Deloitte.

Addressing Cyber Threats
Multi-Factor Authentication for Privileged User Accounts

Contents

Introduction

Why passwords are not enough to protect today's digital economy

Over the past few years, there has been a disturbing trend in the number and types of cyber breaches around the globe. These breaches have shown that everyone is vulnerable, including the most sophisticated Information Technology (IT) organizations, the largest and most respected financial institutions, and even the United States government. Years ago, these attacks were often rogue hackers simply testing their skills and relishing the satisfaction of having infiltrated a protected network and publicly embarrassing an organization, or temporarily interfering with its ability to conduct business. More recently, however, dangerous actors, often sophisticated and well organized state-sponsored cyber 'terrorists', are secretly and quietly exploiting networks over time to obtain sensitive information for nefarious purposes, such as stealing identities or intellectual property. As these cyber terrorists continue to grow in sophistication, the systems that control critical US infrastructure, including power grids, transportation systems, banking infrastructure, and drinking water supplies, as well as our most sensitive military and intelligence programs, become more vulnerable.

Inevitably, whenever a new cyber breach is reported, the question is asked, "How did they do it?" There are many ways to penetrate seemingly secure systems. However, one of the most sought after targets for hackers are the privileged user accounts on any network—those accounts with elevated access privileges to administer and manage security functions on systems. Breaching a privileged user account, as the name implies, provides access (to a server or desktop) that is above and beyond "normal" access privileges. With this type of access, an attacker may more easily move throughout the network to gain access to numerous assets and potentially cause catastrophic damage utilizing the heightened permissions of the user. Yet despite the escalated risk, many privileged accounts today are still protected with only username/password (a type of single-factor authentication), which experts agree is an incredibly weak way to validate the identity of a user.

According to the Fiscal Year 2014 Federal Information Security Management Act (FISMA) Annual Report to Congress[1], the Office of Management and Budget (OMB) conducted an analysis of agency incident and performance data to determine where to focus its oversight efforts in FY 2015. It found that the majority of federal cybersecurity incidents are related to or could potentially have been mitigated by the implementation of strong authentication. Likewise, incident reports produced by the U.S. Computer Emergency Response Team (US-CERT) indicate that in FY 2013, 65% of federal civilian cybersecurity incidents were related to or could have been prevented by strong authentication implementation. Although this figure decreased to 52% in FY 2014, it is still a relatively high percentage when one considers that strong authentication implementation for civilian agency user accounts remains at only 41%, well below the 75% target.[2]

In response to this escalating threat, the Federal Chief Information Officer (CIO), Tony Scott, recently launched an accelerated Cybersecurity Sprint effort requiring federal agencies to take a number of steps to improve the security and resilience of their networks. Key among the provisions of the Cybersecurity Sprint is a requirement to immediately enforce the use of multi-factor authentication for privileged user accounts using Homeland Security Presidential Directive (HSPD)-12 compliant Personal Identity Verification (PIV) cards, or an alternative form of multi-factor authentication.[3]

[1] Annual Report to Congress: Federal Information Security Management Act, OMB, February 27, 2015, p. 23.
[2] Ibid.
[3] The White House. "FACT SHEET: Enhancing and Strengthening the Federal Government's Cybersecurity." N.p., 2015. Web. 6 July 2015.

Multi-factor authentication for privileged users

Multi-factor authentication for privileged users can help mitigate certain risks to your agency's critical assets and data.

Multi-factor authentication protects against intrusion attempts by increasing the difficulty of compromising a privileged user. For instance, PIV-enabled multi-factor authentication operates by requiring the user to enter a PIN (something the user knows) to unlock their PIV's digital certificates (something the user has). The PIV then participates in a cryptographic authentication process with the protected network or server. The cryptographic process is designed to thwart "replay" and other "man-in-the-middle" attacks, and cannot be duplicated by an attacker who does not possess the PIV. Other, non-PIV cryptographic tokens can provide similar capabilities, but none are as widely distributed to the federal and contractor workforce as are PIV cards.

