User Identities Are the Keys to the Kingdom (Agency)

Keep Your Doors Locked

While perimeter security remains important, the routers, firewalls, and intrusion detection systems that protect network access are no longer sufficient protection for Federal agencies against bad actors. Attackers will always try to find ways to breach the network perimeter; it's usually a question of when – not if – they will succeed.

The global, dynamic, and interconnected nature of IT enterprises today – and a proliferation of security threats – require protections that limit the damage attackers can do once they're inside the agency firewall. Agencies need to elevate the importance of data and identity protection.

Each Federal employee has an identity that encompasses their role in the agency and the data and information systems he or she is permitted to access and modify. Protecting those identities is paramount. Even if a single identity is breached, financial data, personally identifiable information, intellectual property, and critical processes – ranging from payroll and benefits to energy and healthcare delivery – could be compromised.

Essentially, a user identity is the keys to anything the user can access, and sometimes even more. Simply educating employees about the value of an identity can greatly improve an agency's security posture. Employees are much more likely to take care with agency IT resources – such as their identity and the materials and systems they access – if they understand what's at stake.

Double Whammy: Attackers Target Privileged Users and Active Directory

In some of the most highly damaging breaches of the last five years, attackers ran exploits designed to gain privileged access to public- and private-sector networks. Privileged users are system administrators or other super-users who can access and control critical computer systems and applications. Because these users have access to sensitive information and the ability to change settings, attackers who compromise their identities can cause catastrophic damage not only to agency operations, but also to agency, employee, and citizen security and privacy. For example, attackers who gain privileged access to a network could deploy ransomware or steal national security information.

Active Directory (AD), Microsoft's proprietary directory service, is a prime target of bad actors because it is a key component of identity management in Federal agencies – and nearly every organization worldwide. In fact, AD breaches are probably the most detected type of breach. The most high-profile AD breach came in 2015 at the Office of Personnel Management, which resulted in the theft of background investigation records of current, former, and prospective Federal employees and contractors. Nearly 22 million individuals were affected.

The OPM breach was the result of a pass-the-hash attack, in which a user's workstation is compromised, and then:

- The bad actor gains administrative permissions to the user's computer and creates a problem that requires someone with elevated permissions to fix it
- An administrator logs onto the computer to remedy the issue, which creates and stores the administrator's password hash in the workstation memory
- The bad actor executes software to extract the hash and makes network connections from the workstation to databases or other resources, posing as the privileged user

"The hash was most likely a domain administrator credential, which is a highly privileged user within Active Directory," noted Dan Conrad, an identity and access management (IAM) strategist for One Identity who works with Federal agencies. "At that point they were able to make a lateral movement across the network to do whatever they wanted. People talk about how the [security clearance] database should have been encrypted. But if you have a privileged credential, it doesn't matter if it's encrypted or not, because the database is decrypted for that privileged user."

Another common AD exploit is password spraying, in which an attacker continuously injects previously compromised passwords and hashes to an authentication web page or other system. The attacker will usually rotate usernames, so instead of finding a password that fits a username, the attacker finds a username that fits a password. Armed with the username and password, the attacker now has access to any resource that the user does. Moreover, if the user has privileged access, so does the attacker. Elevated privilege gives the attacker the ability to do things such as deploy ransomware via group policy updates – in short order owning every Windows machine on the user's domain.

