'Software Is Still Hard': Maximizing Security While Shifting to the Cloud

Best practices leverage agility for keeping data secure as federal agencies move away from legacy IT systems.

Kate Macri
Thu, 08/27/2020 - 15:17

To enable a streamlined, safe and secure shift to the cloud, federal IT leaders need to do three things: maintain network visibility, implement a strong credentialed access policy, and build out a human-centered design approach to the cloud.

“Visibility is where security is going to start,” said Cybersecurity and Infrastructure Security Agency (CISA) Chief Technology Officer Brian Gattoni at a FCW FedRAMP summit this week. “If you can't see it, you can't protect it.”
"Security comes through visibility," said Defense Digital Service Director Brett Goldstein. “Honestly, software is still hard. We don't like to admit it. In all sectors, writing high-quality, low-bug software is hard. Every time you write it and recreate it, you're creating new surface areas (for attackers). We need to decrease independent projects, push reusability. ... That's one of the principles behind the cloud.”

Federal agencies must understand telemetry requirements when shifting to the cloud. Tools like CISA's Continuous Diagnostics and Mitigation (CDM), for example, can help federal agencies make the most of cloud security.

"[We bring on] security orchestration and automation and automated response capabilities, hook them up to the tools to find out who and what is on your network, then we extend that capability to the cloud to ask the same questions, then possibly start sharing playbooks the types of analysis or analytics to quickly respond to the same threat even if it's coming through different vectors," Gattoni said. “They're going to help bring standardization [to federal departments].”

Lance Cleghorn, a digital services expert with the Defense Digital Service, warned federal agencies against complacency when evaluating cloud security.

“There's this huge gulf between being compliant with policies and being secure,” he said at the summit. “I don't think I can overstate how awesome it is to engage the research community while building out cloud infrastructure and get all these unique perspectives on your solution.”

New tools like artificial intelligence, machine learning and automation can help security analysts sift through data to find vulnerabilities and threats, Gattoni added, but shouldn’t be treated as catch-all security measures.

Complacency is still the biggest threat to secure clouds, and federal developers need to be “hungry to learn,” Cleghorn said.
"If your long-term maintainers and staff and developers aren't coming to the table with that mindset, it can be really problematic," he said. "Anyone doing security should really be trying to think like an adversary. So put yourself through training, courses and certifications are a great way to get started in that. Engage in capture the flag exercises and bug bounty. Then when you're going through your audit checklist you can start to understand the idea of applying this registry setting, if this is not applied, what is the real risk to my organization and this machine?"

During the COVID-19 telework era, zero trust practices and credentialed access is more important than ever as federal agencies shift operations to the cloud.

“You cannot over-invest in the planning and implementation of a robust identity and credential access management system,” Gattoni said. “If you can get that correct in your shift from your legacy environment to your cloud environment, you will get benefits down the road. If you can get that in play, you'll be in a much better position. If you don't, you're going to add heaps to challenges to your security professionals.”

Shifting to the cloud doesn't just require vigilant security practices, but also a mindset shift about IT security in terms of design.

“We've designed these [legacy IT] systems for a perimeter security model, so if you break that perimeter, you can essentially go nuts with lateral movement,” said Paul Puckett, director for the Office of Cloud Management at the Army. “If you just pick that up and move it to the cloud, absolutely you should be concerned about your data because you haven't been thoughtful. If you do so in a thoughtful way, you can absolutely be more secure and your costs can be way less than they are today.”

Goldstein said Defense Digital Service employs human-centered design to make the most of cloud services and advised federal agencies to do the same.

“Take this as an opportunity to move from these legacy systems to rethinking processes, de-duplicating, leveraging services and infrastructure, and expecting it to be a big pivot,” he said. “We need to do less checklists, more real assessments. We need to be constantly innovating on security.”