Privileged user accounts typically have the most elevated permissions, or greatest capabilities, in an IT organization and access to the most sensitive information. As a result, those user(s) and/or server accounts also have the potential to cause the most damage. Generally speaking, a privileged user account is typically able to:

- Access, alter and remove data;
- Run programs and enable or remove file shares;
- Add and delete users, change user privileges and enable remote access;
- Read and change database records, access transactions data, change database configuration and schema, add or modify stored procedures;
- Grant and deny network access and enable and disable monitoring; and
- Alter configuration and audit settings.

Due to these elevated permissions, privileged user accounts may be used to compromise the confidentiality, integrity and availability of the system and serve as a jumping off point to attack other critical assets in the environment. While many federal agencies have made progress issuing and using PIV cards for multi-factor authentication, their efforts have been mainly focused on the most prevalent account types—the "regular" user accounts—or non-privileged accounts. Unfortunately, many privileged user accounts are still today protected with weak credentials, often only username/password, leaving systems and applications more vulnerable to attack.

There are many ways attackers may illicitly access a system—as an example—using "Social-Engineering" to obtain legitimate username/password combinations is one of the least expensive and most effective. Multi-factor authentication may improve an agency's security posture if username/password login is disabled, particularly for privileged accounts. Accounts that require multi-factor authentication for login cannot be accessed remotely unless the attacker possesses an authorized physical token associated with those accounts. Multi-factor authentication also mitigates risks associated with certain types of man-in-the-middle attacks, such as the use of malware to steal usernames and passwords as they are entered during what appears to be a login attempt.

Multi-factor authentication: stepping up from username and password

A user's identity can be authenticated using three different types of factors:

- Something you know (e.g., passwords)
- Something you have (e.g., Personal Identification Verification (PIV) cards)
- Something you are (e.g., fingerprints)

Combining two or three types of factors is referred to as "multi-factor authentication." This term is often used interchangeably with the term "two-factor authentication" when two factors are used.

Multi-factor authentication techniques provide additional mitigation against security threats, particularly over single-factor knowledge-based factors like passwords. Despite their prevalent use, passwords have proven susceptible to a host of attacks (e.g., eavesdropping, phishing, and online guessing using advanced computing methods) and offer little to no protection in today's environment.

Despite the compelling security benefits, implementing multi-factor authentication for privileged user accounts is often a cumbersome task further complicated by the intricate web of legacy applications. These accounts are typically managed through a separate directory structure with unique identities for the same individual for both their regular user and privileged user accounts, which are spread across a multitude of infrastructure components. Often, the technical environments being administered do not offer out-of-the-box support for PIV authentication and include legacy infrastructure that is more difficult to PIV-enable. In order to navigate these challenges, agencies should consider pursuing a multi-tiered approach to implementing multi-factor authentication for privileged users, taking into consideration the specific infrastructure and existing investments in place at their agency:

1. Require PIV authentication wherever possible and work rapidly to implement known technical solutions for environments that can support PIV.
2. Leverage other multi-factor authentication tokens where available to eradicate remaining password-enabled accounts.
3. Determine mid- and long-term steps to provide comprehensive protection of privileged user accounts.

Mandatory PIV authentication

The PIV credential serves as the "gold standard" for multi-factor authentication in the Federal Government, providing the highest level of assurance (LOA) in the claimed identity of the user. While the majority of applications are now expected to at least be PIV-enabled, many federal agencies continue to wrestle with technical challenges and vendor/system constraints related to enforcing PIV authentication. For those systems that are PIV-enabled, PIV authentication is often not mandatory, meaning that users are still able to access a system using username/password. Although PIV enablement was viewed as an acceptable interim step toward full multi-factor authentication, recent government communications have made it clear that is no longer the case. Where passwords are still in play, they remain an attack vector for hackers. The bar is now clearly set at mandatory PIV authentication, starting with privileged user accounts, and ending with the eradication of password access for all protected resources.

