Cambridge Housing Authority's Road to FIDO

Overview

The Cambridge Housing Authority (CHA) helps to provide rental assistance and affordable long-term rental housing to low income residents of Cambridge, Mass. The CHA uses IT throughout its organization to help onboard residents into public housing and has limited IT staff.

The Challenge:

At the Authenticate 2021 event, Jay Leslie, CIO of the Cambridge Housing Authority, recounted that his organization was the victim of spear phishing attack and he was looking for a way to help provide a more secure approach to user account authentication.

To help improve its security posture, the CHA was initially looking for a method of multi-factor authentication (MFA) to better secure access to the agency's information resources.

CHA had a number of key requirements for its MFA adoption. One of the requirements was that the MFA method should not require a phone authenticator app, as the CHA doesn't issue company mobile phones broadly. Additionally, there was some resistance to using personal devices for work by CHA staff.

Another primary requirement was that the MFA could not require an additional object for users and IT to keep track of, such as hardware authenticator keys.

The Road to FIDO: Enabling a Better User Experience

CHA considered a number of different approaches before settling on FIDO Authentication.

CHA's users have HID for physical access to CHA offices and an initial idea was to use the smart cards for MFA. The specific HID cards used by CHA however are older and couldn't be reused for access to computer resources.

While researching multi-factor authentication options, CHA came across the FIDO Alliance website. CHA realized that FIDO Authentication could be supported within its existing environment with a lot of the organization's existing processes and infrastructure.

Further investigation led CHA to realize that simple convenient multi-factor authentication was too narrow a goal and that FIDO adoption offered the opportunity for something much greater.

FIDO offered CHA the chance to revolutionize the user experience for its staff. With FIDO, not only could secure Windows authentication be achieved, but by leveraging WebAuthn and SAML single sign on, it also helps to enable secure, seamless passwordless authentication to every major system and application used at the agency.

Why FIDO Standards Matter

For CHA, choosing a standards based approach was a critical factor for multi-factor authentication.

With a small IT staff and limited resources, choosing a technology approach that will stand the test of time is an important factor.

A standards-based approach to strong authentication allows CHA to benefit from industry efforts to utilize a solution that has broad and growing support. A standards based approach with FIDO can be supported for years to come and is a better option than CHA going it alone to cobble together a kludge that's just good enough today, but that may be left behind in a year or two.

How CHA Uses FIDO with Windows Hello

CHA was already running Microsoft Windows on its systems, providing the organization with an easy entry point to the world of FIDO.

The organization implemented FIDO-compliant Windows Hello for Business using the key-based method. CHA's IT team encouraged the use of device PINs for the initial rollout in an effort to support as many users as possible.

The initial Windows Hello for Business rollout was to a small pilot group of users. When the pilot was expanded to a larger group of users, CHA encountered problems due to the organization not fully understanding the infrastructure required to support the solution. After pausing to fully understand the requirements, CHA realized that its small technology team lacked the experience and the time to carry out a full-scale implementation effectively. As such, CHA then identified resources that could help.

From MFA to Organization-wide Passwordless

CHA didn't just choose FIDO for MFA.

The FIDO deployment at CHA is a larger effort to embrace a broader passwordless model throughout the organization. CHA's passwordless project to implement FIDO-compliant Windows Hello for Business also included a SAML SSO component to make all possible systems and applications passwordless.

CHA now has over 250 account holders with most of them using FIDO device-based PINs for authentication instead of passwords on a regular basis.

The Future of FIDO at CHA

FIDO Authentication is set to remain critical to CHA's authentication strategy. Looking forward, the organization is likely to move from device-based PIN authentication to fingerprint or HID card-and-PIN authentication, as acceptance of biometrics and the ubiquity of fingerprint readers and NFC-enabled endpoints grows.

Convenient, Efficient and More Secure

"A 6-digit PIN that doesn't need to be changed periodically is far more convenient to remember and type than a long password. I have found it very easy and efficient to use. The IT department assures me it's more secure, too."

– John Filip, CFO,
Cambridge Housing Authority