CISA Seeks to Define Risk for Industrial Control Systems

Associate Director for Cybersecurity Jeanette Manfra outlines the three pillars for ICS security.

James Mersol

Tue, 05/21/2019 - 17:14

ipopba/istock.com

In the six months since the Cybersecurity and Infrastructure Security Agency Act established CISA, the agency has made great strides towards coordinating election security improvement ahead of 2020 and strengthening the nation's networks and sensitive data against malicious intrusion. Less visible, but no less critical, are CISA's efforts toward industrial control systems (ICS) security —

the protection of the systems that control critical infrastructure and manufacturing throughout the United States. Assistant Director for Cybersecurity for CISA Jeanette Manfra outlined the three pillars of ICS for CISA at Hack the Capitol 2.0 May 15.

Manfra said she sees her role, and CISA's purpose more broadly, as filling a hole on critical infrastructure defense. CISA's goal is to build partnerships and take concrete actions to mitigate risk, rather than influence policy or create regulations. Understanding the threat to critical infrastructure is important, she said, but it's even more important to understand the risk-critical infrastructure faces.

As part of the initiative to define that risk, she also discussed the National Critical Functions set that CISA published earlier this month. The release is the first stage of defining risk and augmenting protection for CISA, Manfra added, without publicly releasing any information that adversaries could use to exploit these functions.

The first pillar of ICS protection is working with industrial partners to share information and learn from past examples to warn potential future victims. As they examined compromised business systems, CISA learned two things.

“We started to uncover the fact that they were exploiting business relationships,” Manfra said. “We're able to identify other potential victims.”

CISA also began to understand how attackers moved within a system.

“We knew that they were trying to find a way to jump into an operational system [from a business system],” said Manfra, adding that this sort of jump is currently difficult to detect and presents a new challenge for CISA to confront. “We've got a couple of proofs of concept going on how we sense and protect against adversaries in that space.”

Those proofs of concept lead into CISA's second pillar of ICS protection — developing new detection and response technologies and methodologies. CISA wants to incentivize its private-sector partners not only to develop an early warning system against ICS intrusions, but also to consider an efficient, low-cost solution.

“Zillions of dollars have been invested for how we sense adversaries on our phones and business networks,” Manfra said. “How do we drive new technologies that are something people can afford because they don’t have those billions of dollars to drop on fancy cybersecurity technologies?”

She hoped that further communication and partnership among CISA, industrial partners and cybersecurity partners would encourage innovation toward an affordable system.

The third pillar is applying the idea of a cyber kill chain — that is, the steps attackers take in a malicious intrusion — and defense in depth to ICS. In the past, federal cybersecurity experts have recommended air-gapping ICS and any system with critical data to mitigate the risk of an attack, but “that’s just not relevant advice anymore,” said Manfra. Now, companies should start by knowing whether their systems are connected to the network — and what network they are connected to — followed by understanding the data contained on ICS and other critical systems.

These three pillars come down to one goal for CISA, said Manfra. “We have got to have much more capability to prevent the attacks from happening,” she said. “Or at least [we have to] detect them quickly so we can stop them and mitigate those consequences.” Further understanding ICS vulnerabilities and where the greatest risk lies are the next task for her team, she said.

However, partnering with the private sector to better understand risk in ICS is just the first step in a long process toward greater ICS security, said Manfra.

“A lot of these ideas are still top level,” she said. “We know we’ve got to add greater value to the community. We’re going to be talking to [everyone involved in ICS] to understand: are these the right things [to focus on]? Where [are] the technology and the policies and the processes that we can improve on?”

CISA will be an equal partner in this process. “Know that we come to this partnership very humbly,” she concluded. “This is a very difficult challenge.”

View printer friendly version
DHS
cisa
industrial control systems

cybersecurity

Standard