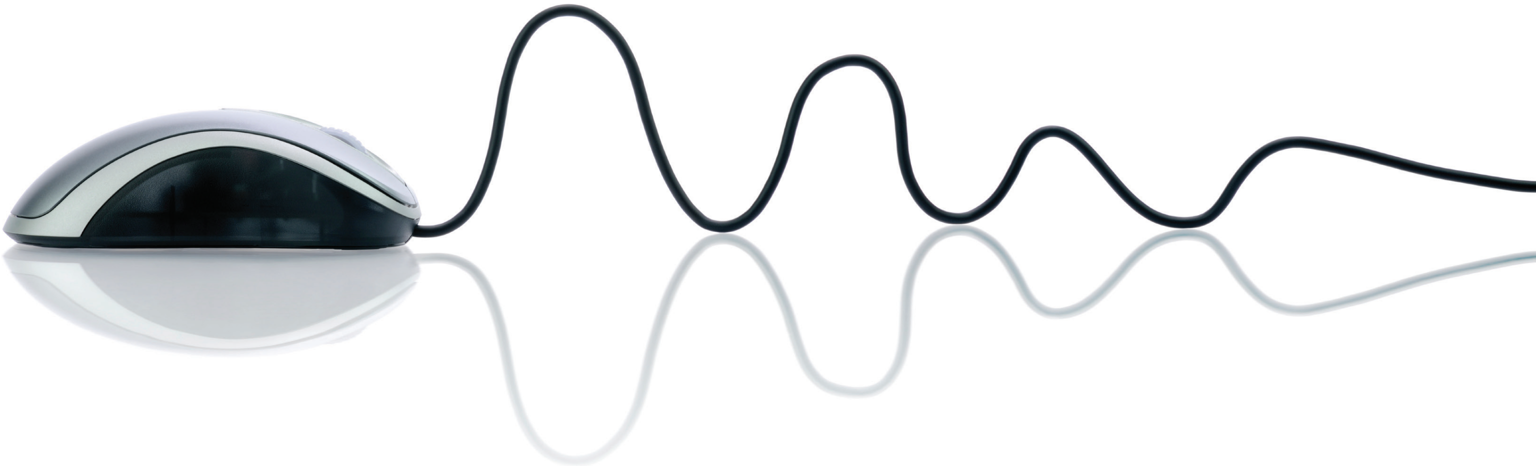
Based on extensive work in the Identity, Credential & Access Management (ICAM) community over the last few years, many technology platforms that were not previously able to support PIV authentication now have technical solutions to do so. Agencies should leverage the guidance and support offered by OMB as part of the Cybersecurity Sprint and work with experienced technical resources to evaluate their environments and pursue PIV implementation across the enterprise for assets that can support it. PIV cards issued to employees and contractors may be used in conjunction with card readers to log into newer operating systems. In some cases PIV middleware must also be installed. Mainframes and systems running older versions of Windows can use commercial software packages to enable PIV-based login. Unix-based systems can also be configured for PIV-based multi-factor login; details vary depending on the Unix variant used by each system.

Some privileged users may find that the User Principal Name (UPN) in their PIV does not match their privileged account(s); this will prevent them from using PIV-based multi-factor authentication when logging into those accounts. Some agencies have issued privileged users a secondary "System Administrator" PIV for authenticating into privileged accounts. While this may not be OMB's preferred method, it is preferable to continued use of single-factor authentication methods.

Other multi-factor authentication tokens

For legacy applications where technology constrains cost-effective PIV authentication implementation, agencies are still expected to replace username/password authentication with an alternative multi-factor authentication technology. If only a portion of a user population uses multi-factor authentication technology, attackers will focus their attention on those who do not. To maximize effectiveness, multi-factor technology must be mandatory for the entire population. This will reduce user convenience somewhat; for instance, if an authentication token is lost, damaged or stolen it must be replaced before the user can access the systems again. However, it will significantly reduce the risk of unauthorized access and loss of sensitive data.

