CISA Advises on Cybersecurity Strategies During the Pandemic

With phishing and the upcoming election, securing infrastructure remains a top necessity that initiatives like TIC 3.0 will advance.

Kate Macri
Thu, 07/02/2020 - 13:02

The Cybersecurity Infrastructure and Security Agency (CISA) had its hands full since the start of the COVID-19 pandemic — helping agencies secure their networks during the mass shift to telework and dealing with more than 7,000 fraudulent domains of the Department of Health and Human Services’ website.

CISA officials are advising on its cybersecurity strategy going forward and its ability to help federal agencies protect critical infrastructures while working remotely. With its core priorities being nation-state activity, phishing, ransomware and
disinformation, the agency is advising on not only coronavirus-related phishing scams, but also election security, noted CISA Deputy Assistant Director for Cybersecurity Richard Driggers.

“With regard to phishing attacks, we've seen scammers really capitalize on the pandemic to trick people into revealing personal info or malicious software,” Driggers said at the 2020 Virtual Cybersecurity Summit last week. “Hospitals have been targeted really from 2017 to 2019, and they've reported half of all ransomware attacks in those two years.”

Foreign governments are also targeting the U.S. health care system.

“Nation-state adversaries have shown an increased interest in COVID-related vaccine development, lab data, research, anything that's going to get the U.S. and the world to a treatment for COVID,” said CISA Assistant Director for Cybersecurity Byran Ware in a conversation with Federal News Network this week. “We've seen not just China, but others target the U.S., both governments and universities and health companies and private companies.”

Driggers said CISA is working with the FBI to “launch a couple of efforts” in the next couple of months “that will not only meet these attacks head on, but include strategies” for combatting them.

“We've shifted our focus to really hone in on the health care sector,” Driggers said. “We also have tech services from vulnerability scanning to malware analysis. We have a vulnerability scan called Cyber Hygiene. It's an automated remote scan, and we issue a report identifying vulnerabilities on devices you have connected to the internet.”

Sean Connelly, TIC Program Manager and Senior Cybersecurity Architect at CISA, said shifting government agencies and the private sector from Trusted Internet Connections (TIC) 2.0 to TIC 3.0 is another big priority in order to ramp up cybersecurity efforts, especially as the coronavirus pandemic continues.

“TIC 3.0 is really a gamechanger from where we were with TIC 2.0,” he said at the 2020 Virtual Cybersecurity Summit. “When the pandemic hit and we saw this enormous surge in telework, [government agencies] really wanted to explore new ways for their employees to get to their data.”
As government agencies and private companies continue to work remotely, infrastructure vulnerabilities that may have been low priority before — like VPN security, for example — now must be key priorities.

“In January, your VPN may have seen a small fraction of your overall business activity, but that's completely different today. You may be relying completely on your VPN,” Ware said.

Connelly said CISA plans to release core guidance documents detailing TIC 3.0 best practices sometime this summer and then move on to collecting best use cases in the government community.

“When we do that, we will then distill lessons learned from those pilots and release those use cases out to the greater community,” Connelly said.

Zero trust architectures are extremely important for government agencies and the private sector during this time, Connelly added at an IBM ThinkGov conference this week.

“Workers, resources — they're becoming increasingly distributed,” he said. “The concept of a traditional network perimeter is dissolving. We used to have fixed desktops, fixed networks, but now look where we are in the last few months even, entirely new networks on entirely different platforms. Zero trust is an ideal solution that can help make those architectures secure, a distributed architecture where data is no longer on a homogenous network.”

As government agencies make the shift to TIC 3.0, they must embrace a zero trust mindset about cybersecurity.

“Zero trust is not about ‘set and forget,’ and that's really where we were with TIC 1.0 and 2.0,” Connelly said. “With zero trust, agencies have to be much more proactive and understand what is happening with their resources. TIC 3.0 guidance encourages agencies to use trust zones and group network components and requirements. You still have to trust something, the data, the app or the user. You have to reestablish that trust all the time. Zero trust has a half life. Trust has to be continually reestablished, and [you have to] build security capabilities closer to the data.”

In addition to adopting cybersecurity best practices, Ware said cybersecurity will
only improve if CISA, government agencies, and the private sector get better at sharing information with each other.

“It still has been incumbent on us and a real focus of ours to make sure we have more two-way exchange, and a lot of time that really just means bringing people together,” he said in his conversation with FNN.

The private sector is often more aware of cyber threats than the intelligence community, he added, which further complicates CISA’s mission.

“There is more threat intel coming from commercial sources than classified sources, and it's often coming faster because of the speed of industry, but also things like classification just slow things down,” Ware said. “We are working all the time with our intelligence community colleagues to downgrade things as quickly as we can to get things out so people can respond to an emerging threat.”

CISA has a three-pronged approach to cybersecurity for the rest of 2020 in light of the pandemic: working toward real-time visibility across all devices, rethinking the way CISA delivers products and services, and making “significant investments” in the cloud.

“We’re adjusting the way tools work, the way the relationships work, the way the authorities work. These are not profound adjustments, but they're adjustments so we can get to the place where we can see the threat across an entire landscape and do a better job of controlling the responses,”Ware said.

To improve CISA’s products and services delivery, CISA’s Quality Services Management Office (QSMO) is working closely with Federal CIO Suzette Kent.

“I think what we're going to get out of that is efficiencies, better alignment across government, working with the vendors of those products and services to make sure we can use the data effectively on the back side to get to that better visibility,”Ware said.

As government agencies and the private sector continue to migrate to the cloud, CISA wants to be ahead of the curve. Really good IT, Ware said, minimizes cybersecurity risk.

“We can't lose visibility,” he said. “We need to do a better job internally of leveraging all the data holdings we have so that we can be a more nimble, more
agile hunt-or-response organization so we can deliver insights to our customer base. We need to build and deploy a very secure cloud and maintain and monitor our activity and all the rest of the government’s activities in the cloud and really leverage the analytics to deliver a better mission performance from a speed perspective, but also unlock the amazing quality of our analysts delivering top notch security results to the .gov community and beyond that.”