TECH BRIEF

Has securing Active Directory been forgotten in a CDM-centric enterprise?

The Department of Homeland Security program, Continuous Diagnostics and Mitigation (CDM), is one of the most significant advancements in cybersecurity by the federal government. If you haven't heard of it, here's how it is described on the DHS web site: "The CDM program is a dynamic approach to fortifying the cybersecurity of government networks and systems." Despite this program delivering tools and technologies necessary to protect sensitive information and enable access to essential government services, one of the key components of access and cybersecurity was overlooked – Active Directory.

https://www.dhs.gov/cdm

Every federal agency, civilian or military, relies on access granted (or denied) by Microsoft Active Directory (AD). In fact, the accounts and privileges in AD have always been key targets for the "bad actors". While securing and controlling AD for any size organization can be a challenge, many agencies have chosen to consolidate directories in an effort to wrap more controls around fewer directories. Obviously, managing fewer directories creates fewer targets and therefore should be easier to control and secure, but if weak controls and policies manage these directories, chaos will quickly ensue.

While CDM addresses some areas of authentication, such as PIV logon, AD is not specifically addressed. These large directories must be controlled with strong policies. And the larger the directory, the larger the risk, which then requires unwavering enforcment of policies to eliminate one-off exceptions.

Additionally, privileged accounts – the "keys to the kingdom" - must be controlled with absolutely no policy exceptions. PIV-enabling privileged accounts can signficantly reduce the vulnerability of these accounts. The National Institute of Standards and Technology (NIST) provides general guidance for managing privileged accounts and many of these recommendations apply directly to AD. NIST recommendations include:

Remove unnecessary access: Remove all privileged account access from users who no longer require access to perform their assigned duties. If they don't need it, why have it?

- Delegation of the AD account – To do this effectively, your AD management tool should enable a least-privilege access model. This means that permissions for individual employees allows them to access the resources they need to do their job, but no more. This model includes limited management of elevated accounts and groups (such as domain admins, enterprise admins and account operators) without granting individuals unlimited privileges.
- Temporal group membership — This means that privilege elevation is not permanent and doesn't "creep" as a privileged user changes jobs. Users will only be part of a privileged group during a specified time period to accomplish specific tasks. They are added to the group at the start time, then removed when that permission expires. So, if a privileged account is an attack target, the impact of that attack is limited to the user's "normal" privileges.
- Controlled administration—This is an administrative service that acts as a firewall around AD. This allows enhanced access control to privileged accounts by defining administrative roles, associated permissions and rules to be strictly enforced, which the sum total is the only way to maintain compliance with security policies.

Remove unnecessary accounts: If the account is no longer required, why is it still there? Again, who needs it?

- Accounts living in AD that are no longer needed or used are vulnerable to compromise, more so than an account with regular activity. You need a solution that provides the ability to programmatically eliminate this vulnerability through a policy. For example, an effective solution can automatically disable accounts that haven't been used in a certain number of days, as well as comes with default policies to automate commonly-scripted de-provisioning tasks, and permits all provision policies to be tailored to an organization's specific needs.

Remove excessive access: Sometimes we call this "role creep", where an admin either changes jobs and keeps the permissions from a previous position or is simply elevated to the top level admin role with access to everything.

- Proper delegation in AD – You should look for a solution that can ensure the admin only keep the permissions necessary to do the job they need to do. Functions such as "dynamic group membership" can be used to ensure the "role creep" does not happen but permissions (or roles) are removed when an admin changes positions.
- Automated provisioning—Automates user and group provisioning, including account

"Delegation needs of large enterprises are **significantly** more complex than native AD can possibly provide."

creation in AD, mailbox creation in Exchange, and group population and resource provisioning in Windows, which helps you save valuable administrative time. The solution you select should automate re-provisioning and de-provisioning, helping to ensure an efficient administrative process over the lifetime of user account or group. This means that when a user's access level needs to be changed or removed, updates in AD, Exchange and Windows are made automatically.

- Having privileged user accounts in privileged groups is a key vulnerability. You will be best served if your solution provides the capability to temporarily populate privileged groups while they're performing privileged tasks, then remove the member from the group when the task is complete. If the user account becomes compromised outside of the privileged window it will not have any elevated privileges so any compromise would be negligible.