Other forms of multi-factor authentication include software cryptographic tokens and one-time password hardware tokens. In some cases, an agency may already have an investment in these technologies that can be leveraged to protect their privileged user accounts in the short term. Agencies should explore the availability of existing solutions within their enterprise and the potential to quickly expand



deployment to all privileged user populations. Expanding the implementation of existing multi-factor solutions is a particularly easy and inexpensive interim approach. However, OMB guidance directs agencies not to spend time and money on new solutions that do not contribute to migrating to the mandated PIV-enabled end-state.

Comprehensive privileged access management

While multi-factor authentication offers a strong protection for an agency's network or systems, it does not fully address security considerations regarding exploitation of privileged user accounts. Agencies need to develop their target state plan—a holistic plan of how they will manage and govern their accounts in compliance with Federal Government controls and requirements. A holistic approach should address not only authentication, but also the following:

- Policies and procedures to govern acceptable user behavior for privileged users and to establish what constitutes anomalous behavior for monitoring and detection.
- Provisioning and ongoing management of the access privileges associated with privileged user accounts to make sure that assigned privileges are still valid and necessary.
- Account activity monitoring and detection to discover anomalous behavior and respond to successful attacks in a timely fashion.
- Session recording and auditing to log privileged access and specific actions taken during a login session.
- Incident response and recovery capabilities to minimize and repair the impacts of successful attacks and restore normal business operations.

There are a variety of commercially available privileged access management solutions that offer governance, analytics, and management capabilities. Analytics may help identify accounts that are likely to serve as jump off points to a more complex attack. Most support systems place no constraints on an employee's ability to reset passwords, allowing a compromised support account to reset accounts throughout the agency and simply log in to privileged accounts to capture critical data. With even a minimal amount of data analysis, large scale but simple proactive defense mechanisms can be implemented, which is particularly effective for environments with a large external contractor workforce or support team.

As part of the Continuous Diagnostics and Mitigation[4] (CDM) program, federal agencies have access to capabilities and tools that identify cybersecurity risks on an ongoing basis, prioritize these risks based upon potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first. These include several privileged access management tools that support the capabilities previously described. Agencies should leverage the funded tools and resources under CDM and plan for implementation and ongoing operations of these capabilities as part of their comprehensive cybersecurity program.

[4] http://www.dhs.gov/cdm

What other measures should agencies consider?

Multi-factor authentication is one component of an agency's cyber protection program.

Multi-factor login and privileged access management should be considered an important part of an overall network security program, not the entire program. User accounts are not the only vulnerable elements of federal systems storing sensitive data. With the widespread adoption of service-oriented architecture over the past decade, Web Services (WS) and Remote Procedure Calls (RPC) are also potential points of attack. Successful attacks on WSs and RPCs can yield access to plain-text (i.e., non-encrypted) sensitive data. System architectures should be upgraded to require mutual authentication between WS and RPC callers and hosts.

Agencies should actively review the logs of their antivirus and antimalware solutions to verify that updates are being installed as required. These reviews can also detect signs of intrusion that may have been missed at the router/firewall level.

An attacker's access and the extent of potential damage can be limited by locking down agency networks. For instance, internet-facing servers may never need to communicate with servers storing sensitive information; when this is the case, the network should not provide a communication path between them. Reworking network configurations to provide only the communication paths required for operations can impede attackers' ability to navigate the internal network following a successful breach, thus giving agencies more time to detect and respond to the attack before critical data has been compromised.

As a longer-term measure, Deloitte Advisory[5] is familiar with emerging network technologies that have frustrated weeks-long intrusion attempts by experienced teams of certified ethical hackers. While these technologies are relatively immature, they show great promise as an element of a cybersecurity strategy.

[5] As used in this document, "Deloitte Advisory" means Deloitte & Touche LLP, which provides audit and enterprise risk services; Deloitte Financial Advisory Services LLP, which provides forensic, dispute, and other consulting services; and its affiliate, Deloitte Transactions and Business Analytics LLP, which provides a wide range of advisory and analytics services. Deloitte Transactions and Business Analytics LLP is not a certified public accounting firm. These entities are separate subsidiaries of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Secure.Vigilant.Resilient.™

Transforming from a traditional, standards-driven IT security program to a *Secure.Vigilant.Resilient.* cyber risk program is not just about spending money differently—it's a fundamentally different approach that prioritizes risk and related spending.

