Link to 2021 ACAMP Wiki

Advance CAMP Fri. Oct 8, 2021

Title: What do people expect out of a managed step up MFA

Room - Lodge

CONVENER: Matthew x Economou

MAIN SCRIBE: Group scribing, everyone join in!

ADDITIONAL CONTRIBUTORS:

# of ATTENDEES: 19

DISCUSSION:

Once the technology is in place, how do IAM teams actually manage MFA deployments?
How do they train users?
How do they interact with other IdP and SP operators?
(The MFA technology is "easy". Managing it seems "hard".)

- NIAID Discovery and Collaboration Platform has security requirements that drive the need for MFA ("FISMA Moderate")
    - SMS not acceptable
    - Need to issue supplement MFA since can't rely on IdPs, which isn't really core mission (MFAPoLR)
- User experience for TOTP?
- How does lost token recovery work?
- Need a MEEM meme
- Meshna: Westchester University had a good session on Monday
- Etan: Students were able to adopt it but with issues with authenticator device loss, but other staff could just not understand why or how to use MFA. Generated web page with step-wise instructions and screenshots for everything. Recorded a video of the process. Even had MFA enrollment and usage classes. Don't change too much at the same time—they enabled MFA at the same time as device replacements and email migrations.

Self-service MFA reset (instead of password reset) because they have certain contact information for them (e.g., SMS). Admins cannot make use of those tools. Some phones (iOS11+ "Offload Unused Apps") will uninstall unused apps, and that can reset secrets like TOTP seeds (e.g., Microsoft Authenticator app for iPhone).

- What about translating training materials?
- Etan: Backup TOTP secrets!
- Kyle: Can people bring personal devices with MFA authenticators into secure spaces?
- Etan: Might be able to work around using hardware tokens (e.g., FIDO2 keys). At JH, secured research spaces aren't places where someone would need to log into something.
- Colin: At University of Washington we have a large medical population and they are not allowed to bring phones into the clinical environment. Tokens have helped but there are still troubles getting full adaption.
- Matthew: How to get leadership buy-in to enforce MFA?
- Etan: Strong working relationships with the CISO, interpersonal trust.
- Benn: CISO support is critical. IT leadership should pretty much get it. Pitching to local bureaucracy is key, getting faculty on board.
- Kyle: What levers do SPs have to move?
- Donald: Many security decisions are dictated by relationships with auditors. It might be possible to use them to drive institutional change.
- Majeed: Lots of MFA adoption driven by email.
- Matthew: How do SPs get IdPs to signal MFA? Some IdPs break if that goes into the SAML request. New entity category? Community outreach? Direct comms with IdP tech contacts?
    - Etan: AuthnContextRef in the SAML request is the correct way, but until there is a standard value for it that is exactly MFA, (potentially the REFEDS value, but may need something broader that is SAML specific), it’s going to require SP<->IdP communication and collaboration. I.E. if an SP needs MFA, ask the IdP how they can do it.
-