Complacency is the Death Knell of Cybersecurity, CISA Warns

Resources and talent only go so far if you're not aware of which systems are most vulnerable and still clicking on phishing emails.

Kate Macri
Wed, 08/12/2020 - 11:52

The biggest roadblock to developing a strong cybersecurity posture at federal agencies isn't resources or talent — it’s complacency.
Federal agencies need to “get back to basics” with their cybersecurity strategies and practice vigilance and consistency, senior officials from CISA, the FBI and the National Counterintelligence and Security Center (NCSC) said. Patching systems and not clicking on phishing campaigns, they added, are some of the most basic and important things a federal agency can do.

“The inability of us as Americans to not click on links from a phishing campaign is really problematic,” said William Evanina, director of the NCSC, at a FCW cybersecurity workshop this week. “When we see the amount of [cyber criminal] activity occurring, it's depressing.”

Federal agencies are especially vulnerable right now as they telework en masse and face unprecedented administrative challenges due to the pandemic.

Tonya Ugoretz, deputy assistant director of the FBI’s cyber division, reminded workshop attendees of the recent cyberattacks on universities and hospitals involved in COVID-19 vaccine research and development.

“Criminals in particular look at things like natural disasters or well-intentioned efforts like government relief packages and see opportunity, they see vulnerabilities and they look to take advantage of those,” Ugoretz said. “It's important not to become numb to this activity. It's asking a lot of our universities at the same time they are grappling with how do they return to educating their students and conduct this cutting edge research, that they are also expected to be fending off highly sophisticated cyber activity.”

Daniel Kroese, associate director of CISA’s National Risk Management Center, thinks federal agencies face a twofold challenge to improving their cybersecurity posture.

“On one hand, we still need to do the basics better,” he said at the workshop. “The patch management, the blocking and tackling. Unfortunately we've seen a spate of ransomware activity across the country, [and organizations are] getting popped because they weren't deploying 10-year-old security best practices. This is no longer acceptable in this day and age, so the basics very much matter.”
Federal agencies also need to forget about a “one-size-fits-all” approach to cybersecurity, and instead tailor their cybersecurity strategies according to the vulnerabilities of their systems and critical infrastructure.

“We also need to aggressively enhance our understanding of the analytic science behind cyber risk management,” Kroese said. “It's about deconstructing the risk equation and adding analytic rigor. True cyber risk management is much more than just patching your stuff.”

When evaluating cyber strategies for different systems, Kroese said federal agencies should ask themselves, “What is the criticality of those systems? If those systems go down, is it a really bad day for the nation? If this thing fails, how easy is it to remedy this problem? Not everything has the same level of impact if it fails.”

Federal agencies need to focus on identifying “concentrated sources of risk,” Kroese added, in order to prioritize cybersecurity measures.

“This is our north star here as we invest in this cyber risk management capability,” he said. “when you're engaging in concentrated risk that's where you have more risk management bang for your buck.”

CISA is working with NTIA and other private sector partners to work to develop software materials and binary analysis tools for federal agencies and private companies with critical infrastructure, like the energy, telecommunications and financial sectors, Kroese said.

Using these tools could help the public and private sectors concentrate their cybersecurity resources more efficiently, and keep them from growing too complacent about the security of their most vulnerable systems.

“Once there's a bad line of code, it's kind of like a pandemic,” Kroese said. “It's so hard to trace it back to patient zero and put it back in the box.”