Increasing Infrastructure and Supply Chain Security at FBI, USCIS, Air Force

Cybersecurity leaders across government point to penetration testing as a solution to identifying many IT vulnerabilities.

Abigail Blue

Mon, 07/22/2019 - 07:13

GovernmentCIO Media & Research President Michael Hoffman talks with FBI Senior IT Security Adviser Manuel Castillo, USCIS Cyber Defense Branch Chief Adrian Monza and Air Force CISO Wanda Jones-Heath. Photo Credit: Geoff Livingston

Perspectives from federal agencies that secure some of America’s most high-value assets revealed that although agencies may agree on methods or best practices for dealing with cybersecurity threats, their approaches are not all that similar.

The U.S. Citizenship and Immigration Services' latest modernization effort is bringing software supply chain attacks to the forefront of cybersecurity threats. Software supply chain attacks are an area of concern for the agency, said Adrian Monza, USCIS Cyber Defense Branch chief, as it incorporates open-source technologies and transitions to a digital immigration processing system called "eProcessing." Monza spoke with other panelists at the GovernmentCIO State of Cyber CXO Tech Forum July 18.

“One of the challenge points, just looking at what’s going on in the larger ecosystem, is the susceptibility of software supply chain attacks," he said during the panel. "We’ve seen these things occur in a number of different areas, typically more focused on financial type crimes, but I think it’s only a matter of time before someone gets the bright idea and says, ‘hey, you know, this is a great way into government systems as well.’”

According to Monza, in order to better understand your software supply chain it is important to ask, “What modules are our developers using [and] what are those dependencies?”

Senior IT Security Adviser for the Federal Bureau of Investigation Manuel Castillo shifted the conversation on supply chain to include not only hardware and software, but also the services purchased from third-party vendors.

“The way that when the FBI looks at it, you have to manage it," he said. "It’s a risk.” The FBI has to determine what its risk appetite is, he added.

The U.S. Air Force has its own model with a certified infrastructure and certified process to strengthen security. CISO Wanda Jones-Heath discussed the branch's Kessel Run project, which uses penetration testing and other innovative tools.
It hardens the Air Force infrastructure by means of a “direct process to ensure that you are developing, testing, developing, testing all at the same time,” she said.

The model has been successful so far in “producing a lot of good outputs” and will be implemented in other services, including the Army and Navy. It is also continuously improving, as the Air Force discovered some gaps and vulnerabilities in the model and is in the process of closing them.

Jones-Heath explained much of the Air Force’s success with penetration testing. She referenced Air Force CIO Bill Marion, who found that “the paperwork, when you go through the traditional process of risk management, it’s just not catching all of the vulnerabilities that [they] know are out there.”

Penetration testing has been able to find the bugs and vulnerabilities that slip through the “paperwork-checking” cracks. The Air Force has found offering bug bounties, as part of its Hack the Air Force program, to be particularly helpful.

Monza echoed Jones-Heath regarding penetration testing. “I will tell you that the results that we’ve seen from that have been just illuminating," he said. "Things that in the paperwork it says … we fixed that, well, maybe we mostly fixed that.”

Penetration testing has given USCIS a better understanding of what it should be focusing on and where the control areas are that have weaknesses, Monza added. His team of penetration testers, or “semi-tame hackers” as he refers to them, has been extremely creative in its methods. The testers have highlighted new ways of getting into a system that the Cyber Defense Branch had never seen before.

Their skills have also been put to the test and utilized in the "internet of things" space as new equipment has been acquired. “A couple of times, we’ve actually identified serious vulnerabilities for the manufacturer, which we then worked with the manufacturer to responsibly disclose to them and retested, and they were resolved,” he said.

Castillo felt that the testing practice is somewhat overhyped and that it is only effective if the vulnerabilities it identifies are subsequently mended.

“One of the issues that I have seen in over 20 years, it’s if you don’t know what you have,” he said. “If you don’t know what you have in the machines, and you’re not patching and fixing [the] vulnerabilities, you’re really not doing a favor to your organization.”

The panel concluded with a brief discussion of risk management. Monza addressed the inherent risk associated with the use of legacy systems.

“Just by moving to a more modern code base, by moving to modern development practices, that inherently is going to help us buy down a lot of risk," he said. "It’s important to also look at what’s the risk of what you have, not just what’s the risk of what you’re moving to.”

At USCIS, the belief is that a job is not completed until the old system is unplugged.

View printer friendly version

CXO Tech Forum State Cyber 2019
risk management
Federal Cybersecurity
infrastructure
software
cyberattacks
Air Force
USCIS
FBI
Standard