when an exploit becomes available for that critical vulnerability, they're going to use that to get into our system. So how are you tackling critical patches versus non-critical patches, and how quickly are you working to take care of the critical patches first?”

But agencies can’t really know where their vulnerabilities are until they gain real-time visibility of their network. That’s why taking inventory of all nodes and deploying sensors and scanners across the network is paramount.

“Once we get the sensors and scanners out there and bring the data up to the agency and federal dashboards, it's only as good as the data being reported,” Cox added. “We need to make sure the data is reflective of what is down on the ground. One of the key things we've had to do is build partnerships with the agencies and really build up the trust that when the data gets to the dashboard they'll be able to use it, and the federal team is going to work with agencies to get the problems fixed, not come down with a hammer and say, why isn't this getting fixed?”

National Security Agency DevOps Security Lead Emily Fox said cybersecurity professionals should work with developers to prevent vulnerabilities before they happen.

“Make sure your security folks understand where they fit in that cross functional team, a lot of them get a little lost,” she said at a DevNation Federal event this week. “We want them to be side by side with those on the development team, they should be there to answer any and all questions, and they should be curious in learning about how the product works.”

As federal agencies move away from the waterfall code method, cybersecurity professionals need to understand how that changes the relationship between them and developers.
“As we're moving forward and migrating into the cloud and adopting these new architectural designs ... you've changed how developers really function,” Fox said. “The struggle for some security professionals is they're so used to waterfall and this giant chunk of code being dropped on their life [to test], and now developers are saying, we're going to release code 100 times a day and security professionals are like, what, I'm not going through all that code, that's crazy.”

Each federal agency needs to figure out what works best for their security professionals and break down testing into prioritized, manageable bites of work instead of asking them to run tests all day.

“It depends on the mission and risk of the organization,” Fox said, adding that you'd typically expect a lot of testing to be done on the locks to your house, for example. “If it's a lock on your cabinet and you don’t have any kids, it’s probably less important to test that lock. But if it's the lock to your house, you want to make sure it's going to lock when you need it to and unlock it when you need it to. It's context-dependent.”

Both Cox and Fox said federal agencies should be mindful of their IT contracts with the private sector. Agencies should bake the right language into their contracts regarding penetration testing and visibility in order to ensure maximum security.

“Part of what is critical is when an agency is moving to the cloud, they negotiate the right clauses into the contract with the service provider to help that agency get the visibility they need,” Cox said. “They may not be able to get all the visibility they'd like, but it doesn't hurt to push as hard as they can so they can get an understanding at any point in time how protected their data is out in the cloud.”

Some agencies’ cybersecurity strategies are in better shape than others, which also means information-sharing across agencies is important. CISA is already working on a shared-agency platform to help agencies increase visibility across the board.

“Security professionals: what you need to learn is be progressive and open to learning,” Fox said. “Security is not a dirty word. DevOps is security.”