Taking Security Further:

How adaptive MFA is solving government's authentication challenges

There's a gaping hole in the middle of IT security. Passwords have proliferated beyond count, while the requirements of consumer applications and arduous IT authentication policies have made passwords increasingly complex. Users are throwing up their hands in frustration.

As a result, people practice increasingly bad password hygiene. The most popular password, according to a recent report on an analysis of some 10 million actual passwords? It's "123456." And number eight on the list? "Password."[1] Despite reminders from IT staff, 73 percent of passwords are duplicates.[2] This can make credentials vulnerable to "man in the middle" attacks, phishing and other ploys.

Many organizations are turning to multi-factor authentication (MFA) to manage employee access. In this paradigm, a security system requires multiple means of authentication from independent categories to verify the user's credentials. The secondary authentication can take several forms, such as a hard token or a "push" code that can be delivered to a mobile device.

However, adaptive MFA takes this further, noting access patterns and then adapting policy around each user or group.

To better understand the potential significance of adaptive MFA in the government enterprise, it's helpful to look at some of the most prominent public sector IT opportunities and challenges, especially surrounding authentication protocols.

CLOUD

The opportunity: Cloud computing has opened new frontiers for the government enterprise. Virtualization offers benefits of scalability, cost savings and application consolidation. As a result, 47 percent of all government organizations are using cloud services.[3]

The challenge: Cloud-based applications operate in a siloed identity model, one in which a user's identity is tied to an application and does not extend across the enterprise. This may stymie IT's efforts to deliver uniform control policies across applications. Managing identity piecemeal is impractical, and an administrative burden.

EMPLOYEE MOBILITY

The opportunity: Once desk-bound, government employees are now mobile. This has been a boon for productivity, with tablet-, laptop- and phone-toting civil servants delivering meaningful work products while on the go. BYOD has fueled the trend with 74 percent of government workers using their own tablets for work purposes and 49 percent working on their personal smartphones.[4]

The challenge: The rise of mobility creates an authentication challenge for government IT, as the proliferation of devices makes it difficult to implement a standard authentication regime. IT leaders struggle to deliver a uniform user experience to employees on the front end, while on the back end they must wrangle with the complexities inherent in trying to integrate their mobile security solutions with those driving authentication in their on-premises, proprietary systems. Device trust also is an issue, as IT managers may have no ready way to ensure they are providing access to a managed device.

CITIZEN SERVICE

The opportunity: The digital revolution has reshaped the civic relationship. Cities today offer online means for people to apply for permits, get their streets plowed or complain about their noisy neighbors.

The challenge: This trend puts an especially high premium on robust and reliable authentication. First, government handles sensitive data — including an array of financial and health information. Almost two-thirds of Americans want government to do a better job securing their data.[5] Government also needs to ensure that those who log in to claim benefits are who they say they are.

MFA: A Partial Fix

Multi-factor authentication goes a long way toward addressing these pressing challenges.

Ideally, an MFA solution will prevent a bad actor from accessing a system using only a victim's primary credentials. It will work across a broad range of VPNs using both security assertion markup language (SAML) and Radius to deliver comprehensive, seamless authentication across all enterprise applications accessed from the public internet — whether cloud-based, in the DMZ or protected by a VPN.

The most effective MFA solutions will offer a range of secure second-factor alternatives depending on the needs of the user base and the sensitivity of the information in play. Second-factor options can be tailored based on an accepted risk profile or convenience for a specific user type or group of users. This user-specific second factor might include security questions, a soft token which generates a random one-time pass code or a text message that delivers a single-use code.

Taken together, these measures can deliver a strong and versatile authentication solution. Adaptive MFA takes it one step further.

The Adaptive Solution

Adaptive MFA is a powerful tool that allows administrators to automatically generate policies over time. By interpreting and responding to user behaviors, MFA allows an organization to deliver the strongest level of security needed for a given situation, while still recognizing and responding to users as individuals.

Take the simple example of the mobile worker. An employee who travels frequently might encounter only a minimal set of security challenges when checking email overseas. Another employee who rarely leaves the office would be prompted to a higher level of authorization if he or she tried to log in from abroad. An unexpected shift in user behaviors might trigger stronger authentication. Suspicious events could likewise trigger risk-based policies. Attempted access through a proxy, for instance, might prompt a higher-level authentication challenge or deny access.

In an environment where employees can bring their own devices, agencies can offer a greater degree of security, mobility and convenience by reducing restrictions and enabling services for known devices that meet organizational policies. Additionally, they can restrict, add additional checks or even block unknown devices that do not meet organizational security standards.

Best Practices for Implementing Adaptive MFA

Educate users: Multi-factor authentication may come as something of an adjustment for employees accustomed to password protocols. It's important to have buy-in from across the organization before implementing a new procedure.

Balance security vs. usability: One of the great strengths of adaptive MFA is its ability to create a customized user experience, and a flexible policy framework enables just that. Security always seeks to balance resilience against ease; any adaptive MFA implementation should seek to leverage the inherent ability to deliver maximum security with minimum requirements or complexity.

Provide multiple avenues: The flexibility of MFA means it is possible to offer multiple means of access. That's important when dealing with a diverse user base, which may include individuals with minimal cell services. The important thing is to consider the full range of available options.

Given the need to put MFA in front of all applications — whether it be on-premises or in the cloud — an MFA solution shouldn't be viewed as a "point" solution which provides only second-factor authentication. Ideally, an adaptive MFA solution will be integrated into an enterprise-grade identity management service — specifically a cloud-based identity portal.

A portal solution enables IT leaders to share their MFA implementation easily across legacy operations, thus leveraging the full potential of the cloud and extending to their existing on-premises infrastructure and network layer. MFA isn't a silver bullet, but as a part of your broader identity strategy and security solution stack, it can help prevent breaches without hindering end user experience.

1. *https://www.huffingtonpost.com/entry/2016-most-common-passwords_us_587f9663e4b0c147f0bc299d*
2. *http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/*
3. *https://www.gartner.com/smarterwithgartner/understanding-cloud-adoption-in-government/*
4. *https://www.govtechworks.com/employees-wanting-mobile-access-may-get-it-as-5g-services-come-into-play/#gs.l9vqR7o*
5. *https://newsroom.accenture.com/news/most-us-citizens-experiencing-cyber-insecurity-and-wish-government-agencies-had-stronger-cyber-defense-mechanisms-to-protect-their-digital-data-accenture-research-finds.htm*

This piece was developed and written by the Center for Digital Government Content Studio, with information and input from Okta.

PRODUCED BY: CENTER FOR DIGITAL GOVERNMENT

SPONSORED BY: okta

The Center for Digital Government is a national research and advisory institute focused on technology policy and best practices in state and local government. The Center provides public- and private-sector leaders with decision support and actionable insight to help drive 21st-century government. The Center is a division of e.Republic, the nation's only media and research company focused exclusively on state and local government and education. **www.centerdigitalgov.com**

Okta is the leading independent provider of identity for the enterprise. The Okta Identity Cloud connects and protects employees of many of the world's largest enterprises. It also securely connects enterprises to their partners, suppliers and customers. With deep integrations to over 5,000 applications, the Okta Identity Cloud enables simple and secure access for any user from any device. Thousands of customers, including 20th Century Fox, Adobe, Dish Networks, Experian, Flex, LinkedIn, and News Corp, trust Okta to help them work faster, boost revenue and stay secure. Okta helps customers fulfill their missions faster by making it safe and easy to use the technologies they need to do their most significant work.

Learn more at: **www.okta.com**