FCW | Workshop

Authentication for the new normal

Agencies' rapid adjustments in 2020 have highlighted the limits of traditional access management

Authentication is fundamental to security. That was true before COVID-19, but for agencies that had been engaged in digital transformation, conversations had been largely top driven and framed in terms of strategic planning for enterprise agility, interoperability, and collaboration.

The rapid pivot to most people working remotely put a spotlight on authentication, which became an urgent need almost overnight. Future plans became imperatives: increased adoption of multi-cloud architecture, collaboration software, and remote provisioning, for example.

"What's driving these changes is not your traditional methods, your executives. It's really been the pandemic that has completely changed how we work," said Jeff Frederick, senior solutions engineer for federal at Yubico. "Remote work has exploded by orders of magnitude."

Frederick cited a recent report that 83 percent of organizations surveyed were increasing multi-cloud adoption to support telework, yet 42 percent of those said their cyber-strategies were not keeping pace with those changes.

Work-from-home meant losing physical protections such as door readers and badges. Family members could potentially view sensitive data; a device might be shared among household members. Home routers are often less secure, and home networks not usually managed by IT professionals.

Agencies want authentication methods that are easy to navigate and adopt, Frederick said. They need to provide "ironclad protection" against threats and attacks—and to account for how to provision and credential a disperse workforce.

The most common authentication methods are generally easy to use, but also more vulnerable, he said: the username/password approach has an attack penetration rate of about 80 percent. For some basic Multi-Factor Authentication (MFA) protocols—2FA, SMS text, code via email—the rate is still 10 to 50 percent because the underlying technologies were not originally built for security.

Smart card authenticators—PIV, CAC—offer very strong security, but have usability issues and infrastructure complexities, particularly for a remote workforce.

For authentication protocols approaching zero-percent penetration rate, Frederick advised deploying technologies and tools that are purpose-built for security. Password-free authentication protocols, notably FIDO2 and WebAuthn, are new capabilities that can reduce man-in-the-middle attacks, among other benefits.

These protocols use public/private key cryptography similar to PIV and CAC, he said, "but without all the back-end overhead."

Security keys are a solution that checks all of the boxes: highly secure, easy to use, and provide multiple mechanisms of MFA support. Yubico's technology, the YubiKey, meets those criteria, as well as crucial federal standards for credentialing and authentication, he said.

"Every time you register your security key with a service, it creates a new public/private key pair that is … unique to one service and one service only."

– JEFF FREDERICK, SR. SOLUTIONS ENGINEER—FEDERAL, YUBICO

The objective, he said, is, "many apps, no shared secrets. … Every time you register your security key with a service, it creates a new public/private key pair that is not shared, each unique to one service and one service only."

A single YubiKey can support six capabilities—FIDO2, PIV/CAC, mobile 2FA or RSA-type OTP tokens, and password and OpenPGP encryption. That way, Frederick said, "You don't need multiple things hanging off your badge lanyard all day."

Having a solution that binds identity to an authenticator (the token) instead of a device enables bring-your-own device and single-device/multi-user situations, as well as enabling user-driven workflow. From an employee perspective, he said, "If I need to update a credential, I can do it myself; I don't need the help desk."

In terms of delivery, he said that Yubico has been working with a number of agencies during the pandemic that are issuing YubiKeys to employees. "We generally can slip right in to their existing issuance process," he said,

Cost per item is low enough that many agencies have been able to provide employees with a backup, he said, noting his own practice of keeping one key immediately on hand and another securely stored elsewhere. However, both keys do need to be registered.

"In the FIDO protocol most [intrusion detection and prevention systems] allow you to register multiple keys. All that they store is the public identity; the links to the public key to your identity is all that ever gets exposed out in the wild," he said.

Article Source: FCW Digital Transformation Workshop | September 22, 2020