With security and privacy breaches on the rise and a corresponding increase in regulation, the threats to a federal agency extend well beyond the particulars of any one incident. Government leaders have a compelling need to understand and reduce their security and privacy exposure. The sheer volume, variety, complexity and intensity of threats, and the speed at which they have evolved have greatly elevated the urgency with which they are being addressed at the highest levels of the Federal Government. Agency leaders are responsible for implementing adequate measures to protect the enterprise and for the efficacy of the related investments.

Deloitte Advisory has long served as an advisor to the Federal Government in assessing and addressing cyber security risk through its ***Secure.Vigilant.Resilient.*** suite of services. Being secure means focusing protection around the risk-sensitive assets at the heart of a federal agency's mission. Given the reach and complexity of its digital ecosystem, an agency can't secure everything equally. Being secure means focusing protection around the risk-sensitive assets at the heart of the agency's mission. Deloitte Advisory's **Secure** service assists in protecting our government clients' critical assets, including both information and infrastructure, by implementing risk-prioritized controls to protect against known and emerging threats and comply with standards and regulations. The design and technology recommendations for multi-factor authentication, for example, fall under this service.

By plotting the motives and psychology of adversaries, and considering the potential for accidental damage, cyber risk strategists anticipate what might occur and design detection systems accordingly. Today's costliest attacks tend to be the ones that are highly targeted. Being vigilant means establishing threat awareness throughout the agency, and developing the capacity to detect patterns of behavior that may indicate, or even predict, compromise of critical assets. Agency leaders need sufficient understanding of the threat landscape to provide cyber risk guidance to the technical teams responsible for translating the guidance into effective operational capabilities. Deloitte Advisory's **Vigilant** service assists our clients in identifying and understanding threats against critical assets by establishing situational risk and threat awareness across the environment to detect violations and anomalies.

Being resilient means having the capacity to rapidly contain the damage of a breach and mobilize the diverse resources needed to reduce impact—including direct costs and service disruption, as well as reputational damage. While resilience requires investment in traditional technology-based redundancy and disaster recovery capabilities, the bigger picture includes a complete set of crisis management capabilities. Incident response and crisis management must feed continuous improvement processes. Resilient agencies take the time to absorb important lessons, and modify the secure and vigilant aspects of the program to emerge stronger than before. Finally, Deloitte Advisory's **Resilient** service assists our clients in minimizing the impact of incidents when they occur by setting up a process to handle critical incidents, quickly return to normal operations, and repair damage to the business.

Summary

Over the last several years, cyber hackers have become very sophisticated and persistent in breaching high value targets such as Federal Government systems. High-profile breaches of government data systems are increasing in frequency and scope of damage. Deloitte Advisory recommends that agencies respond by securing privileged accounts as a critical short-term step toward full compliance with National Institute of Standards and Technology (NIST) and OMB guidance.

A policy requiring across-the-board, no-exception use of PIV-enabled login to privileged accounts is an achievable, high-impact step toward full compliance. While the use of PIV-based multi-factor authentication for access to privileged accounts is a strong first step, it may be complicated by a myriad of legacy infrastructure components—and it is only one element of a comprehensive cyber defense strategy.

Contacts

To learn more about how your agency can become secure, vigilant, and resilient, please contact:

Deborah Golden
Deloitte Advisory Principal | Federal Cyber Risk Services Leader
Deloitte & Touche LLP
debgolden@deloitte.com

Chris Goodwin
Deloitte Advisory Principal | Federal Cyber Risk Services Identity and Access Management Leader
Deloitte & Touche LLP
wgoodwin@deloitte.com

This document contains general information only and Deloitte is not, by means of this document, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This document is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this document.