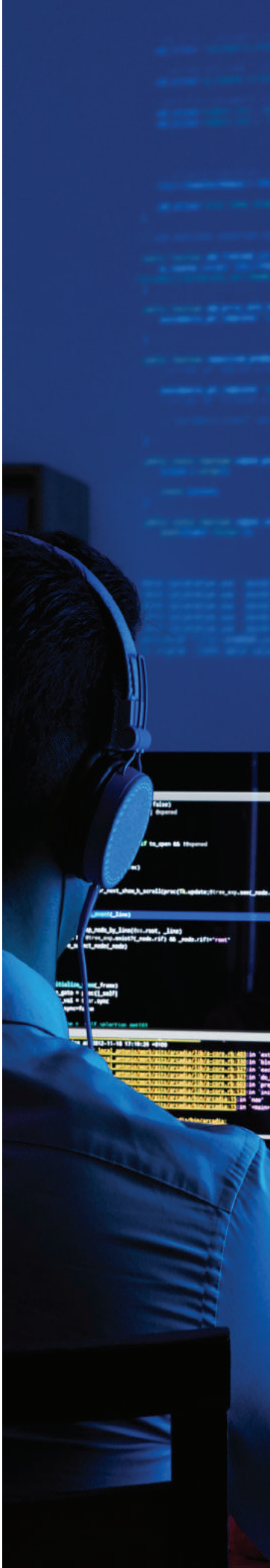
If that happens, the agency has two rather grim choices: pay the ransom or rebuild AD, Conrad said.

Fighting Back: Agencies Require Identity and Access Management

Agency resources are secure only when the right people get the right access to the right resources at the right time, in the right way, and the agency can prove it. Agencies can achieve this state only when identity is at the core of their security strategy. An enterprise IAM solution enables this desired end state with applications that allow administrators to change user roles, track and document their activities, and enforce policies. An integrated IAM solution enables enterprise-wide administration of user permissions and helps ensure compliance with government policies and regulations. Each user's identity is maintained, modified, and monitored throughout its use, from onboarding to eventual offboarding.

Key components of an IAM solution include:

- **Identity governance**, which allows administrators to define, enforce, review, and audit IAM policy, and also map IAM functions to compliance requirements and audit user access to support compliance reporting
- **Identity administration**, which enables administrators to automatically create, modify, or delete identities and grant privileges for resources including systems, software, and data. Identity administration enables organizations to centralize policies and processes across the enterprise and automate provisioning and password management for systems, platforms, and applications
- **Privileged access management (PAM)**, which allows administrators to control elevated (or privileged) access and permissions for certain users, accounts, processes, and systems. PAM tools gather the credentials of privileged users into a secure repository to isolate their use and log their activity, which lowers the risk of credential theft or misuse



- **AD management**, which generates and enforces access rules for AD and Azure Active Directory (AAD), eliminating errors and inconsistencies common with native approaches and automating numerous tasks, including creating user and group accounts and assigning and removing user access rights in AD, AAD, and AD-joined systems

Some agencies will want a point product to fill in a gap in their IAM portfolio. The greatest value to an enterprise, however, comes from a holistic solution that encompasses all facets of IAM – and integrates with the leading cloud platforms and enterprise platforms and applications. One Identity, a Quest company, offers a complete solution, as well as the ability to implement a single product to fill a gap. Coupled with solution aggregator DLT's expansive access to government contract vehicles and deep network of Federal agency IT partners, Federal agencies have a one-stop source for IAM capabilities with DLT.

Beyond improving security across the enterprise, IAM brings many benefits to Federal agencies:

- **Ease of use for end users**. Agency employees no longer have to manage myriad accounts to access applications and resources because their unique identity provides access with a single set of credentials
- **IT staff efficiency and cost savings**. Automation reduces the amount of time spent on routine IT administration tasks, such as onboarding and offboarding, and reduces requests for help desk assistance, resulting in cost savings
- **Seamless workflows**. Administrators and employees alike benefit from policies applied enterprise-wide, so their access and permissions happen automatically, with no user action required
- **Elevated security posture**. When policy is determined and implemented with automation, access vulnerabilities are significantly reduced and are no longer dependent on manual, one-off processes to ensure the security of the enterprise

One Identity and DLT: A Comprehensive IAM Solution

The need for IAM is clear: Perimeter security is no longer sufficient to protect agency networks and information, and the repercussions of attacks launched from the inside are severe – potentially halting vital agency operations and public services and jeopardizing the personal information of millions of workers and citizens. With One Identity and DLT, agencies gain a holistic suite of IAM tools to thwart agency compromise from the inside.

Protect your agency from malicious malware attacks.

Request a quote to learn more.