Zero Trust Promises 'One Identity to Rule Them All'

GSA's approach to managing passwords resembles shared services.

James Mersol

Wed, 01/29/2020 - 16:45

Photo Credit: guvendemir/iStock

Passwords are a big challenge in government.

Anyone who has spent any time as a government employee or contractor — or even created an account on a government website — is all too familiar with the tortuous password requirements of many federal agencies. The password cannot be too short, nor too long. It must include an uppercase letter, a lowercase letter, a number and a special character, for instance. Some agencies require users to change their passwords every 90 days, others every 30 days, and then the new password cannot be a repeat of the past 10 passwords used.

On top of these requirements, there are some rules of common sense that everyone knows they should follow even if not everyone does. (Password1234 shall not pass security standards.) Each system, program and account one uses should have a different password. With the number of logins used in the average work day, writing them down to remember them is a major security risk, and using a password manager requires its own equally strong password.

It’s enough to make anyone wonder why nobody has invented a better system.

“The biggest challenge we have now is passwords,” said Phil Lam, executive director of identity for the General Services Administration, at a Zero Trust event on Jan. 28. “We should have a more holistic view of identity.”

Lam advocated for an identity-based approach to security, based upon the principles of Zero Trust, as a way to not only remove the headaches around passwords, but also to provide better services to citizens.

“At GSA, when we think about identity, we think about it as a shared service,” Lam said. “To us, when we look at citizens and how they interact with government, it’s a little silly to think that a citizen needs a new identity at the VA, and another one at the Postal Service and another one at the Social Security Administration.”

A secure single sign-on would give citizens “more personalized experiences” with the government as well as lower the barriers to digital engagement, he said.

“One of the big pillars of that is that it has to be easy to use,” Lam said. He added that at GSA usability is a major priority for security, especially Zero Trust, to ensure that both employees and citizens support the technology.

Zero Trust's application to identity is nothing new. It can apply to data and enterprise alongside citizens to reduce the hurdles of applying Zero Trust to those cases.

"Citizen identities — and we've been implementing them for years and years — [have] always had the concept of Zero Trust," Lam said. "Now what we've come to realize is that there are some commonalities even in security where you can break down [barriers between different accounts] and still enable appropriate access. Maybe that's a concept that we can employ as well in enterprise: that there are requirements that we can all unify around — around identity, specifically — that provide eligibility or benefits access and still maintain the principles of Zero Trust."

An identity-based approach to security also removes two additional issues exclusive to passwords.

"The problem with credentials is that they are system-specific," said DHS CISO Paul Beckman, "[and] passwords need to be coupled with a second factor."

Beckman spoke highly of the public-key infrastructure (PKI) that underpins encryption in systems from communications to authentication and said "passwords have a place," but they cannot be the sole means of security.

For most government employees and contractors, the PIV or CAC card fulfills the role of a second authentication factor. Even if a database of government credentials were breached, it would be difficult for malicious actors to access any of those accounts without physical access to those cards.

"When we look at citizens, though, they don't have that," Lam said. "They have passwords. They have SMS texts, sometimes … emailed PIN codes. Can we move beyond that? Can we leverage biometrics? … Are there continuous authentication mechanisms we can look at?"

At the Department of Agriculture, drivers of Zero Trust are already thinking about using existing tools to create a secure system for the users they serve, said USDA CISO Venice Goodwine.

“We stick with the principles ‘what you know, what you have, what you are,’ typical for multi-factor,” she said. “We try to say at USDA, ‘meet the users where they are’ … identity proofing is going to be different depending on the end user that requires access to the service.”

Goodwine said there is no single approach that will work for all agencies, even when tailoring access management to its own employees. USDA has learned this lesson as a platform provider to other agencies.

“As a shared-service provider, the cybersecurity requirements are defined by the customer,” she said. “It can be complex, because DOJ … wants something different than DHS, that we may provide a service to. I think ensuring that the requirements based on the risk tolerance of each agency is what we need to incorporate into our platform that we share.”

Beckman shared that he has a subscription notice for all of his email accounts — personal and professional — on the website haveibeenpwned.com and encouraged everyone to do the same. The website is a free service that checks both the surface web and dark web for compromised credentials and notifies users if their information is found, along with breaches that may have caused the information leak.

“If you are not subscribed to that website today, you need to go and subscribe to that immediately,” Beckman urged. “The scary thing is that I get emails from this website on a monthly or bimonthly basis.”

With these known challenges, why are passwords still so common?

“Passwords have remained so prominent for so long because of how inexpensive they are,” Beckman said. “They’re very easy to embed into an application … to issue to a user … to manage at that point because a lot of people do self-service [through a challenge question, for example].”

Beckman reiterated that the problem with security is the choice among secure, fast and cheap products, where one can only have two of the three.

“Fast and cheap is the king, and passwords play into that,” he said.

Beckman agreed that the next step for security is going to be identity-based and that CISA will likely take on integrating identity security throughout government.

“It is going to be all-around identity,” he said, “and [Zero Trust] gives us an ability to figure out how we all centralize around identity and create that one identity to rule them all.”

View printer friendly version
Zero Trust
identity management
passwords
GSA
USDA
DHS
Standard