Every Federal Agency Should Think About Securing the Supply Chain

Cybersecurity basics and risk management are key elements of IT supply chain security.

Kate Macri
Fri, 10/09/2020 - 13:51

The lines delineating IT supply chain security from cybersecurity and infrastructure protection are blurrier than ever, so federal agencies must consider all three together as part of a whole.
“It's almost impossible to look at them as separate disciplines at this point,” said Daniel Kroese, associate director of the National Risk Management Center at CISA during GovernmentCIO Media and Research's virtual event this week. “We're really just talking about the existing principles of cybersecurity and infrastructure security with a third-party trust and assurance lens on it. It's a layer on top of what we have already done.”

In a panel on IT supply chain security, Kroese and Dell Federal Cybersecurity Practice Manager Dan Carroll discussed the ways in which the software and hardware supply chains impact a federal agency’s cybersecurity and risk management.

Since federal agencies increasingly rely on commercial, off-the-shelf software applications — and many of those applications rely on open-source code — it opens up a broader attack surface for government agencies.

“Software represents a potentially concentrated source of risk if you don't have the vulnerability management and acquisition strategies around it,” Kroese said. “We're working to deploy a series of tools across government agencies, but also private sector partners in the critical infrastructure community to do this supply chain analysis so that if there are vulnerabilities ... we can track it, understand where it is and patch that swiftly.”

Carroll said accountability and collaboration are key for federal agencies and private-sector suppliers looking to secure the software supply chain.

“The realization that I have an organization, I have a number of people focused on protecting my software, is dwarfed by the number of people who want to exploit my software,” he said at the event. “The big part of a secure supply chain is secure development; a secure development lifecycle that is well defined.”

One of the ways federal agencies can vet their software is by adopting a zero trust approach.
“As we're continuing to mature, you're looking at these emerging security models like zero trust where you're not just validating software when it's developed, but when it boots up every time and as it transfers layers through the service model,” Carroll said.

Zero trust is an innovative cybersecurity approach uniquely positioned to address supply chain risk because it requires federal agencies to constantly validate access points on its network (like software applications). Under a zero trust mindset, even an open source-based software application can be validated under the proper protocols and conditions.

“If you're starting from the standard of zero trust, it means recognizing how just one bad click or one malicious line of code can set off a cascading set of events that can have enormous damage to not just your enterprise but other organizations, national security, public health and safety,” Kroese said. “You need to bake in security on the front end so it's easy to localize.”

Federal agencies also need to recognize how tightly intertwined the software and hardware supply chains are. The 5G network, for example, will be defined by how the software influences the hardware, Kroese said.

“Before you would have physical switches and lines in the ground, and now a whole host of functionality is now controlled by software when before it was the physical arrangement,” he said. “You have the software that enables the firmware capabilities. What if those monthly software updates introduce more vulnerability to the system? It's really hard to differentiate the line between where the software ends and the hardware starts.”

In a rapidly digitizing federal environment, some federal agencies may face numerous challenges to securing their IT supply chains because there are so many moving parts they cannot control, like shippers, third-party logistics providers (3PLs), and Tier 2 and 3 suppliers.

When international shipper Maersk faced massive cyberattacks a few years ago, Kroese said, some of the biggest victims were downline members of the supply chain, like pharmaceutical manufacturer Merck and FedEx, a 3PL.
“Federal agencies need to “model out some of this connectivity so we can see how something over there impacts something over here,” he said.

“When people think about technology they tend to think about the tech in front of them, not understanding there are layers and layers of software under that like Windows 10,” Carroll added, “and they come from lots of different sources. The system is not made by one company. ... Being able to come together and create trust and protect against things like insertion, unintentional or malicious, is key.”

Federal suppliers may need to start thinking of themselves as IT companies in order to maintain the right mindset about cybersecurity, supply chain risk management and infrastructure protection.

“Everybody in some capacity in this day and age whether they like it or not is an IT company,” he said. “You may be a bank and don't want to be an IT company, but you still need to protect all that data. You may ship boxes but you're right, you have tons of customer data and credit card data and you need to protect all that data.”

For federal agencies looking to ramp up their security strategies for IT systems and supply chains, Kroese said the first place to start is with the cybersecurity basics: patching, continuous monitoring, validating access and scanning for threats.

“Basics still very much matter,” he said. “Innovation is great, but don't let it be a crutch to not do what you need to do today and now.”