Intelligence Leaders Look to Secure the Supply Chain from Beginning to End

Protecting the nation's critical mission systems requires support from everyone involved.

James Mersol

Wed, 04/03/2019 - 17:31

rkankaro/iStock

Federal agencies are concerned that gaps in security and threat monitoring create vulnerabilities for the contractors who build, operate and maintain information systems for the government, and those vulnerabilities in turn create risks for entire government networks. Rather than task any one office or organization with identifying and closing these gaps, improving supply chain security will require an effort from everyone involved in the process.

At the Intelligence and National Security Alliance's Supply Chain Security Breakfast Monday, marking the start of National Supply Chain Integrity Month, Bill Evanina, director of the National Counterintelligence and Security Center, encouraged all cybersecurity professionals to read the Secretary of the Navy's Cybersecurity Readiness Review.

He quoted from it to underscore his concerns about mission-critical systems: "The systems the U.S. relies upon to mobilize, deploy and sustain forces have been extensively targeted by potential adversaries and compromised to such extent that their reliability is questionable."

Repairing the Weakest Link – A Whole-of-Organization Approach

In keeping with the supply-chain analogy, a common focus for improvement is the "weakest link" – the contractor or office that has had the least training in security or counterintelligence and is, therefore, most likely to become the target of information breaches and other attacks.

"Those weak links are in our acquisition and procurement communities … whether you're government or in the private sector," Evanina said.

Acquisition professionals are charged with choosing the vendors for government hardware, software and services, yet are rarely, if ever, included in conversations about security. Moreover, they receive no counterintelligence or cybersecurity training outside of the basic employee training, which does not include how to vet vendors for potential security risks or active threats.

"I would start simple," Evanina said, when asked about possible changes for procurement and acquisition. "If you're in a procurement and acquisition role, [you should have] mandatory minimum training, like one hour a year of understanding what the threats are, what the vulnerabilities are and what the intent of our adversaries is."

Some agency cybersecurity leads have expressed concerns that it is difficult to get many organizations to bolster their security without showing the return on their investment. At the RSA Federal Summit March 26, Matthew Scholl, deputy division chief for the computer security division at NIST, explained what happened when he approached a utility company with a plan to improve its security.

“The first question they asked me was, ‘How many customers will we lose this year to cyber?’,” Scholl said. “They know how many customers will be affected by downed power lines, and that’s how they plan how many chainsaws to buy in a given year.”

A solution some officials have proposed to this disconnect is to integrate security into every other business function so that public and private organizations will stop treating it like an add-on cost.

“The only way I believe we can [fix the weak links] is through a very sound enterprise-wide security process … that means the cost is free,” Evanina said. “If we make security part of mission, the counterintelligence piece will take care of itself.”

Others have proposed that cybersecurity professionals should frame improvements in terms of their organizations’ interests.

“Cybersecurity is not the most important thing,” Scholl said. “It is a supportive element to a business. Everything we keep talking about here is about protecting the business’ most critical asset, which is usually data.”

Evanina and Scholl’s comments indicate that both public and private organizations need to treat cybersecurity as essential protection for their assets, which in turn are essential to their missions. This approach should foster cooperation between information security executives and their counterparts in the c-suite.

“Have a cup of coffee once a month with your CISO, your CIO, your CSO, your head of human resources and your head of procurement and acquisition,” Evanina suggested. “Have them meet … to talk about what it means from an enterprise-wide perspective to understand the threat factors your [organization] faces.”

A Whole-of-Nation Approach

Agency security program leads and experts in defense and intelligence agree that no one department, office, company or team can accomplish cybersecurity on its own. Instead, it needs to be a nationwide effort, including the private sector, government agencies and the public.

“2018 was a horrific year for us with respect to the arrest and indictments of insider threats,” said Evanina. “In the private sector, over 20 individuals and companies from China alone were arrested or indicted by the FBI and [Department of Justice]. Inside the government … we had a U.S. citizen with a clearance plead guilty to committing espionage on behalf of China and it had almost no news. What hurts us every day as a country becomes numb … we cannot become numb.”

Beyond raising awareness, improving supply chain integrity requires adjustments in public-private partnerships. For example, when assessing bids for government contracts, government acquisition officers could give “extra credit” to companies that demonstrate that they have implemented an enterprise-wide approach to security or otherwise integrated security into their supply chain.

Improving supply chain integrity also requires examining previously overlooked parts of the chain. “Heating, ventilation and air conditioning (HVAC) is the most critical part of keeping the servers cool and the data clean.” Evanina said. “When [the server company] built that farm and hired that HVAC company to cool that facility, were they thinking about security or counterintelligence threat vectors from our adversaries in the supply chain?”

This effort also requires ongoing monitoring. Organizations carefully evaluate contractors responsible for developing a product or building a system, but do not apply the same scrutiny to those maintaining the system or supporting a program, Evanina said.

“Supply chain comes in all colors, all shapes, and all sizes,” Evanina said. “We have to have the right individuals to talk about the metaphors, analogies, mitigations, the best practices and the worst-case scenarios.”

View printer friendly version
cybersecurity

partnerships
national security
NIST
Standard