As remote work continues beyond the pandemic, how are the threats governments face changing?

We’re starting to see an alignment between what governments once did to provide remote access and what happens in people’s personal lives. Now government employees are more like regular consumers in the commercial space, only they’re accessing government resources, and we must take precautions.

How are solutions evolving?

We’re talking about tokenization of access — zero-trust solutions and more modern authenticators where you assume that the user could be on any connection — not necessarily inside of the walls or on a VPN. That means proving that you are who you say you are with multifactor authentication (MFA), that your device is healthy enough and if you’re using a personal device, that you are meeting the “must-be-this-tall-to-ride-the-rollercoaster requirements.”

In government, we’re seeing the opening of the aperture to these more modern and less expensive authenticators that the consumer space uses. We’re starting to see a push to normalize how the technology is used, and the government choice of solution is beginning to match the consumer choice of solution.

What steps should government leaders take?

For state and local governments, it always starts with identity. That involves a strong identity solution so you’re not having to recreate that stovepipe of usernames for every single application. Most municipalities have the things they need for this.

After identity, the next step is strong MFA to make the user prove they are who they say they are. Because users have to do something extra beside entering a password, that also addresses the insider threat — which is especially important at the state and local levels where there may not be the same overarching requirements you find in the federal government.

How should governments evaluate solutions?

Look for ones that aren’t a wholesale replacement. You want to be able to modernize your authentication with a portable choice that inserts new capabilities. The difference in scale for implementation is weeks versus years.

What is the biggest threat governments continue to face?

Probably the most important aspect involves ransomware attacks. Multifactor authentication will help prevent them, but with most attacks, the intruder will be inside your network for some period of time before they start locking you out so they understand what they’re leveraging against you. If you have a healthy multifactor environment that allows you to detect the use of credentials and enables users to report when theirs are used without their knowledge, you can zero in on where you need to look to see if someone is in the network. So the number one thing that you can do in advance of attack is multifactor, and the number one thing you would do after an attack is also multifactor.

Remember that attackers are opportunistic — they’re going to go to the lowest-hanging fruit. They are going to move on to someone else if you can make your threat surface smaller and protect your systems in a way that identifies threats quickly.

Duo Security, now part of Cisco, is the leading multi-factor authentication (MFA) and Zero Trust for the Workforce provider. Duo’s zero-trust security platform, Duo Beyond, enables organizations to provide secure access to all of their critical applications - for any user, from anywhere, and with any device. Duo is a trusted partner to more than 21,000 customers globally, including Dresser-Rand, Etsy, Facebook, Paramount Pictures, Random House, Zillow and more. Founded in Ann Arbor, Michigan, Duo has offices in growing hubs in Austin, Texas; San Francisco, California; and London. Visit Duo.com

© 2021 e.Republic. All rights reserved.