Remove unnecessary permissions: Remove all unnecessary permissions from privileged accounts. If they don't need access—don't give it. When AD was first released, it was a huge improvement over the directory of NT 4.0 in that it had a delegation model. Not much has changed since then. Delegation needs of large enterprises are significantly more complex than native AD can possibly provide.

- Granular delegation – Natively granularly delegating rights in AD (particularly AD Admin rights) is difficult, time-consuming, and error-prone. Effective solutions provide automation, pre-built workflows, and reports to enable more granular access rights than native AD tools.
- Look for a solution that provides for any AD task or group of tasks to be easily delegated to any level, and even outside of AD's OU structure. This allows for flexibility in designing your permissions and delegation model and even allows for overlap of delegation without over-permissioning.

The NIST recommendations are general principals designed to apply to all information systems. Hopefully focusing some of those recommendations directly at AD provides valuable insight.
AD, as we know it, is in a state of transition itself. While working to secure the traditional on-premises AD, many enterprise initiatives are examining the feasibility of moving this critical service to the cloud. If your organization is using Office 365 or "O365", then you're already using AD in the cloud. With most enterprises that have already completed studies on cloud AD feasibiltiy, we see them coming to the conclusion that hybrid AD is the next logical step.

Help has arrived

Active Roles – Hybrid Active Directory, simple and secure

With today's hybrid AD environments and native tools with limited capabilities, Microsoft Active Directory (AD) and Azure Active Directory (AAD) administrators struggle to keep up with requests to create, change or remove access.
Thankfully, help has arrived. With One Identity Active Roles, you can solve your security issues and meet those never-ending compliance requirements by securing and protecting on-prem and cloud AD resources simply and efficiently.

- Overcomes native-tools limitations

- Manages identities for Exchange Online, Lync, SharePoint Online and Office 365 and many more
- Provides a single, intuitive tool for hybrid environment

With the cloud comes security questions. While Azure AD is offered from a FEDRAMP certified cloud, this doesn't mean that Microsoft is going to keep your policies around access and standardization in line. With Active Roles managing your on-prem AD as well as your Azure AD (AAD) you will be able to:

- Enforce strong and flexible policies for administration, structure, even attribute control.
- Synchronize on-prem AD with AAD through simple, easy to control connectors
- Manage both the on-prem and cloud ADs with a single interface (MMC or Web UI)
- Provide top-level admins with a familiar look and feel in an admin tool but control "accidents" with strong, flexible policies.
- Allow fine-grained access for administrators both in the on-prem and cloud AD

Creating well-thought-out policies to secure and manage AD can be a very complex task, but the critical piece of the security pie is how those policies are implemented. Writing them down and expecting administrators at all levels to abide and enforce is simply not reasonable. Active Roles from One Identity allows enterprises with large Active Directories to implement much stronger policies for control and delegation as well as enhance capabilities through automation.

CDM and NIST have both armed us with some good technology and concepts to make significant strides forward in securing the US Government critical information. While they don't specifically address securing on-prem or cloud AD, it is critical that we translate the concepts and apply them to the system that is providing millions of access decisions every day for every federal government agency.

About the Author .

Dan Conrad is an Identity and Access Management Expert with One Identity. Dan joined One Identity, a Quest Software business in 2007 and his responsibilities have included systems consultant and a solutions architect for compliance solutions. Dan's experience has led him to specialize in working with large federal government customers requiring complex solutions.

Dan started his government IT career in the Air Force where he administered networks with up to 100,000 users for more than 20 years. He retired from the USAF in 2004 as a Master Sergeant and returned to government IT as a contractor to the US Army MEDCOM where his primary focus was AD design, migration and sustainment.

Dan holds a Bachelor of Science degree in Information Systems Management from Wayland Baptist University and two Associates of Science degrees from the Community College of the Air Force. He holds many certifications, the highlights include Certified Information Systems Security Professional (CISSP), Microsoft Certified IT Professional (MCITP), and Microsoft Certified Systems Engineer/Microsoft Certified Systems Administrator (MCSE/MCSA).

For More Information

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

About One Identity

The One Identity family of identity and access management (IAM) solutions, offers IAM for the real world including business-centric, modular and integrated, and future-ready solutions for identity governance, access management, and privileged management.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our Web site (**www.quest.com**) for regional and international office information.

ONE IDENTITY™