US Government on Phishing-Resistant MFA

On January 26, 2022, the Office of the Management and Budget (OMB) issued a memo with the subject "Moving the U.S. Government Towards Zero Trust Cybersecurity Principles." This memo sets the groundwork for creating a zero trust architecture for federal agencies, with the goal of meeting this objective by the end of 2024. This is an exciting and necessary move made after the Biden administration released a previous Executive Order on improving cybersecurity.

While this memo is specifically for government agencies and vendors and contractors they work with, the guidance provided is one all organizations should be following and worth reading. The basic tenet of zero trust is "never trust, always verify" and by engaging in this mindset your organization will be able to move from more of a "detection" strategy to more of a "prevention" program.

Three key takeaways from the memo

1. **All multi-factor authentication (MFA) is NOT created equal:** MFA solutions that are password-based are prone to a whole host of attacks because passwords are one of the weakest factors you can use, along with one-time passwords and SMS text messages with codes. The added friction of these factors gives a false sense of security as all of them can be easily hacked.

   The memo explicitly states that passwordless MFA is where agencies should be moving to: "Agencies are encouraged to pursue greater use of passwordless multi-factor authentication as they modernize their authentication systems."

2. **Phishable MFA factors aren't going to cut it anymore:** The memo states that for "agency staff, contractors, and partners, phishing-resistant MFA is required." In fact, "phishing-resistant MFA" is mentioned over a dozen times in the memo. One-time codes, magic links, SMS text messages, and push notifications are all able to be phished by bad actors and should not be used anymore.

   Adversaries have tools to automate attacks against passwords and other phishable factors at scale. It's now time to move beyond these insecure factors and move towards secure factors, like biometrics and cryptographic security keys.

3. **The foundation of zero trust will be built on very strong authentication into every application:** By moving to zero trust, it will require solutions that provide cryptographic proof of user identity, and control access to only authorized and secure devices. This is the best way to ensure the identity of users accessing critical resources and preventing malicious actors from entering into networks where they could wreak havoc.

Significant sections in the memo

While the memo is worth a read in its entirety, we pulled the key sections that highlight the changes and new mentality agencies and other organizations will need to adopt as they move to a zero trust architecture.

Definition of zero trust and securing identity and access controls

"The foundational tenet of the Zero Trust Model is that no actor, system, network, or service operating outside or within the security perimeter is trusted. Instead, we must verify anything and everything attempting to establish access."

"Tightening access controls will require agencies to leverage data from different sources to make intelligent decisions, such as analyzing device and user information to assess the security posture of all activity on agency systems."

Emphasis on strong, phishing-resistant MFA in both its integration and enforcement

"MFA will generally protect against some common methods of gaining unauthorized account access, such as guessing weak passwords or reusing passwords obtained from a data breach. However, many approaches to multi-factor authentication will not protect against sophisticated phishing attacks, which can convincingly spoof official applications and involve dynamic interaction with users. Users can be fooled into providing a one-time code or responding to a security prompt that grants the attacker account access. These attacks can be fully automated and operate cheaply at significant scale."

"Agencies must require their users to use a phishing-resistant method to access agency-hosted accounts. For routine self-service access by agency staff, contractors, and partners, agency systems must discontinue support for authentication methods that fail to resist phishing, including protocols that register phone numbers for SMS or voice calls, supply one-time codes, or receive push notifications."

Passwordless MFA is encouraged

*"Agencies are permitted under current guidance to use phishing-resistant authenticators that do not yet support PIV or Derived PIV (such as **FIDO2** and Web Authentication-based authenticators) in order to meet the requirements of this strategy. To the greatest extent possible, agencies should centrally implement support for non-PIV authenticators in their enterprise identity management systems, so that these authenticators are centrally managed and connected to enterprise identities."*

"Agencies are encouraged to pursue greater use of passwordless multi-factor authentication as they modernize their authentication systems."

Beyond Identity

Beyond Identity is fundamentally changing the way the world logs in–eliminating passwords and all phishable factors to provide users with the most secure and frictionless authentication on the planet. Our invisible, passwordless MFA platform enables companies to secure access to applications and critical data, stop ransomware and account takeover attacks, meet compliance requirements, and dramatically improve the user experience and conversion rates. Our revolutionary zero-trust approach to authentication cryptographically binds the user's identity to their device, and continuously analyzes hundreds of risk signals for risk-based authentication. For more information on why Snowflake, Unqork, Roblox, and IAG use Beyond Identity, check out www.beyondidentity.com.