FEDInsider

4 Ways to Maintain A Strong Mobile Security Foundation

Identity Management is a Key to Securing Government Mobility Programs

Featuring:

- **Mark Azar**
  IdAM Project Manager,
  The Efiia Group

- **Vincent Sritapan**
  Cyber QSMO Section Chief,
  CISA

- **Ross Foard**
  IT Specialist
  (INFOSEC), CISA

When the pandemic struck, government agencies were struck with the question of how to maintain continuity. Agencies quickly transitioned to a remote workforce. This included equipping employees with mobility tools like smartphones and laptops to enable them to work from home. But permitting employees to work remotely was only half the battle. The next question was how to protect those same employees, their devices and the data they generate within this new remote environment.

The answer was a concentration on getting an identity management strategy correct, while modifying and enhancing other existing security frameworks to work more efficiently with a remote workforce. Agencies have been operating under this mobile footing for over a year now, and have learned many important lessons about mobile cybersecurity. Three experts on the subject shared their thoughts and experiences during a recent FedInsider virtual panel. These are four of the key ideas they advocated.

1. Agencies Need to Fully Understand Their Frameworks to Support Proper Authentication Platforms

When it comes to building mobile security foundations, it's important to understand how to optimize all existing security protocols as well as how to incorporate various identity management functions. Examples of existing frameworks include the NIST Special Publication 800-157 guidelines, which outline the government's Personal Identity Verification (PIV) system. This worked extremely well with Common Access Cards (CAC) in the physical environment, but needed modified for remote work.

"A lot of agencies, especially larger ones, have been deploying derived PIV credentials," said Ross Foard, Senior Engineer for the CDM Program at the Cybersecurity and Infrastructure Security Agency (CISA). "And that gave them a framework to continue to operate with a strong assurance credential even as they moved into the pandemic and to a more distributed working from home environment."

Foard said that other NIST frameworks also provided a good starting point for mobility security, such as Special Publication 800-63-3, which looks at digital identity guidelines. Using that framework as a starting point, agencies have come up with alternative authentication methods that can be used to grant mobile workers access for specific purposes rather than the usual blanket authority provided by a PIV system. The pandemic has increased the need for these alternate authentications, and there is no indication that this need will change anytime soon, Foard noted.

2. Make Sure Your Environment Is Robust in Addition to Being Mobile

It's important to remember that the pandemic forced a sharp increase in the number of remote workers over a very a short period of time. This has presented problems with ensuring that mobility platforms could handle the same number of applications as agencies used prior to the pandemic. Agencies have had to quickly adapt solutions such as bolstering their available VPN bandwidth and deactivating non-essential applications.

Vincent Sritapan, Cyber QSMO Section Chief with CISA says that turning off non-essential features should not be huge deal for most agencies. Many times, their loss won't even be noticed. "The truth is, you can always turn those features back on if people ask for them," Sritapan said, "When enough people scream for something, then you'll know."

Each agency will have to remain vigilant about what programs and applications it supports for its remote workforce. Not only will this save bandwidth, but it also will reduce the number of identities and access levels that need to be monitored.

3. Agencies Must Understand Security Standards Within Deployed Frameworks

One of the most important factors in implementing a successful mobile security foundation is maintaining compliance with established government standards. Agency officials need to understand exactly why architecting and developing solutions compliant to established standards and guidance like NIST Special Publication 800-63-3 is so important.

"When it comes to identity, we specifically focus on mapping the intended use case to the proper assurance level within the NIST SP 800-63-3 guidelines themselves," said Mark Azar, Identity and Access Manager Project Manager with the Efiia Group. "Identity, authentication, and federation assurance levels are categorized as levels one, two, or three to provide increasing security controls to mitigate increasing risk for real-world implementation scenarios." The key is leveraging the correct assurance level in the right context, and understanding when to instill the proper security measures while still maintaining proper usability to ensure an intuitive user experience that we should all expect in 2021.

NIST defines an authenticator assurance level (AAL) by the strength of the authentication process. It's important that agencies understand not only their preferred AAL for each program, but also deploy it in a way that everything within their framework remains compliant per the established guidance. Azar notes that this is often fairly straightforward when dealing with local access. However, it gets a little more challenging for mobility programs because NIST has special AAL rules defined in NIST SP 800-157 that are tailored for smartphones and tablets running mobile operating systems. But the good news is that there are many proven solutions readily available so you do not have to incur unnecessary risk when you go true-mobile.

4. Use Identity Management to Aim Towards Zero Trust

Security in government is always a top priority, and identity management is good way to verify who is accessing agency resources. But it's only one aspect of security. The goal should be to use identity management to support a full zero trust program, where the least amount of access is given to each user, and only for the task at hand. This is even more important when working in a distributed mobile environment.

"Recently, we've made sure our clients adopt a zero trust model quickly as the modern workplace has changed," said Azar. "Remote workers need to safely access decentralized resources that are no longer just on-premise," which makes a powerful framework like zero trust all the more critical in order to ensure security.

Azar's employer, Efiia, has leveraged CompliantID, which includes SailPoint identity governance workflows for managing user access to applications protected by other cloud access management services. The solution enables government to engage with external stakeholders and citizens in real-time using a zero trust architecture, with support for single or multiple personas. CompliantID enables AAL2 and AAL3 multi-factor authentication, in alignment with guidance prescribed by NIST Special Publication 800-63-3.

Azar says that the old system of "trust but verify" isn't strong enough anymore for government work. Agencies need to move to a zero trust policy which is based off "don't trust, always verify." The core principles of security such as least privilege and separation / segregation of duties are just as important as ever. Basic identity management is a great first step, but it's only the foundation for zero trust networking in government.

FEDInsider

Hosky Communications Inc.
3811 Massachusetts Avenue, NW
Washington, DC 20016

- (202) 237-0300
- Info@FedInsider.com
- FedInsider.com
- @FedInsiderNews
- Linkedin.com/company/FedInsider
- @FedInsider

carahsoft.

Carahsoft
1493 Sunset Hills Road
Reston, VA 20190
Contact: Maggie Manfredi

- (703) 230-7488
- Maggie.Manfredi@Carahsoft.com
- Carahsoft.com/vendors/SailPoint
- Facebook.com/Carahsoft
- Linkedin.com/company/Carahsoft
- @Carahsoft

SailPoint

SailPoint
11120 Four Points Drive
Austin, TX 78726
Contact: Cathy Cromley

- (703) 517-4419
- Cathy.Cromley@SailPoint.com
- Sailpoint.com/identity-for/government
- Facebook.com/SailPoint
- Linkedin.com/company/SailPoint-Technologies
- @SailPoint